

Telematics System Security

VACLAV JIROVSKY

Contents

1. Introduction.....	2
2. Security models	4
3. Cryptography	5
3.1 Basic Cryptosystems.....	6
3.2 Data Encryption Standard – DES	11
3.3 Other Used Ciphers.....	18
3.4 Public Key Cryptography	18
3.5 Cryptographic Checksum	22
3.6 Keyless hash function HMAC	24
3.7 Cipher Techniques – Block and Stream Ciphers	24
3.8 Cryptography in Networks.....	27
4. Attack analysis	30
4.1 Attacks by a User.....	31
4.2 Attacks by Service Provider.....	34
4.3 Attacks by Service Charger	35
4.4 Attacks by Hacker.....	36
4.5 Attacks by Hacktivist or Terrorist.....	38
4.6 Communication Provider Attacks.....	40
4.7 Attacks by Enterprise.....	40
4.8 Attacks by Government	42
4.9 Attacks by Foreign Power.....	43
5. Asset based threat analysis.....	44
5.1 Threatened Assets	44
5.2 Taxonomy of Threats	45
5.3 Threats, Objects and Assets	48
6. Technology of Wireless Attacks.....	50
6.1 Eavesdropping	50
6.2 Attack on Authentication	55
6.3 Skimming.....	58
6.4 Hiding and jamming	58
7. Conclusion	66

1 Introduction

Under telematic systems we usually understand the system consisting of many elements distributed in large territory where some of these elements are mobile elements. The behavior of the system consists of interaction among elements and we assume that these interactions have to be undisturbed – secure. Because we have seen some non-identical understanding in the scientific community, let us define the meaning of any possible misinterpreted term just for purpose of this chapter. Later on we will see important usage of these definitions.

First term, we have to define, is **safety**, used to assure that a life-critical system behaves as needed even when some pieces fail. We can distinguish among different extents of defective operation and usually we use term

- **fault**, when some piece of equipment does not operate as designed,
- **failure**, when a human being, the part of system, has to cope with the situation,
- **critical failure**, endangers one or a few people while
- **catastrophic failure**, endangers, harms or kills a significant number of people.

When looking for safety measures, we can identify different modes of safe operation of the system and we say that system is

- **probabilistically safe**, when system has no single point of failure, and enough redundant sensors, computers and effectors so that it is very unlikely¹ to cause harm,
- **inherently safe**, when system is a clever arrangement of parts that cannot cause harm, but this is not always possible²,
- **fail-safe**, when system is one that cannot cause harm even if it fails. A "fault-tolerant" system can continue to operate with faults though its operation may be degraded in some fashion.

These combined terms describe the term **safety** as it is accepted in the system theory. From the point of view, which we follow in this chapter, we have to accept a human as an integral part of the system, so failure of the system could be also caused by the human being incorporated. In the context of definitions above, the safe system cannot cause harm to any element of its own, so it means that it cannot cause harm to a human element too. Going further, under safety we can understand all measures leading to the survival of a human in the system, when unexpected situation will happen as a result of erroneous behavior of the internal element of the system, usually the human one. In this case an external or internal power causing harm or damage is a secondary entity, introduced as a result of erroneous behavior of the internal element. As an example of safety we can introduce measures incorporated by a designer to the car body, which should save the driver's life in the case of accident caused by the misoperation³ of the driver itself.

Now, when we define the safety, what can we do about security? The many of official definitions could be found, e.g. "The **security** is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences" [7]. In this sense, when we expect a human being as a part of system, the security should be understood as a complex of measures leading to the survival of a human in the system under influence of external hostile environment or influences. So, on the contrary to safety, the definition of security is calling for some primary external power to be introduced first. If we use an example of the car from the previous definition, the secure car will be designed to save lives of the crew, when the car is attacked by automatic gun shooting.

¹ Term "very unlikely" usually means that less than one human life is lost in when system operates for reasonably long time e.g. a billion hours.

² . For example, "inherently safe" airplanes are not possible.

³ Under the driver misoperation is assumed any situation which is caused by driver or improper driver reaction to its environment, including third party influence, even if, in the reality, driver had not been able to take any measures leading to return the car to normal operation.

In the security area we can be often dragged into some other important views of the system quality like reliability or privacy. The **reliability** covers “the ability of a system or component to perform its required functions under stated conditions for a specified period of time” [8]. It is often reported as a probability that a device will perform its intended function during a specified period of time under stated conditions. Mathematically, this may be expressed as

$$R(t) = \Pr\{T \succ t\} = \int_t^{\infty} f(x) dx \quad (1)$$

where

t - is the length of the period of time, which is assumed to start from time zero,

f(x) - is the failure probability density function,

R(t) – is a mathematical expression of reliability and

Pr – is an abbreviation for probability function.

First, it is clearly seen that reliability is a probability function, which means that failure of the system is regarded as a random phenomenon. We do not express any information on individual failures, the causes of failures, or relationships between failures, except that the likelihood for failures to occur over time according to the given probability function. Also, the reliability is restricted to operation under stated conditions. In the reliability area, we can also hear terms like survivability, resistance, resilience, persistence or failure counter. These terms are far away of our goal and some definitions could be found e.g. in [79].

Nevertheless, there is one important quality from the security point of view remaining – the very often discussed term “**privacy**”. According to Eric Hughes, we could define privacy as a “power to selectively reveal oneself to the world”[30]. More broadly, we could say that the privacy is the ability of a person to control the availability of information about and exposure of himself/herself to the environment. The privacy is also related to being able to function in a society anonymously, including pseudonymous or blind credential identification. From day-today life we know some examples of privacy giving rise to special concerns like

- **political privacy**, where secret ballot is the most widespread measure to ensure that political views are not known to anyone other than a voting person,
- **consumer privacy**, which covers laws and regulations seek to protect any individual from loss of privacy due to failures or limitations of corporate customer privacy measures,
- **medical privacy**, where law prevents doctors to release medical record of patient to any person than other doctors treating the patient. These records have been historically paper files inherently exposed some level of physical security being held in partial file in ambulance files of different doctors, mostly in an unintegrated fashion. With increasing influence of information technologies the files become more integrated and more accessible, so privacy of medical data becomes a real task of today,
- **information technology ends user privacy**; also called data privacy, Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. The challenge in data privacy is to share data while protecting the personally identifiable information.
- Consider the example of health data which are collected from hospitals in a district; it is a standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared.

The legal protection of the right to privacy in general and of data privacy in particular varies greatly throughout the world. Some ways in which privacy is lost include among others waiver of privacy right included in the terms of a contract or theft of confidential information, e.g. by computer cracking.

In the following chapters we focus on the security issues of the system and specifically on the telematic system. First of all we will describe a model of the telematic system from the point of view of security so we would be able to analyze the security conditions using the model defined. Then, the security analysis of each

part of the system will be provided and necessary security measures will be recommended and evaluated when appropriate.

2 Security models

The model of the telematic system from the security point of view could be discussed in two different models. The first model represents the general system security covering different views of system security including physical security, personal security or organizational security. The layered model of general system security is depicted in Fig. 1 and comprises

- **organization security**, which includes security of procedures, processes and management
- **personal security** covering employees security, visitors security and rules for classification of the information and
- **product security** consisting of application security and IT security including used technology and communication means.

The security layers described above are often developed as a specific discipline and anchored in specific security standards and rules. Individually we can deal with

- security, confidentiality and integrity policies including hybrid approach;
- identification and authorization of telematic object;
- etc.;

Last but not least we have to mention security issues covering different classes of security in the view of the security standards.

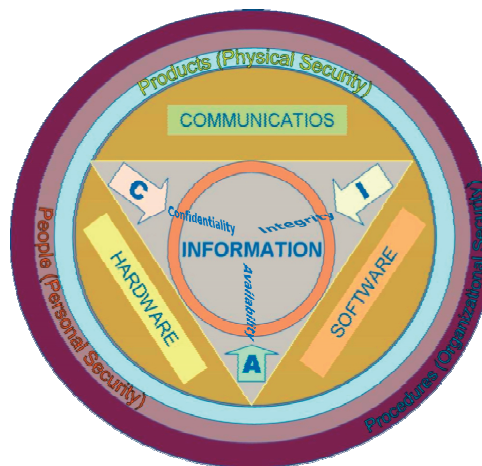


Fig. 1 Layered model of general system security

The second model could be a simple “technology” point of view as showed in Fig. 2. To discuss individual parts of the chain we have to state, that any of part of the chain could be attacked without exception. At the same time the pure technological view leaves out any intention of attack itself, dealing just with its technological mechanism.

Based on these presumptions we should specifically discuss mobile part of the telematic system (with yellow background)

- the sensor channel, where most of the information is coming from. The sensor channel could be understood either as real sensor of automotive unit or roadside equipment connected to actual local processing unit by wired or wireless channel or receiver of the information from environment. The example of the first case could be e.g. air pressure sensor in the automobile tire, which transfers information to the automobile control unit using wireless channel, the second case could be represented

by e.g. DSRC toll unit behind the automobile front window, receiving beacon from transmitter of the roadside equipment;

- wireless mobile communication channel which could be used for communication between
 - mobile units, automobiles and other transportation means, where communication channel is created between two moving objects;
 - mobile unit and fixed roadside equipment, where one part of the system is a moving object and the other one is fixed to the terrestrial environment of the trajectory of the moving object;

and the fixed part of the system created by

- common communication environment which could be based on any networking technology wired or wireless, used in telecommunication branch;
- processing part of the system consisting of information processing means as servers, storages, peripheral communication unit etc.

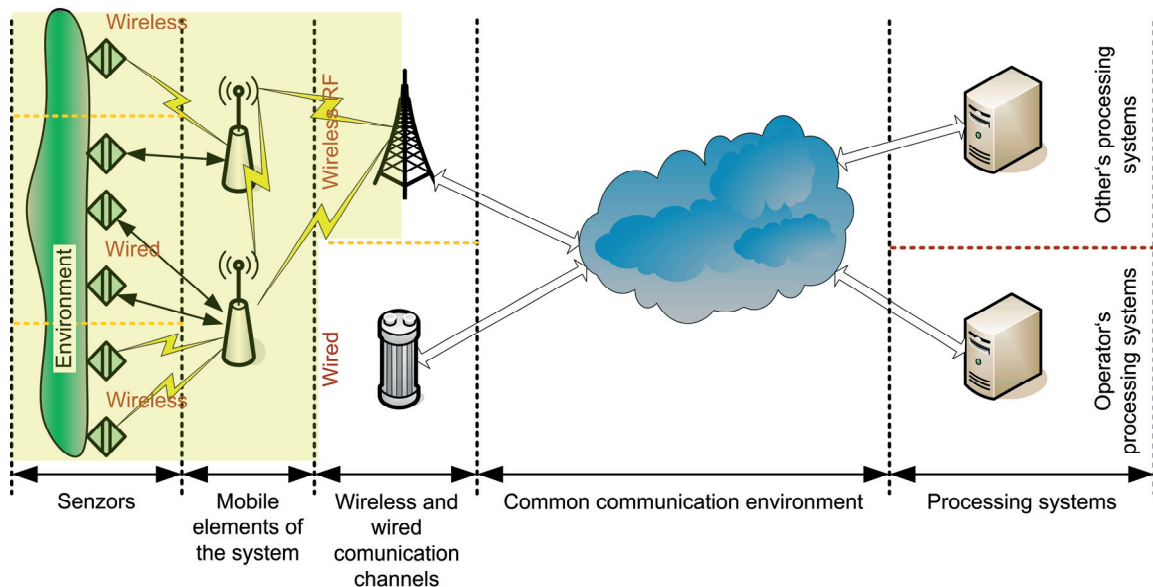


Fig. 2 The information flow chain for the security model of the telematic system

The most of the security issues in this chapter will be focused on

- physical properties of wireless signal transmission and its misusing;
- penetration of physical wireless and wired channels and their abuse;
- model of attacks on the link and network layer of the ISO/OSI model;
- using cryptography in telematic channels.

3 Cryptography

The cryptography is a supporting tool in any information system ensuring secure information exchange via channels which could be accessible to the public and potentially to the enemy. Cryptographic protocols are cornerstone for secure or hidden communication and mathematical methods behind the cryptographic algorithms used create deep mathematic subject. Within the context of the book we should only overview major points of the cryptography relevant to potential readers.

From historical point of view the name **cryptography** comes from two Greek words “κρυπτός” read as “kryptos”, which means “hidden” or “secret”; and “γράφειν”, read as “gráphin”, which is expression for “writing” [46]. We can also sometimes hear the word “**cryptology**”, created similarly by adding Greek word

“λογία”, meaning “to study”, to the root, as a name for the science studying principles of cryptography. The science targeted at the principles of breaking the cryptographic codes is known as “**cryptoanalysis**”. The basic component of cryptography is a cryptosystem which could be defined as follows:

Def. 1 *A cryptosystem is a five-tuple $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, \mathcal{C})$ where $\mathcal{M}$ is a set of plaintexts, $\mathcal{K}$ is a set of keys, $\mathcal{C}$ is a set of ciphertexts, $\mathcal{E}: \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$ is a set of enciphering functions and $\mathcal{D}: \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ is a set of deciphering functions.*

For better understanding the definition let us assume the well-known Caesar cipher in which letters in the text are shifted by a specific number of places. So, if the key is 3, then the letter “A” becomes letter “D” (in alphabet A, B, C, D, E ... encrypted letter is replaced by letter on position of the original letter plus 3), letter “B” becomes a letter “E” etc.

The goal of the cryptography is to keep enciphered information secret from the adversary even we assume that adversary knows the algorithm used to encipher original text called plaintext. In this case the key knowledge to decipher encrypted text is a **cryptographic key**. Three types of attack could be assumed

- **ciphertext only attack**, when the adversary has access to the ciphertext only. In this case the goal of the adversary is to find corresponding plaintext and possibly key used;
- **known plaintext attack**, when the adversary has in his possession a ciphertext as well as plaintext originally enciphered. The goal is to find the cryptographic key used to encipher the text or key to decipher the encrypted text¹;
- **chosen plaintext attack**, when encrypted plaintext is in the adversary’s possession and the adversary is asking if a specific plaintext has been a source for the encrypted ciphertext presented. The goal is to find a respective key used²;
- **chosen-ciphertext attack**, when the cryptanalyst may be able to choose ciphertexts and learn their corresponding plaintexts.

A good cryptosystem should protect against all four types of attacks.

The cryptoanalysis uses different methods, but the most important role is played by mathematics and statistics. The most well-known statistical methods use the so called “models of language” based on a different statistical characteristic of a specific language. A good example could be found in Edgar Allan Poe’s short story “The Gold Bug” where the author describes a cipher that uses polyphonic substitution. The detail description of a method for solving a simple substitution cipher using letter frequencies in English alphabet is described as a part of the mystery [59].

3.1 Basic Cryptosystems

The classical cryptosystems, also called symmetric or single key cryptosystems, are the systems using the same key for enciphering and deciphering. In mathematical sense we can write

$$D_k = E_k^{-1} \quad \text{for all } E_k \in \mathcal{C}, k \in \mathcal{K} \text{ where } D_k \in \mathcal{D} \quad (2)$$

where

$\mathcal{E}$ – is set of enciphering functions,

$\mathcal{D}$ – is set of deciphering functions,

¹ In the case of asymmetric cryptography two keys are used and the one used for encrypting of information is publicly known. In this case the goal of adversary is to find key for decryption of the enciphered text.

² **Well-known** attack of that type is called “gardening”, where the term was coined at Bletchley Park, England, during World War II. The gardening is scheme to entice the Germans to include known plaintext, which the British called “cribs”, in their encrypted messages. The technique used was claimed to have been most effective against messages produced by the German Navy's Enigma machines.

C – is set of ciphertext,

K – is set of keys¹.

There are two basic classical ciphers – transposition ciphers and substitution ciphers.

3.1.1 Transposition Ciphers and Substitution Ciphers

The transposition enciphering rearranges characters in the plaintext while letters are not changed, which could be understood mathematically as a permutation function. Because the permutation does not change the statistical characteristic of the plaintext, e.g. frequency of characters, the transposition cipher can be detected by comparing character frequencies with a model of the language.

Attacking a transposition cipher is possible by rearrangement of letters in the ciphertext. This process, known as anagramming, uses the so called n-gram frequency tables. Let us assume the well-known text from elementary programming “HELLO WORLD” which, by using transposition, could be encrypted as “HLOOLELWRD”. By using the Konheim’s digram table [37] the digram “HE” occurs in English with the frequency of 3,05%. Other important frequencies for the deciphering are listed in the [Table 1](#).

Table 1 Digram frequencies

Digram	Frequency in %
“HE”	3,05
“HO”	0,43
“HL”	> 0,1
“HW”	> 0,1
“HR”	> 0,1
“HD”	> 0,1
“WH”	0,26
“EH”	≥ 0,02
“LH”	≥ 0,02
“OH”	≥ 0,02
“RH”	≥ 0,02
“DH”	≥ 0,02

Using the [Table 1](#) we can suggest that character “E” follows character “H”. Let us arrange letters in such a way, that first two letters from the top of the diagram frequency table will form the top of the two letter column where the first block of five letters (“HLOOL”) is adjacent to the corresponding letter in the second block (“ELWRD”). The result is as follows

H	E
L	L
O	W
O	R
L	D

Reading the letters first in row and then in column order produces original plaintext “HELLO WORLD”. Another possible arrangement will be two lines of five letters, but this arrangement is compatible and leads to the same result.

On the contrary to the transposition ciphers, the substitution cipher changes characters in plaintext while producing ciphertext. Let us recall the Caesar cipher with key 3 discussed above in this chapter where each letter in the plaintext is substituted by a letter in three character distance. Mathematically, the letters are

¹ See definition Def. 1

mapped to the corresponding alphabet in distance 3. Such a cipher is susceptible to statistical ciphertext only attack. If we use our preferred plaintext “HELLO WORLD” and encrypt it by the Caesar cipher with key 3, we get ciphertext “KHOOR ZRUOG”. Computing frequency of each letter we obtain result as in Table 2.

Table 2 Statistical frequencies of characters in cipher

Character	Frequency
“G”	0,1
“H”	0,1
“K”	0,1
“O”	0,3
“R”	0,2
“U”	0,1
“Z”	0,1

To compare statistic found in the ciphertext and characteristic frequencies of the language model we have to use a frequency table for English, which could be found e.g. in [37] as it is shown in Table 3.

Table 3 English character frequency table

Char.	Freq.	Char.	Freq.	Char.	Freq.	Char.	Freq.
a	0,080	h	0,060	o	0,080	v	0,010
b	0,015	i	0,065	p	0,020	w	0,015
c	0,030	j	0,005	q	0,002	x	0,005
d	0,040	k	0,005	r	0,065	y	0,020
e	0,130	l	0,035	s	0,060	z	0,002
f	0,020	m	0,030	t	0,090		
g	0,015	n	0,070	u	0,030		

Now we apply the character based model and compute correlation value of the frequency of each letter in the ciphertext and character frequency of the same character according to (3).

$$\varphi(i) = \sum_0^{25} f(c)p(c-i) \quad (3)$$

where

$\varphi(i)$ – is the correlation of the frequency of the letter “i” with corresponding character in frequency table,

$f(c)$ – is a frequency of character “c” in ciphertext,

$p(c-i)$ – is frequency of a character at specified position in alphabet.

The value of $(c-i)$ has to be calculated in arithmetic modulo 26 and compared against Table 3, where letter “a” corresponds to position “0”, letter “b” corresponds to position “1” etc. By evaluation of equation (3) we obtain

$$\begin{aligned} \varphi(i) = & 0,1 \cdot p(6-i) + 0,1 \cdot p(7-i) + 0,1 \cdot p(10-i) + 0,3 \cdot p(14-i) + \\ & + 0,2 \cdot p(17-i) + 0,1 \cdot p(20-i) + 0,1 \cdot p(25-i) \end{aligned} \quad (4)$$

with enumeration of the (4) shown in graphical representation in Fig. 3.

This correlation should be a maximum when key “k” translates the ciphertext into English. We include the red watermark in the graph, which is empirically set to the value 0,054 just to point out important high values. Based on the watermark we can get the following plaintext solution

Table 4 Plaintext solution	
Value of “i”	Plaintext
3	HELLO WORLD
6	EBIIL TLOIA
10	AXEEH PHKEW

where the only meaningful text is generated when the key has value 3. As we can see, the statistics does not solve the ciphertext only problem directly, but substantially narrows the number of possible solutions.

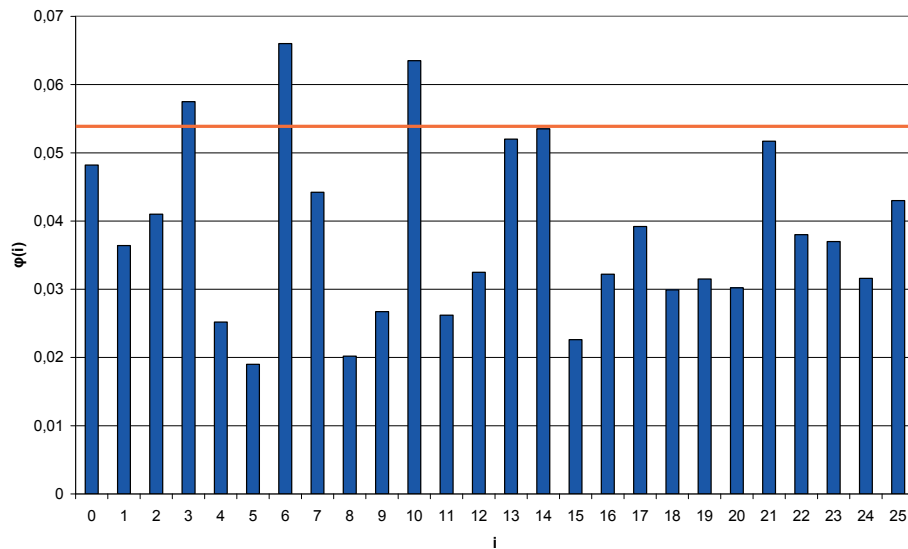


Fig. 3 Enumeration of equation (4)

3.1.2 Vigenère Cipher and One Time Pad

The code known as the cipher was originally described by Blaise de Vigenère in front of the court of Henry III of France¹, in 1586. Some sources assign the origin of the method to Giovan Battista Bellaso, lowering the attribution of Vigenère [33]. The Vigenère cipher gained a reputation for being exceptionally strong². The genius of Victorian era Charles Babbage was known to have broken a variant of the cipher as early as 1854, However, he didn't publish his work [68].

This type of ciphering is based on long random key which might obscure the statistic. The mechanics of Vigenère cipher works in such a way that it chooses sequence of keys represented by a string. Then, the key characters are applied to successive plaintext characters and, when the end of the key is reached, the process starts over again. The length of the key is called period of cipher.

For encryption and decryption of the text table called “Vigenère tableau” is used – the copy of the table is in Table 5. When encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

Table 5 Vigenère tableau

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

¹ Henry III (September 19, 1551 – August 2, 1589), fourth son of King Henry II and Catherine de' Medici.

² Scientific American described the Vigenère cipher as "impossible of translation" [35].

B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

As an example let us encipher our sentence “HELLO WORLD” using key “CODE”. The result is given in

Table 6 Enciphered text using key “CODE”

Key	C	O	D	E	C	O	D	E	C	O
Plaintext	H	E	L	L	O	W	O	R	L	D
Ciphertext	J	S	O	P	Q	K	R	V	N	R

The difference in the frequencies of letters in the ciphertext is measured and expressed as an **index of coincidence**. This value is defined as a probability that two randomly selected letters from the ciphertext will be the same. If F_c is the frequency of cipher letter “c” and N length of the ciphertext, than it could be shown that index of coincidence I for English alphabet is expressed as

$$I = \frac{1}{N(N-1)} \sum_{i=0}^{25} F_i \cdot (F_i - 1) \quad (5)$$

The lower index of coincidence calculated by equation (5) is, the longer period of the cipher is and less variations in the characters of the ciphertext could be expected. This index will be a valuable help for code breakers showing right way of their deductions.

The Vigenère cipher has been considered unbreakable for many years until Prussian cavalry officer Kasiski introduced a method of attacking polyalphabetic substitution ciphers, such as the Vigenère cipher [34]. It was first published in 1863, but it seems to be independently discovered by Charles Babbage as early as 1846 (see above). Kasiski noticed that repetitions occur when characters of the key appear over the same characters in the ciphertext and the number of character between the repetitions is a multiple of period. From the repetitions, we can set the probable period, using the index of coincidence to check the estimation. Applying Kasiski method,

Vigenère cipher the enciphered text with short key could be deciphered using pen and paper. For more complex and longer keys, a computer would be of good help.

The **one-time pad** is a version of Vigenère cipher when the key string is chosen at random and is at least as long as the message, so the repetition does not occur. This kind of enciphering, when knowing the ciphertext does not decrease the uncertainty of the plaintext is known as the **perfect secrecy** and could be defined as follows:

Def. 2 *Let M be a random variable that takes values from the set of messages $m_1, m_2, \dots, m_n$. The cipher $C=E(M)$ achieves perfect secrecy if $H(M | C)=H(M)$.*

For one-time pad the random variable M is selected from set of n -letter messages. In this case the uncertainty or entropy could be expressed in bits as $H(M)$

$$H(M) = -\sum_{i=1}^n p \cdot (M = m_i) \cdot \log_2 p(M = m_i) \quad (6)$$

where $\log_2$ means logarithm with the base 2. If the attacker intercepts e.g. $C = \text{RRTS}$ the conditional uncertainty (entropy) of M is $H(M | C)$ expressed as

$$H(M | C) = -\sum_{j=1}^m p \cdot (C = c_j) \cdot \left[\sum_{i=1}^n p(M = m_i | C = c_j) \cdot \log_2 p(M = m_i | C = c_j) \right] \quad (7)$$

However, the attacker has gleaned no more information than was initially available, because the key is four randomly chosen letters. Any message could produce the intercepted ciphertext. Hence $H(M | C) = H(M)$ and the cipher achieved perfect secrecy.

3.2 Data Encryption Standard – DES

The Data encryption Standard DES [53] was introduced to encipher sensitive but non-classified data. It is bit oriented cipher called **product cipher**, because of using both transposition and substitution enciphering methods. Its input, output and key are each 64 bit long and the set of 64 bit is referred as the **block**.

The cipher consists of 16 iterations, each iteration using separate key of 48 bits. These separate keys, known as “round keys” are generated from the key block by dropping parity bits. What is interesting, there are some serious questions about just why the standard key was 56 bits. Officially, the key length is 64 bits, but during the standardization process, the key was modified at the request of the NSA¹ so that 8 of the bits were used as parity checks. There have been a lot of speculations why the NSA pushed through this change. Journalist released an idea that NSA knew some kind of trick that could be used against a 56 bit key, or that 56 bits put the encryption within the range of what they could crack using a brute force attack. But no one has ever admitted to either solution and no one knows of any way that a 56 bit key could have been feasibly cracked using brute force with the technology of the time.

DES algorithm is a rather elegant combination of simplicity and complexity. It is simple repetitive structure based on lookup tables, which gives it deceptive simplicity. But it has to be said that those lookup tables are actually an implementation of a very complex non-linear discrete mathematical function. The basic structure is a three-step process: permute the input data, run it through a sequence of 16 passes using a ladder-like data flow structure, and then reverse the initial permutation. The permutation itself does not really add anything to the encryption. Nevertheless it adds a step to the computation and increases its complexity. Both permutations at the start and finish just add computation time, which prolongs the time needed to perform a brute-force attack.

¹ National Security Agency - is a cryptology intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. government communications and information systems, which involves cryptanalysis and cryptography.

Two input blocks of 32-bit pass after initial permutation through an encryption ladder called a Feistel¹ structure, where at each step, one of the two blocks is put through the so called a Feistel block. The output from the Feistel structure is then exclusive-ordered with the result of the previous step. This is illustrated by the diagram at Fig. 4.

The Feistel-box folds the encryption key into the process. The functionality of each F-box is illustrated in the diagram in Fig. 6. As an input there are 32 bit half-blocks, and a 48-bit sub-key. The Feistel-box fulfills the following functions

- expand the input half-block from 32 to 48 bits by reshuffling and copying some other bits. When numbering bits from 0 to 31, the expanded 48-bit block consists of following bits – 31, 0, 1, 2, 3, 4, 3, 4, 5, 6, 7, 8, 7, 8, 9, 10, 11, 12, 11, 12, 13, 14, 15, 16, 15, 16, 17, 18, 19, 20, 19, 20, 21, 22, 23, 22, 23, 24, 25, 26, 27, 28, 27, 28, 29, 30, 31, 0. In this bit structure we start with a copy of bit 31, and then use bits roughly in order duplicating pairs (3,4), (7,8), (11,12), (19,20), (22,23), (27,28) and ending with bit 0;
- exclusive-or the expanded half-block with the sub-key;
- split resulting 48 bits into eight six-bit micro-blocks;
- pass each six-bit micro-block through a substitution box, the so called S-box and generating a 4 bit result;
- the results of S-boxes are concatenated together, resulting in a 32 bit result;
- provide a permutation, giving the final output of the F-box.

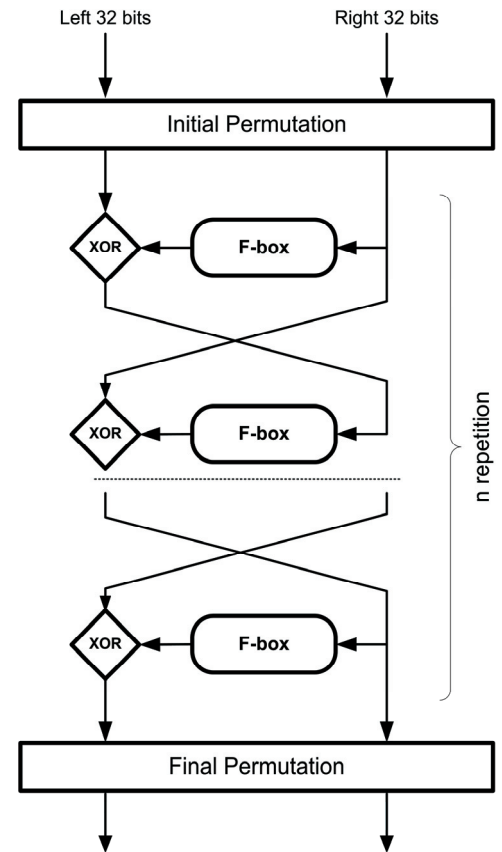


Fig. 4 DES encryption algorithm

In accordance with our previous text we can identify the expansion, X-or, and S-box complex as a sort of substitution cipher; and the final permutation as a kind of transposition cipher. So the full process of DES is a rather complicated series of permutations and substitutions. The magic of the permutation lies in the specific permutation functions or the S-box functions. These processes are based on lots of complicated tables and it is out of the framework of the chapter to describe it in details. The reader can get more information on the details of DES encryption procedure in e.g. [3].

The main role of the encryption key is that it effectively selects where the copied bits are really going to be passed through into the output of the S-boxes: since each S-box takes 6 bits, but loses two of them². It is controlled by the sub-key which four bits will pass. The process of generating sub-keys is similar to the ladder process connecting the F-boxes. We start with a 56 bit key, which will be permuted and then split in half. Then we push the result through a left-bitshift and a permutation, generating the first sub-key. Next shift and permutation generate the second sub-key. By repeating this process we obtain individual sub-key after each permutation. The process is illustrated in figure Fig. 7.

3.2.1 Feistel Networks

Feistel networks are a particular structure for designing symmetric encryption schemes. They were described within the context of the Lucifer³ cipher of IBM. A Feistel network is parameterized by round functions $f_1, \dots, f_d$ is a function $\{0, 1\}^{2^n} \rightarrow \{0, 1\}^{2^n}$ which adheres to the following program which operates in d rounds, typically between values 12 and 16, where the i -th round executes the following operations

¹ Horst Feistel (January 30, 1915–November 14, 1990), born in Berlin moved to the United States in 1934. His research at IBM led to the development of the Lucifer and Data Encryption Standard (DES) ciphers.

² As a matter of fact, it is a four-bit substitution.

³ Lucifer was the predecessor of the Data Encryption Standard (DES), which is built upon the same design.

- (i) split the round input into two halves $L_{i-1} \parallel R_{i-1}$,
- (ii) apply the round function f_i to the right half yielding $f_i(R_{i-1})$,
- (iii) compute the XOR of this value with the left half $L_{i-1} \oplus f_i(R_{i-1})$,
- (iv) swap the left and right side, thus yielding the round output $R_{i-1} \parallel L_{i-1} \oplus f_i(R_{i-1}) = L_i \parallel R_i$.

This process is depicted in Fig. 5. Feistel networks are appealing because of their simple design. The round functions f_i can be any functions; in particular it needs not to be invertible, but still the following definition could be proposed.

Def. 3 Every Feistel network $F : \{0; 1\}^{2n} \rightarrow \{0; 1\}^{2n}$ constitutes a permutation.

Feistel networks have an important property that the same hardware circuit can be used for both – encryption and decryption. There are two minor modifications when a ciphertext should be decrypted in a Feistel network, but these do not affect the network itself but the handling of inputs of the circuit, i.e., messages and inputs of round functions. Namely

- the round functions need to be applied in different order,
- writing $c = L_d \parallel R_d$ as the ciphertext, one inputs $R_d \parallel L_d$ to the network for decryption, i.e., one exchanges the left and the right half of the ciphertext.

Then one can easily verify that the round functions compute the decryption operation as defined in the above mentioned proof.

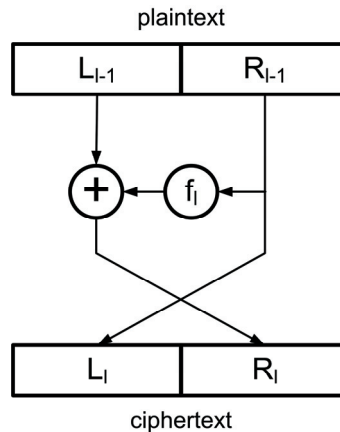


Fig. 5 One round in Feistel Network

The purpose of using Feistel function – the splitting the block, the shuffling through the ladder of F-boxes, the expansion, contraction, and permutation of the half-block as it moves through the F-box, could be seen more elegantly in terms of the information theory as "confusion and diffusion". When we shuffle bits around, we diffuse the bits of the plaintext message all over the place, so that without knowing how the key guided it, the end-result is a very complex string of information, which mixes the plaintext, the encryption key, and various information about the particulars of the S-boxes in a thoroughly confused and diffused way. There is a lot of information being added to the string, and without the key you don't know how to separate the information from the string you have.

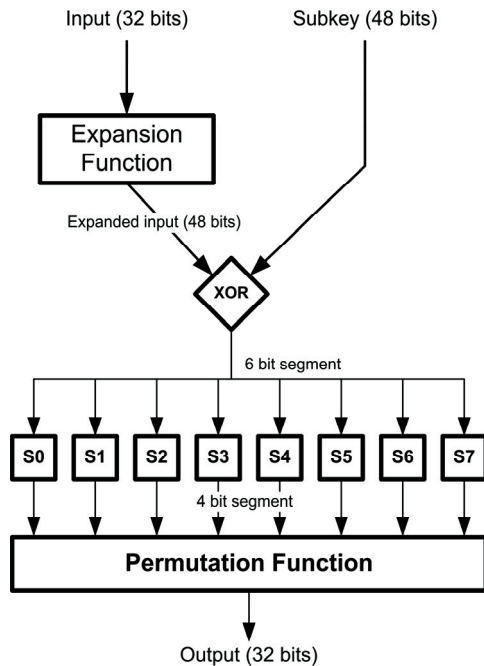


Fig. 6 Feistel box

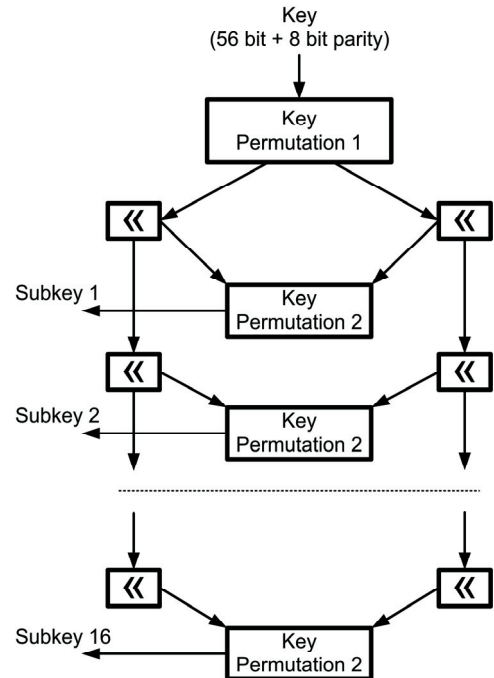


Fig. 7 Sub-keys generation

3.2.2 DES Modes of Operation

Given a block-cipher, there are several ways it can be used to actually encrypt long messages. FIPS PUB 81 defines four modes of operation – ECB, CBC, OFB, CFB), which can be applied to any block cipher. We will review them along with the counter mode (CTR) in further paragraphs.

3.2.2.1 Electronic Codebook (ECB) Mode

The Electronic Codebook (ECB) mode is defined as in Fig. 8. In ECB encryption, a plain text data block ($p_1, p_2, \dots$) is used directly as the DES input block. The input block is then processed through a DES device in the encrypt state. The resultant output block is used directly as cipher text ($c_1, c_2, \dots$) or may be used in subsequent applications.

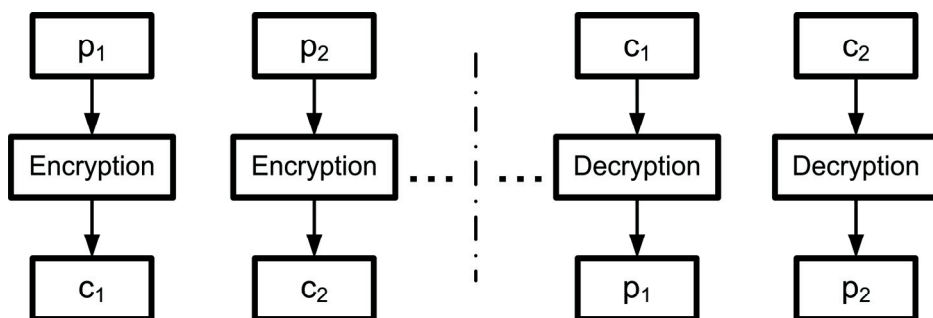


Fig. 8 Encryption and Decryption in ECB mode

In ECB decryption, a cipher text block ($c_1, c_2, \dots$) is used directly as the DES input block. The input block is then processed through a DES device in the decrypt state. The resultant output block ($p_1, p_2, \dots$) is the plain text or may be used in subsequent applications. The ECB decryption process is the same as the ECB encryption process except that the decrypt state of the DES device is used rather than the encrypt state.

3.2.2.2 Cipher Block Chaining (CBC) Mode

The Cipher Block Chaining (CBC) mode is defined as in Fig. 9. A message to be encrypted is divided into blocks. In CBC encryption, the first DES input block is formed by exclusive-ORing the first block of a message with a 64-bit initialization vector (IV). The input block is processed through a DES device in the encrypt state and the resulting output block is used as the cipher text.

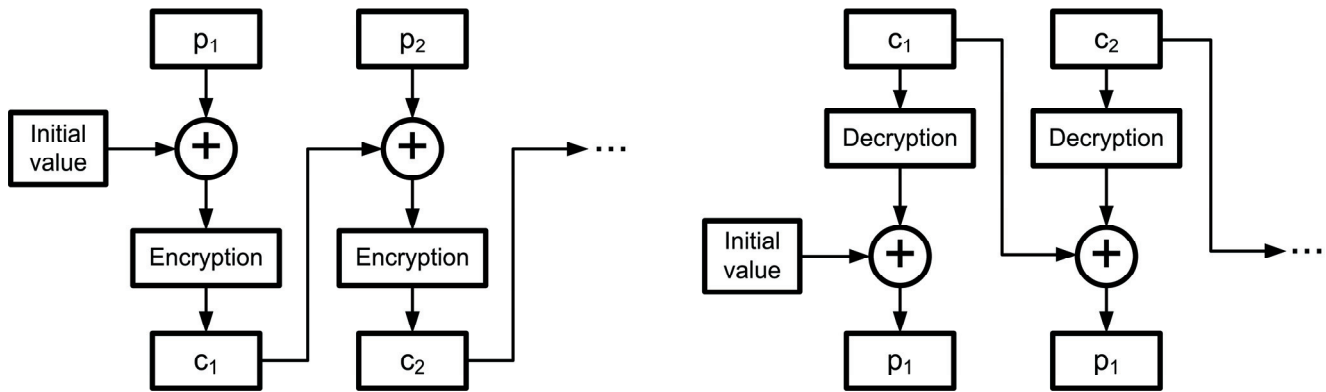


Fig. 9 Encryption and Decryption in CBC Mode

This first cipher text block is then exclusive-ORed with the second plain text data block to produce the second DES input block. The second input block is similarly processed through the DES device in the encrypt state to produce the second cipher text block. This encryption process continues to "chain" a successive cipher and plain text blocks together until the last plain text block in the message is encrypted. If the message does not consist of an integral number of data blocks, then the final partial data block should be encrypted in a way specified for the application.

In CBC decryption, the first cipher text block of an encrypted message is used as the input block and is processed through a DES device in the decrypt state. The resulting output block, which equals the original input block to the DES during encryption, is exclusive-ORed with the initial value, which must be the same as that used during encryption, to produce the first plain text block.

The second cipher text block is then used as the input block and is processed through the DES in the decrypt state and the resulting output block is exclusive-ORed with the first cipher text block to produce the second plain text data block. The CBC decryption process continues in this way until the last complete cipher text block is decrypted. Cipher text representing a partial data block must be decrypted in the way as specified for the application.

3.2.2.3 Cipher Feedback (CFB) Mode

The Cipher Feedback (CFB) mode is defined as in Fig. 10. A message to be encrypted is divided into data units each containing "k" bits. In both the CFB encrypt and decrypt operations, an initialization vector of proper length L is used. The initialization vector is placed in the least significant bits of the DES input block with the unused bits set to "0's".

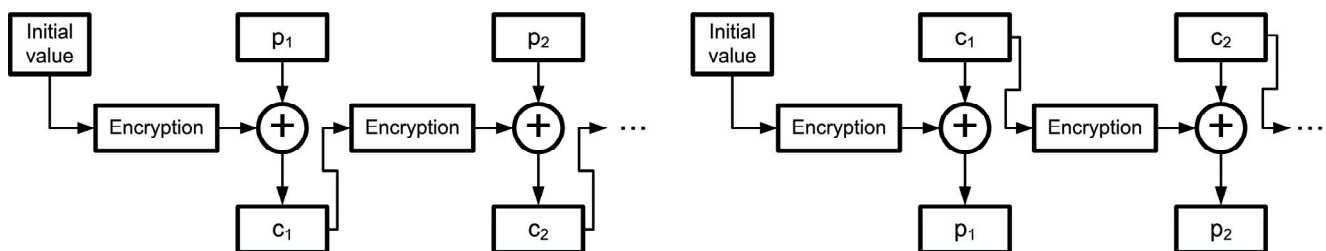


Fig. 10 Encryption and Decryption in CFB Mode

This input block is processed through the DES device in the encrypt state to produce an output block. During encryption, cipher text is produced by exclusive-ORing a K-bit plain text data unit with the most significant "k"

bits of the output block. Similarly, during decryption, plain text is produced by exclusive-ORing a K -bit unit of cipher text with the most significant “ k ” bits of the output block.

In both cases the unused bits of the DES output block are discarded. In both cases the next input block is created by discarding the most significant “ k ” bits of the previous input block, shifting the remaining bits “ k ” positions to the left and then inserting the “ k ” bits of cipher text just produced in the encryption operation or just used in the decrypt operation into the least significant bit positions. This input block is then processed through the DES device in the encrypt state to produce the next output block. This process continues until the entire plain text message has been encrypted or until the entire cipher text message has been decrypted.

The CFB mode may operate on data units of length l through 64 inclusive. K -bit CFB is defined to be the CFB mode operating on data units of length k for $k \in \{1, 2, \dots, 64\}$. For each operation of the DES device one k -bit unit of plain text produces one k -bit unit of cipher text or one k -bit unit of cipher text produces one k -bit unit of plain text.

An acceptable alternative for 8-bit CFB when enciphering 7-bit entities using an 8-bit feedback path is to insert a “1” bit in bit position one of the 8-bit feedback paths. This alternative is called the 7-bit CFB(a) mode of operation and results in a “1” being always placed in bit location 57 of the DES input block.

3.2.2.4 Output Feedback (OFB) Mode

The Output Feedback (OFB) is similar to CFB mode and it is defined according to Fig. 11. A message to be encrypted is divided into data units each containing “ k ” bits where $k \in \{1, 2, \dots, 64\}$. In both of the OFB encrypt and decrypt operations, an initialization vector of proper length is used. The initialization vector is placed in the least significant bits of the DES input block with the unused bits set to “0’s”. This input block is processed through the DES device in the encrypt state to produce an output block. During encryption, cipher text is produced by exclusive-ORing a k -bit plain text data unit with the most significant “ k ” bits of the output block.

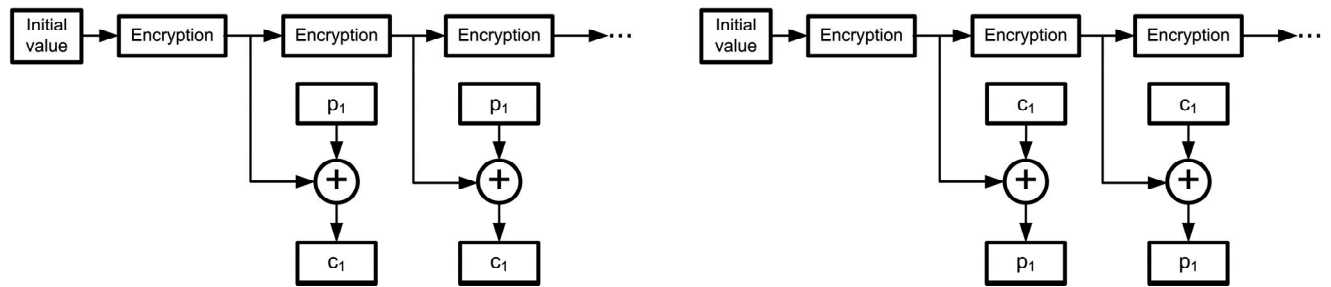


Fig. 11 Encryption and Decryption in OFB Mode

There are also some other advanced modes like (Counter Mode) which is similar to OFB and which turns a block cipher into a stream cipher. It generates each block of the stream cipher by encrypting successive values of a “counter”. The counter can be any simple function which produces a sequence that is guaranteed not to be repeated for a long time. However using an actual counter is the simplest and most popular choice.

3.2.3 Strengthening DES

Several ways were proposed for strengthening DES and, in particular, for coping with its major problem with the short key-size. In the following text, we shall present some of them.

3.2.3.1 Double-DES (2DES)

A first attempt at strengthening DES consisted in applying the encryption operation twice with different keys ($K1; K2$), thus computing $E(K1; E(K2; p))$. While the original intention was to double the effective key-size, Double-DES does not improve much on the security of DES because of a “man-in-the-middle” attack, which can be summarized as follows. Let us assume that we are given a plaintext/ciphertext pair ($p; c$), i.e., $c = E(K1; E(K2; p))$ for some $K1$ and $K2$ which should be decrypted by adversary. So the necessary steps will be

- (i) Decrypt the given ciphertext c with every possible key K where the number of possible key is 2^{56} . This yields a table with combination of all keys, so this step requires 2^{56} executions of DES.
- (ii) Sort this table with respect to the second entry. This takes steps in the order of $2^{56} \log(2^{56})$.

(iii) Encrypt the message p with any possible key K_i and look up the resulting encryption in the second column of the table, until a matching ciphertext $E(K_i; p)$ is found. Let i be the row containing such a ciphertext. This step takes at most 2^{56} executions of DES.

(iv) Let K_2 denote the key in the first column of the table at row i . Then the correct key is

$$(K_1, K_2^i) \quad (8)$$

Since the sorting step does not produce a noticeable overhead over execution DES 2^{56} times, we ignore its cost in the overall complexity. Then one sees that the total number of DES executions is $2 \cdot 2^{56} = 2^{57}$, so the effective key-length of Double-DES is at most 57 bits. Since there is almost no improvement over DES, Double-DES is in fact never used.

3.2.3.2 3.5.2 Triple-DES (3DES)

A very common variant of DES is Triple-DES (3DES); in fact, this construction can be applied to any block cipher to increase its effective key-size. Given three independent DES keys K_1 ; K_2 ; K_3 one calculates 3DES as follows:

$$E^{3DES}((K_1, K_2, K_3), m) := E(K_1, D(K_2, E(K_3, m))) \quad (9)$$

Decryption is given by

$$D^{3DES}((K_1, K_2, K_3), m) := D(K_3, E(K_2, D(K_1, m))) \quad (10)$$

Using such a method the key size is increased to $3 \cdot 56 = 168$ bits. However, a man-in-the-middle attack is also possible

3.2.3.3 3.5.3 DESX

Another variant of DES is DESX, which is not that widely used although it provides an even larger effective key size than 3DES and is even roughly three times faster. A key is defined as a triple $(K_1; K_2; K_3)$ where $K_1, K_3 \in \{0, 1\}^{64}$ and $K_2 \in \{0, 1\}^{56}$. Thus K_2 is a DES key and K_1, K_3 are random binary strings of the same length as the message blocks. Encryption and decryption are defined as

$$\begin{aligned} E^{DESX}((K_1, K_2, K_3), p) &:= K_3 \oplus E(K_2, K_1 \oplus p) \\ D^{DESX}((K_1, K_2, K_3), c) &:= K_1 \oplus E(K_2, K_3 \oplus c) \end{aligned} \quad (11)$$

The following theorem was given by Kilian and Rogaway in 1998; it proves that DESX has an effective key size of at least 119 bit.

Def. 4 Let (E, D) be an ideal cipher with key size l and block size b . Let $(K_1, K_2, K_3) \in \{0, 1\}^{2b+l}$, and let $EX((K_1, K_2, K_3), m) := K_3 \oplus E(K_2, K_1 \oplus m)$ a cipher having key size $k = 2b + l$. Then the effective key size of EX is at least $k - b - l = b + l - l$ bit. In particular, the effective key size of DESX is at least $64 + 56 - l = 119$ bits.

Similarly, during decryption, plain text is produced by exclusive-ORing a k -bit unit of cipher text with the most significant “ k ” bits of the output block. In both cases the unused bits of the DES output block are discarded and the next input block is created by discarding the most significant “ k ” bits of the previous input block, shifting the remaining bits “ k ” positions to the left and then inserting the “ k ” bits of output just used into the least significant bit positions. This input block is then processed through the DES device in the encrypt state to produce the next output block. This process continues until the entire plain text message has been encrypted or until the entire cipher text message has been decrypted.

The OFB mode may operate on data units of length 1 through 64 inclusive. K-bit OFB is defined as the OFB mode operating on data units of length “k” for $k = 1, 2, \dots, 64$. For each operation of the DES device one k-bit unit of plain text produces one k-bit unit of cipher text or one k-bit unit of cipher text produces one k-bit unit of plain text.

3.3 Other Used Ciphers

To overcome weakness of the DES enciphering, several algorithms were proposed. The so called NewDES, which despite of its name has no mutual properties with original DES, is a new algorithm with block size of 64 bits and key length of 120 bits [64]. However this cipher could be broken by using an attack similar to differential cryptanalysis [62]. Another cipher with block size of 64 bits and key size of 64 bits is FEAL¹ cipher. FEAL is designed to be much faster in software and based on Feistel algorithm similarly to DES. There have been several different revisions of FEAL, though all are Feistel ciphers, and make use of the same basic round function and operate on a 64-bit block [51, 66]. The FEAL encryption algorithm was originally designed as software for 8-bit microprocessors but later FEAL-N/NX variants were developed to improve the security. There N represents a number of rounds with 64-bit keys, NX using 128-bit keys. The most recently used version is FEAL-32X.

REDOC-II operates on 80-bit blocks using 160-bit key [22]. The cipher has 10 rounds, and uses key-dependent S-boxes and masks used to select tables for different rounds of the cipher. REDOC III is more efficient cipher operating on 80-bit block and accepts a variable-length key of up to 20 480 bits [62]. The algorithm consists only of XOR-ing key bytes with message bytes, and uses no permutations or substitutions.

As a proposed alternative of DES, the LOKI89 cryptosystem was designed [20]. Nevertheless, because of its vulnerability to differential cryptanalysis [14], had been replaced by the successor LOKI91 [19]. Khufu has a block size of 64 bits and key size of 512 bits [49]. When used with 24 or 32 rounds, it is resistant to a chosen plaintext attack. The S-boxes of Khufu are computed from keys. Similar cipher Khafre [49] uses fixed S-boxes, but it is probably the reason why it has been broken [14].

IDEA², developed by Xuejia Lai and James Massey, is generally regarded to be one of the best and most secure block algorithms available to the public today. It uses a 64-bits block and 128-bit key [41] and it is designed to be resistant to differential cryptanalysis. The encrypting uses three major operations – exclusive OR, addition modulo 2^{16} and multiplication modulo $2^{16} - 1$. Some attacks³ have been made against reduced round IDEA [62, 13]. IDEA was used in Pretty Good Privacy (PGP) v2.0 [25], and is an optional algorithm in the OpenPGP standard.

3.4 Public Key Cryptography

The biggest problem of dissemination of encrypted messages is the distribution of keys. Let us suppose we want to pass information secretly to our party which is far away, we need to agree on some sort of key that we both can use to encode/decode messages. The pain (in the neck) is how to move a key secretly. If we mail them, they might be stolen. If we send them cryptographically, and someone has broken your code, that person will also have the next key. If we have to go to party location regularly to hand-deliver the next key, that is not only expensive, but it also shows that we are in contact. If we hire some courier to deliver the new key, we have to trust the courier etc.

The public key cryptography solves this problem by using one way coding. The encipherment key is public, so to send a secret message would be easily achieved by encrypting the message by “public key”. At receiving side, the message cannot be deciphered by using the same public key, but only by using “private key”, which is orthogonal to the public key. The orthogonality is achieved by special function. Because one key is public and its complementary key must remain secret, a public key cryptosystem must meet the following three conditions

- it must be computationally easy to encipher or decipher a message given the appropriate key,
- it must be computationally infeasible to derive the private key from the public key,

¹ Fast data Encipherment ALgorithm

² IDEA – International Data Encryption Algorithm. IDEA is patented; licensing information can be obtained from Ascom.

³ No successful linear or algebraic weaknesses have been reported. The best attack which applies to all keys can break IDEA reduced to 6 rounds; the full IDEA cipher uses 8.5 rounds.

- it must be computationally infeasible to determine the private key from a chosen plaintext.

The first cipher to meet these requirements generates a shared session key. The second one provides both – secrecy and authentication.

3.4.1 Diffie-Hellman coding

The Diffie-Hellman scheme [23] was the first public key cryptosystem proposed. A pair of users uses this algorithm to generate a common key. The generation is based on a discrete logarithm problem of finding logarithms in a finite field. Given a field definition, such definitions always include some operation analogous to multiplication, so it is always possible to construct an analog of exponentiation, and two numbers, a base and a target, find the power which the base must be raised to in order to yield the target. In mathematical language: to find value of k such that $n = g^k \pmod{p}$ for given set n, g , and prime p . Although solutions are known for small values of p , the difficulty increases exponentially as p increases [42].

In Diffie-Hellman cryptosystem all users share a common modulus p and number g different from $0, 1$ or $p-1$. Each user chooses a private key k and computes its public key K . When two users communicate, each one enciphers the other's public key using their own private key, and uses the result as shared secret key S .

Example 1:

Two users A and B have chosen common $p = 53$ and $g = 17$. They also choose their private keys to be $k_A = 5$ and $k_B = 7$. Their public keys are $K_A = 17^5 \pmod{53} = 40$ and $K_B = 17^7 \pmod{53} = 6$. When user B wants to send a message to user A, it computes a shared secret key by enciphering public key user A using his private key

$$S_{B,A} = K_A^{k_B} \pmod{p} = 40^7 \pmod{53} = 38$$

and encipher its message using this key. When user A receives the message, it computes the key it shared with user B as follows

$$S_{A,B} = K_B^{k_A} \pmod{p} = 6^5 \pmod{53} = 38$$

and subsequently decipher the message. The mathematical properties of modular exponentiation ensure that for any two users A and B is $S_{A,B} = S_{B,A}$.

Because users share a common secret key S , the Diffie-Hellman scheme is an example of a symmetric key exchange protocol. Under the assumption that solving the discrete logarithm problem is computationally infeasible, deriving private key from corresponding public key is also computationally infeasible. In practice, p must be very large for this assumption to be met (hundreds of bits).

Diffie and Hellman proposed a system that requires the dynamic exchange of keys for every sender-receiver pair and in practice, usually for every communications session, hence the term “session key”. This two-way key negotiation is useful in further complicating attacks, but requires additional communications overhead. This was one of the reasons for designing the RSA system, which reduces communications overhead with the ability to have static, unchanging keys for each receiver that are “advertised” by a formal “trusted authority” or distributed in an informal “web of trust”. Before we continue with the description of RSA encryption system we need some more mathematical background.

3.4.2 Mathematical background for RSA

The public key cryptography is based on some theorems listed below. The first one is Fermat's Little Theorem

Def. 5 If p is a prime number, and a is an integer such that $(a, p) \equiv 1$, then $a^{p-1} \equiv 1 \pmod{p}$.¹

The extension of Fermat's Little Theorem deals with relative primes and creates a good background to build an asymmetric (public) cryptography system based on distinguishing between encipherment and decipherment keys.

Def. 6 If $(a, m) \equiv 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is the number of integers less than m that are

¹ Two integers a and p are “coprimes” or “relative primes”, which means that their greatest common divisor is 1.

relatively prime to m . The number m is not necessarily prime.

To use the theorems mentioned above we still need one theorem more, the theorem called Chinese remainder theorem. The theorem provides a correspondence between a system of equations modulo a set of pair-wise relative prime moduli and an equation modulo of their product.

Def. 7 Let p and q be two numbers, not necessarily primes, but such that greatest common divisor $(p, q) = 1$. Then if $a = b \pmod{p}$ and $a = b \pmod{q}$ we have $a = b \pmod{p \cdot q}$.

These three theorems create mathematical background for RSA cryptographic system.

3.4.3 RSA cryptography

RSA¹ is an exponentiation cipher using two keys – public key and private key. While the public key can be known to everyone and is used for encrypting messages, messages encrypted with the public key can only be decrypted using the secret private key. If we choose two large prime numbers p and q and let $n = p \cdot q$ then the totient² $\phi(n)$ of n is the number of numbers less than n with no common divisor with n .

Example 2:

$\phi(4) = 2$ (1 and 3 are relatively prime to 4),
 $\phi(5) = 4$ (1, 2, 3, and 4 are relatively prime to 5),
 $\phi(6) = 2$ (1 and 5 are relatively prime to 6),
 $\phi(7) = 6$ (1, 2, 3, 4, 5, and 6 are relatively prime to 7),
 $\phi(8) = 4$ (1, 3, 5, and 7 are relatively prime to 8), and
 $\phi(9) = 6$ (1, 2, 4, 5, 7, and 8 are relatively prime to 9).

Let choose integer $e < n$ that is relatively prime to $\phi(n)$. Find a second integer d such that

$$e \cdot d \pmod{\phi(n)} = 1 \quad (12)$$

The public key is in the case (e, n) and the private key is d . If m will be a message, then $c = m^e \pmod{n}$ and $m = c^d \pmod{n}$.

Example 3:

Let $p = 7$ and $q = 11$. Then $n = 77$ and $\phi(n) = 60$. If user A chooses $e = 17$ its private key will be $d = 53$. In this cryptosystem each plaintext character is represented by number between 0 ("A") and 25 ("Z"), number 26 represents a blank. If user B wants to send a message to user A it has to code it according to the representation of characters above. Assume that user B wants to send plaintext "HELLO" to user A , so it has to code sequence 07 04 11 11 14 using user A public key. The resulting ciphertext will be
 $07^{17} \pmod{77} = 28$
 $04^{17} \pmod{77} = 16$
 $11^{17} \pmod{77} = 44 \dots$
Resulting ciphertext will be 28 16 44 44 42.

In addition to confidentiality, RSA is able to provide data and origin authentication. If user A enciphers her message using her private key, anyone can read it, but if anyone alters the message, altered message cannot be deciphered correctly. Also, there could be dual enciphering – first private key of user A and then public key of user B . When user B receives the message it decodes it first by its private key and resulting message deciphered by public key of user A . So the recipient uses the recipient's private key to decipher the message and the sender's public key to authenticate it.

¹ RSA stands for **R**ivest, **S**hamir and **A**dleman who first publicly described it for public-key cryptography.

² Euler's Totient Function is denoted by the Greek letter phi, and is defined by number of numbers between 1 and $N-1$ which are relatively prime to N .

Example 4:

Suppose that user “A” wants to send a message to user “B” message “HELLO WORLD” encrypted and authenticated. Again, assume that user “A” private key is 53 and the user “B” public key is 37 (and its private key will be 13 according to equation (12) using $\phi(n)=60$). The plaintext will be represented by sequence of decimal values 07 04 11 11 14 26 22 14 17 11 03. So enciphering the plaintext using user “A” private key we obtain

$$\begin{aligned}
 (07^{53} \bmod 77)^{37} \bmod 77 &= 07 \\
 (04^{53} \bmod 77)^{37} \bmod 77 &= 37 \\
 (11^{53} \bmod 77)^{37} \bmod 77 &= 44 \\
 (11^{53} \bmod 77)^{37} \bmod 77 &= 44 \\
 (14^{53} \bmod 77)^{37} \bmod 77 &= 14 \\
 (26^{53} \bmod 77)^{37} \bmod 77 &= 59 \\
 (22^{53} \bmod 77)^{37} \bmod 77 &= 22 \\
 (14^{53} \bmod 77)^{37} \bmod 77 &= 14 \\
 (17^{53} \bmod 77)^{37} \bmod 77 &= 61 \\
 (11^{53} \bmod 77)^{37} \bmod 77 &= 44 \\
 (03^{53} \bmod 77)^{37} \bmod 77 &= 47
 \end{aligned}$$

Resulting ciphertext received by user “B” is 07 37 44 44 14 59 22 14 61 44 47. When user “B” wants to decipher the ciphertext, he has to use recipient private key, that means its own private key, to decipher the message

$$\begin{aligned}
 07^{13} \bmod 77 &= 35 \\
 37^{53} \bmod 77 &= 09 \\
 44^{53} \bmod 77 &= 44 \\
 \dots \\
 47^{53} \bmod 77 &= 05
 \end{aligned}$$

and then the sender’s public key to authenticate it. The final decoding is

$$\begin{aligned}
 07^{17} \bmod 77 &= 07 \\
 07^{17} \bmod 77 &= 04 \\
 07^{17} \bmod 77 &= 11 \\
 \dots \\
 07^{17} \bmod 77 &= 03
 \end{aligned}$$

If the enciphered message is changed, the receiver will receive an unreadable code.

It should be said that use of public key system provides a technical means for nonrepudiation of origin. The message is deciphered by using user A public key and, because the public key is orthogonal to the private key, only the private key could have enciphered the message. Because user A is the only one who knows this private key, only this user can encipher the message. The underlying assumption is that user A private key has not been compromised or someone has not impersonated user A as well as that the public key bearing the name of user A really does belong to it.

In practice, no one would use block of the size presented here. The issue is that RSA cannot be broken by using techniques to break classical substitution enciphering¹. Furthermore, although no individual block can be changed without detection, an attacker can rearrange blocks and change meaning of the message.

Example 5:

To show the robustness of RSA coding let us assume two simple messages used by a military unit. In both examples a high commander sends a message to headquarters requesting simple answer “ON” or “NO”.

¹ From previous examples it could be deducted that ciphertext could be easily deciphered by using e.g. statistics of characters in English alphabet. This is only fiction arised from simple example.

Story 1:

The high commander is asking headquarters if attack is ON. The headquarters respond with simple message “ON” enciphered by RSA cipher with 2048 bit modulus, but each letter is coded in a separate block padded with random numbers. Let’s assume, that attacker intercepts the message and swaps order of blocks. In this case after deciphering, the high commander will receive a quite opposite message “NO”, which is definitely not correct. Moreover, if the attacker knows that headquarters use only two messages, then it can break the cipher.

Story 2:

Let’s assume the same situation as before, but the block is composed of six bit block number, then the character coded and remaining bits of random data. In this case, rearranging of blocks cannot be used – it will be simply disclosed. To find which block contains letter “O” is also difficult, because in this case the attacker needs 2^{1010} computations, which is at the moment computationally infeasible.

3.5 Cryptographic Checksum

In the common view the checksum is a mathematical function generating a set of k bits from a set of n bits where $k \ll n$. If someone is going to send a message to other party and wants to give an opportunity to other party to verify if the message was received correctly, adding a small deterministic chunk of bits at the end of message should help.

Def. 8 *A cryptographic checksum function (also called hash function or one-way function) $h: A \rightarrow B$ is a function with following properties*

- For any $x \in A$, $h(x)$ is easy to compute
- For any $y \in B$ is computationally infeasible to find $x \in A$ such that $h(x) = y$
- It is computationally infeasible to find $x, x' \in A$ such that $x \neq x'$ and $h(x) = h(x')$

We have to add another definition describing the situation in third property of definition above.

Def. 9 *If $x \neq x'$ and $h(x) = h(x')$, x and x' are in collision.*

Also the third property could be rephrased as in

Def. 10 *Given $x \in A$, it is computationally infeasible to find another $x' \in A$ such that $x \neq x'$ and $h(x) = h(x')$.*

Even though the third property in Def. 8 looks similar to Def. 10, they are subtly different. It is considerably harder to find an x' meeting the conditions in Def. 10 than to find a pair x and x' meeting the condition in third property of Def. 8. To explain this statement we have to discuss some properties of cryptographic function.

Let us have a checksum containing fewer bits than the message. There have to be more messages than one, producing the same checksum. Furthermore, given any message, the checksum it produces can be determined only by computing the checksum, so cryptographic checksum behaves as a random function. The size of output of cryptographic checksum is important and related to the so called pigeonhole principle, which looks obvious.

Def. 11 *Pigeonhole principle: If there are n containers for $n+1$ objects, at least one container holds two objects.*

To understand the principle above, consider cryptographic checksum function that computes hashes of four bits and set of files each of which contains six bits. This yields $2^4=16$ possible hashes and $2^6=64$ possible files. Hence, four different files correspond to the same hash.

Now let us assume that we have a hash function of 128 bits, so apparently the probability to find a message corresponding to a given hash would be 2^{-128} . Nevertheless, the probability of finding two messages with the same hash will be a half of it, 2^{-64} . Actually, while the pigeonhole principle shows us the obvious fact that to

place $n+1$ object into n containers one expects that there should be at least one container consisting of more than one object, pointing out the collision problem, to find the amount of collisions is a different story.

This sort of problem is known under the name of the “birthday paradox”. Let us try to explain why there is a chance that among 23 randomly chosen people there would be two who share the same birthday with probability of almost 51%. The intuition would suggest it should be much less, hence the name, even there is nothing paradoxical. Among 23 people there are 253 pairs, each of which has one-to-365 odds of being a hit. The reason why statement above appears counter intuitive is because your chances of finding among 22 people somebody with the same birthday as yours and not just someone else’s are strongly against you. This could explain why inverting a hash function would be much more difficult than just finding a collision. When analyzing the birthday paradox we shall find that in order to attain probability better than 50% of finding a collision in a hash function with n -bit output, it suffices to evaluate the function on approximately $1,2 \cdot \sqrt{2n}$ randomly chosen inputs¹.

Def. 12 *A **keyed** cryptographic checksum function requires a cryptographic key as a part of computation while a **keyless** does not.*

Regarding the definition Def. 12, keyed hash function, accepts as an input a secret key and an output, short piece of information, could be used to authenticate a message. The algorithm, sometimes called the “MAC value” protects both the message’s data integrity as well as its authenticity by allowing verifiers² to detect any changes to the message content. MACs differ from digital signatures which we learned in an asymmetric coding, just because the MAC values are both generated and verified using the same secret key (symmetric encryption). As a matter of fact, due to this property, MACs do not provide the non-repudiation function.

Some authors substitute a Message Integrity Code (MIC) in place for the term MAC³. However, the MIC is a usually understood distinct term from MAC, not expecting that operations use secret keys – so it means that any MIC intended for ensuring message integrity has to be encrypted or otherwise protected against tampering. While the MIC algorithm always produces the same MIC, assuming the same algorithm is used, the MAC algorithm is designed to produce matching MACs only if the same input – message, secret key and initialization vector is used. Implementation of MAC algorithms can be constructed from other simple cryptographic algorithms, or constructed especially and based on universal hash function.

Example 6:

Let us consider DES enciphering working in Cipher Block Chaining (CBC) method used as a message authentication code if 64 bits or fewer is required. The message is enciphered and last “ n ” bits of the last output create cryptographic hash. Because the DES requires a cryptographic key, the hash function is keyed cryptographic checksum function⁴. Assuming that hash is at most 64 bits, to find two inputs producing the same hash requires 2^{32} messages.

The example of keyless hash functions are in Table 7. All these functions, keyed or keyless, are used by cryptographic applications to create “fingerprints” of much longer messages. They use different names – cryptographic checksum, hash, digital signature or digest.

In Table 7 there are two columns dealing with attack complexity

- the **preimage attack** is a classification of attacks on hash functions finding a message that has a specific hash value. There are two types of preimage attacks
 - first preimage attack – given a hash h , finds a message m such that $\text{hash}(m) = h$,
 - second preimage attack – given a fixed message m_1 , finds a different message m_2 such that $\text{hash}(m_2) = \text{hash}(m_1)$;
- the **collision attack** – based on finding two arbitrary different messages m_1 and m_2 such that $\text{hash}(m_1) = \text{hash}(m_2)$.

¹ Using this equation we shall find that nearest upper integer of $1,2 \cdot \sqrt{365}$ is 23.

² Assuming that verifier also possess the secret key.

³ It happens especially in communication, where the acronym MAC is traditionally used for Media Access Control.

⁴ Also called DES-MAC.

The collision attack has a modification, the so called prefix collision attack dealing with two different prefixes p_1, p_2 find two appendages m_1 and m_2 such that $\text{hash}(p_1 \parallel m_1) = \text{hash}(p_2 \parallel m_2)$ (where “ $\parallel$ ” is used for the concatenation operation).

Table 7 Examples of keyless hash functions

Algorithm	Output size (bits)	Block size	Length size	Word size	Attack complexity	
					Collision attack	Preimage attack
MD2	128	128	–	32	$2^{63,3}$	2^{73} [70]
MD4	128	512	64	32	3 [52]	$2^{70,4}$ [28]
MD5	128	512	64	32	$2^{20,96}$ [75]	$2^{123,4}$ [61]
SHA-1	160	512	64	32	2^{51}	–
SHA-256/224	256/224	512	64	32	–	–
SHA-512/384	512/384	1024	128	64	–	–
Snefru	128/256	512	512	128	$2^{88,5}$ [15]	–

3.6 Keyless hash function HMAC

HMAC (Hash-based Message Authentication Code) is a generic term for an algorithm that uses a keyless hash function and a cryptographic key to produce keyed hash function. This mechanism enables user “A” to validate that the data sent by user “B” are unchanged in transit. Without the key, anyone can change the data and recompute the message authentication code without user “A” cognizance.

The need for HMAC arose because keyed hash functions are derived from cryptographic algorithms and many countries have restricted their import/export of software implementing such algorithms. There is no restriction on software implementation of keyless hash function, because these functions cannot be used to hide the information. Hence HMAC builds on keyless hash function using cryptographic key to create a keyed hash function. Any cryptographic hash function may be used in the calculation of an HMAC. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key.

Def. 13 Let h be a keyless hash function that hashes data in blocks of b bytes to produce a hash l bytes long. Let k be a cryptographic key and assume that the length of the key k is no bigger than block b . Further, let k' be the key k padded with “0” to make a block b bytes and $ipad$ the sequence of bytes containing the bits “00110110” repeated b times and $opad$ similar sequence with bits “01011100”. Then HMAC- h function with key k for message m is

$$HMAC - h(k, m) = h(k' \oplus opad \parallel h(k' \oplus ipad \parallel m))$$

where

- $\oplus$ is function exclusive or,
- $\parallel$ is concatenation.

Analysis in [10] shows that the strength of HMAC depends on the strength of hash function h . Various HMAC functions are used in Internet security protocols.

3.7 Cipher Techniques – Block and Stream Ciphers

Using cryptosystem over a network deals with many problems because cryptographic systems are sensitive to environment. Using cipher without consideration of the environment in which it is to be used may not provide the security that the user expects. Let us discuss the following examples

- using a forward search to decipher a message enciphered in public key cryptosystem is discussed [67]. Let us assume that user “C” knows that user “A” is going to send to user “B” one of two messages – “BUY” or “SELL”. In this case there is only uncertainty in which of these two messages was sent. To solve the problem, user “C” enciphers both the messages with user “B” public key waiting for the messages from user “A” being sent. The message sent is then intercepted by user “C” and comparing to both ciphertext computed user “C” knows which message was sent. If the size of the set of plaintexts is reasonably small, we can encipher all possible messages and reveal coded plaintext by simple search for intercepted pattern in pre-prepared set of ciphertexts. This attack is for public key cryptosystem and does not reveal the private key, only the plaintext message;
- Denning points out certain cases where parts of ciphertext message can be deleted, replayed or reordered. If e.g. user “A” sends to user “B” the message “LIVE” and the message is enciphered by a public key, the block of the message can be intercepted by user “C” and rearranged. User “B” then receives completely different message “EVIL”. Even if user “A” digitally signed each part of the original message, user “B” cannot recognize it. The problem is that individual parts of the message are not bound to each other. So, because each part of the message is independent, there is no way to detect whether any part of message is deleted, replaced or added or when the parts are rearranged¹;
- sometimes, even if the message itself is undecipherable, it would be enough to use independence of the parts of the message to get the information related to the structure of enciphered message. The regularity arises because each part of the message is enciphered separately, so the same plaintext always produces the same ciphertext. This type of encipherment is called code book mode (CBM), because each part is effectively looked up in a list of plaintext/ciphertext pairs.

Despite using sophisticated cryptosystems and means of cryptosystem, the cipher produced provides inadequate security if not used carefully.

Some ciphers divide a message into a sequence of small chunks or blocks enciphering each block with the same key. The example of block cipher is DES enciphering system breaking the message into 64-bit blocks and using the same 56-bit key to encipher each block. Block cipher enciphers and deciphers multiple bits at once so the software implementation of the cipher is usually very fast. An error in transmission of one block does not affect other blocks because each block is enciphered independently. The weakness of the cipher lays in this independence – identical plaintext blocks using the same key produce identical ciphertext blocks. The analyst can search for data by determining what the encipherment of specific plaintext block is. To prevent this type of an attack some information on the block number is inserted into plaintext block before it is enciphered².

Cipher block chaining method does not require the extra information to be inserted and occupying the space in the block. Before the plaintext block is enciphered, the block is exclusive-ored with previous ciphertext block. In addition, this technique requires so called “initialization vector” to be exclusive-ored with first plaintext block. The enciphering technique could be described by indicating E_k as an encipherment algorithm with key k and initialization vector i as

$$\begin{aligned} c_0 &= E_k \cdot (m_0 \oplus i) \\ c_i &= E_k (m_i \oplus c_{i-1}) \quad \text{for } i \succ 1 \end{aligned} \tag{13}$$

Other approaches to the block enciphering involve multiple encryptions when using more than one key. Let us consider two keys k and k' enciphering message as $c = E_k \cdot (E_{k'}(m))$. It looks attractive because it has an effective key length of $2n$, whereas the keys to E are only of the length of n . The DES has two modes of triple encryption – one using sequence Encryption – Decryption – Encryption and one using the DES algorithm three times.

The example of stream cipher is a one-time pad (see page 11). Bit oriented ciphers implement a one-time pad cipher by using exclusive-or on each bit of the key with one bit of the message. The problem of the stream cipher is the generation of the key which will be random and infinitely long. This is usually bypassed by generating random bits infinitely from a source different from the message itself. The simplest cipher extracts

¹ We do not expect application of cryptographic checksum on the whole message or digital signing of whole message.

² The information inserted is usually last bits of previous block or block number.

bits from a register used as a key. The content of the respective register is changed on the basis of current content of the register.

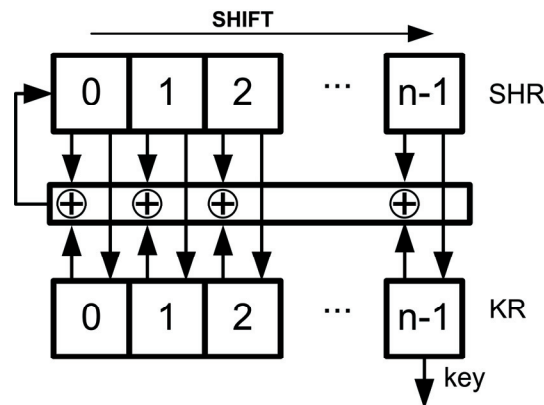


Fig. 12 Generation of a key with n-stage linear feedback shift register

Example 7:

Let us consider key generation with n-stage linear feedback shift register according to Fig. 12. Two n-bit registers create a shift and store mechanism where SHR register is a right shift register and KR register is used to store last key generated. When a new key has to be generated, the SHR register is shifted one bit to the right and output value of function $SHR_0 \cdot KR_0 \oplus SHR_1 \cdot KR_1 \oplus \dots \oplus SHR_{n-1} \cdot KR_{n-1}$ is inserted to the leftmost bit of SHR. Then the content of the SHR is gated to the KR replacing bit key in the bit n-1 of KR.

The method showed in the example above is an attempt to simulate a one-time pad by generating a long key sequence from little information. Naturally, if the key is shorter than the message, the breaking part of the ciphertext gives the cryptanalyst information on other parts of the ciphertext. In the case of the n-stage linear feedback shift register a known plaintext attack can reveal parts of the sequence. If the known plaintext is of the length $2n$, the sequence for n-stage register can be determined completely.

When using a non-linear feedback in the shift register architecture than instead of keeping the sequence in specific register, the key required is a specific function of the register content. Let us consider only the shift register of length n bits $SHR_0, SHR_1, \dots, SHR_n$. To generate a key bit, SHR is shifted one bit to the right and a new bit is set to an output value of the function $f(SHR_0, SHR_1, \dots, SHR_n)$, where f is any function of n inputs. Unlike n-stage linear feedback shift register, the non-linear variant is not commonly used, because there is no theory how to build such a register with long periods.

The problems of generation of the key for synchronous stream cipher and vulnerability of the linear feedback shift register are also solved by using a method called output feedback mode. In this case we should define the method by using E as an encipherment function, k as a cryptographic key and r as a register. To obtain a bit for the key, we compute $E_k(r)$ and put the output value into the register. The rightmost bit of the result is exclusive-or'ed with one bit of the message and the process is repeated until the whole message is enciphered. The key and the initial value in the register are key elements for this method. The substantial difference from non-linear feedback register method is that the register is never shifted.

Last but not least we should mention the method called counter method where instead of using a register it simply uses a counter that is incremented for every encipherment. The initial value of the counter is a part of the key and by setting the value to the counter at the start of enciphering a user can generate i -th bit of the key without generating bits $0 \dots i-1$.

To generate a key for a stream cipher is not a simple problem having in mind that the user has to handle the key value, the initial value and enciphering as a multiple variables problem. The self-synchronous stream cipher solves the problem of existence of key and initial value by obtaining a key from message itself.

Example 8:

The following text shows the Vigenere cipher with key drawn from plaintext

key:	X	H	E	L	L	O	W	O	R	L
plaintext:	H	E	L	L	O	W	O	R	L	D
ciphertext:	E	L	P	W	Z	K	K	F	C	O

The only problem with this cipher is the selection of a key as a plaintext because any regularity in the plaintext shows up in ciphertext. An alternative is to use the ciphertext as a key stream. Any good cipher produces pseudorandom ciphertext, which could approximate a random one-time pad much better than original plaintext¹. Unfortunately even this type of an autokey cipher is weak and plaintext can be deduced from ciphertext.

Example 9:

Let us have a cipher from the example above but enciphered with key generated from ciphertext

key:	X	E	I	T	E	S	O	C	T	E
plaintext:	H	E	L	L	O	W	O	R	L	D
ciphertext:	E	I	T	E	S	O	C	T	E	H

To follow analyst process let us consider the first characters of the ciphertext “EIT...”. Evidently the letter “I” in ciphertext is a product of encryption of some letter by key “E”, the letter “T” in ciphertext is product of encryption of some letter by the key “I” etc. Decryption using Vigenere table yields letter “E”. Continuing in this fashion, an analyst can reconstruct whole plaintext except for the first character.

To find a solution which will not be so weak, let us go back to the use of a shift register constructing an autokey method called the cipher feedback mode. If E is an encipherment function, k a cryptographic key and r is a register then, to obtain a bit for the key, we should compute $E_k(r)$. It could be done according to Fig. 13 where rightmost bit of the result is exclusive-or’ed with the respective bit of the message. The resulting ciphertext is loaded into the leftmost bit of the shift register, which is then shifted one bit right accordingly. The advantage of a cipher feedback mode is the so called self-healed property. If a bit is corrupted during transmission of the ciphertext, next n bits will be deciphered incorrectly. But after receiving n uncorrupted bits, the shift register will be reinitialized to a proper value and the remainder of the ciphertext is deciphered properly.

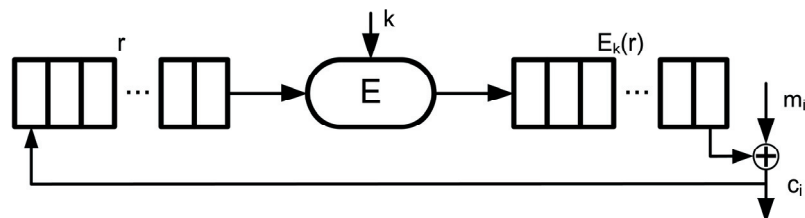


Fig. 13 Cipher feedback mode

3.8 Cryptography in Networks

The network consisting hosts and communication links is most vulnerable environment for the information transfer. Before we study relevant properties of the network, we have to describe architecture of the network using standard network models.

The best and most valuable model had been developed by the International Organization for Standardization (ISO) during its work on OSI² framework architecture. OSI had two major components: an abstract model of networking, called the Basic Reference Model, or Seven-Layer Model, and a set of specific protocols. The concept of a seven layer model was provided by the work of Charles Bachman³. Since that time, various

¹ In contrary to ciphertext, plaintext in any language has some rules which limit the sequences of characters to some limited set of permutation.

² Open Systems Interconnection

³ Charles William Bachman (1924), an American computer scientist. He is particularly known for his work in the area of databases.

aspects of OSI design evolved from experiences with the ARPANET, the fledgling Internet etc. The new design was documented in ISO 7498 and its various addenda.

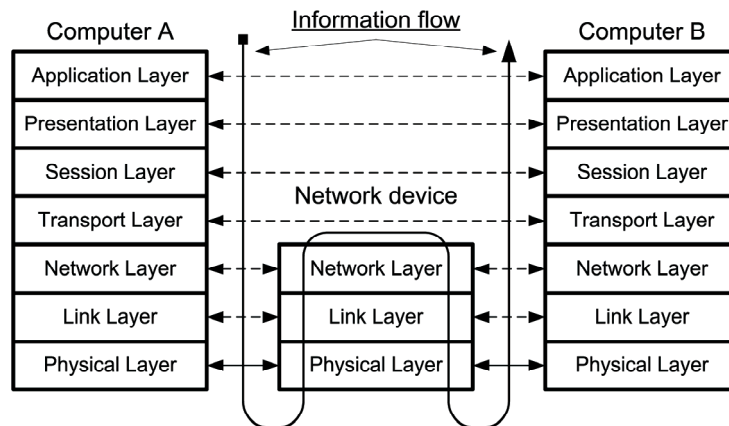


Fig. 14 Basic ISO/OSI seven layer architecture

In this model, shown in Fig. 14, a networking system was divided into layers. Within each layer, one or more entities implement its functionality and each entity interacts directly only with the neighbor layers providing facilities for use by the surrounding layers. The dashed lines in Fig. 14 indicate peer to peer communication of appropriate layers using internal entities belonging to the particular layer only. According to information flow shown in Fig. 14 e.g. Session Layer in Computer A starts transmission of information by invoking Transport Layer routines on the Computer A, falling down to the Network Layer and Link Layer, where Link Layer actually puts bits into Physical Layer. The role of Physical Layer is to transfer bits via medium to the next “hop”, either network device or another host computer, where information rises up to Link Layer, Network Layer etc. finally reaching the appropriate application.

We have seen that communication is based on the information exchange where certain rules have to be adopted. Such a set of rules is called a protocol, or communication protocol and they have to be accepted by all “node” on the way of the information flow

Def. 14 Let hosts $C_0, \dots, C_n$ be such hosts that C_i and C_{i+1} , where $0 \leq i < n$, are directly connected. A communication protocol where C_0 and C_n are endpoints is called **end-to-end communication protocol** while communication protocol where C_j and C_{j+1} are endpoints is called **link protocol**.

The main difference between the end-to-end protocol and link protocol is that the intermediate host plays no part in the end-to-end protocol other than forwarding messages. According to these differentiations one should recognize different levels of message security treatment using cryptographic methods.

In the end-to-end encryption each host shares a cryptographic key with each destination¹. The key can be selected on a per-host or per-host-pair basis. During transmission the sending host encrypts the message and forwards the message to the nearest intermediate host. The intermediate host forwards message, as it is, to the next intermediate host and the process continues until the destination of message is reached. Then the destination host deciphers the message, so the message remains enciphered throughout its journey and neither the attacker monitoring the network nor the attacker on the intermediate host can read the message. However, the message header containing the routing information cannot be enciphered, so the attacker can read the routing information used to forward the message.

Link encryption expects sharing the cryptographic key among pairs of neighboring hosts – each host shares a cryptographic key with its neighbor². The keys may be set on a per-host basis or on a per-host-pair basis, similarly to the end-to-end protocol. The message is deciphered at each intermediate host, re-enciphered for the next hop and forwarded. Attackers, monitoring the network will not be able to read the message but the attacker at the intermediate host will be able to do so.

¹ If encryption is based on public key cryptography the host can obtain the necessary public key of each destination from respective authority.

² Link encryption base on public key is rare because of key chaining - each host has to have its neighbor public key.

Example 10:

Consider a network of four hosts *A*, *B*, *C* and *D*. Each host is directly connected to other three. With keys distributed on per-host basis, each host has its own key, making four keys in all. Each host has the keys for other three as well as its own, so all hosts use the same key to communicate to particular other host – e.g. all hosts have the same key to communicate with host *A*. When keys are distributed on the per-host-pair basis, each host has one key per possible connection, making six keys in all. Unlike the per-host situation each host uses different key to communicate with e.g. host *A*.

The difference in encryption between the end-to-end and link protocols leads to affect a cryptanalysis. A cryptanalyst can deduce information not only from the content of the message but from the sender and recipient identity¹.

Example 11:

If the messages between *telnet* client and server are enciphered, the encipherment and decipherment happens only on client and server side [71]. The protocol uses the end-to-end encryption.

The *PPP Encryption Control Protocol* enciphers messages between intermediate nodes [50]. When a host gets the message, it decipheres the message, determines which neighbor to send it to, re-enciphers the message using the key appropriate to the neighbor and sends it to that neighbor. In this case the link encryption is used.

Several widely used Internet protocols illustrate the use of the end-to-end encryption and link encryption protocol. The electronic mail is a typical example of a chain of servers and possible use of cryptography. Two protocols are used – PEM² and PGP³.

In 1985 the Internet Research Task Force on Privacy began a study of problem of eavesdropping or modification of the message during its journey through the network. The goal of the study was to develop such an electronic mail protocol that would provide confidentiality, origin authentication, data integrity and non-repudiation of origin. Similar common goals are peculiar to other protocol like security transport layer protocol SSL⁴ or different mechanism of network layer security IPsec⁵.

The communication security could be dispersed in several layers, depending on the application requisite. If security services are focused on the particular application, then the application layer security would be appropriate and the end-to-end cryptographic protocol serves as a sufficient solution. If more generic security services are needed, lower layer security protocols can supply security services to multiple applications and can do so whether or not the application has its own mechanism for security services. These services are appropriate when intermediate hosts are not trusted, when the end hosts support the transport protocol, and when the application uses the connection-oriented protocol.

Network layer mechanisms such as IPsec may provide security services on either an end-to-end or a link basis. They are appropriate when securing connectionless channels or when the infrastructure supports the network layer security mechanism. Considering authentication services, we have to state that the security at transport layer like SSL doesn't authenticate the message to the recipient, it merely authenticates the transport connection.

If we use cryptosystem without considering the protocols directing its use, the security services that the cryptosystem is to provide can be deficient. Pre-computation attacks, assumption about messages sizes and statistical attacks can all compromise messages. Stream and block ciphers have different orientations that affect solutions to these problems. Stream ciphers emulate a one-time pad either through an externally keyed source, such as an LFSR, which generates a stream key bits from an initial seed, or internally, such as autokey ciphers or through feedback modes. Block ciphers emulate "code books" in which a set of bits maps to different set of bits. Over a network, cryptographic protocols and cryptosystems are the basis for many security services,

¹ It is known, that over 50% of information necessary for police investigation or military intelligence is identity of communicating parties. E.g. during the Allied invasion of Normandy in World War II the Germans deducted which vessels were commander ships by observing frequency of sending and receiving messages.

² PEM – **P**rivacy-enhanced **E**lectronic **M**ail

³ PGP – **P**retty **G**ood **P**rivacy

⁴ SSL – **S**ecure **S**ocket **L**ayer

⁵ IPsec – **I**P **S**ecurity

including confidentiality, authentication, integrity and non-repudiation. These services can be provided at different layers, depending on the assumption of network needs and expectation of users.

4 Attack analysis

The attack analysis could be done by applying two different models. Based on the social position of an attacker and its motivation we can create the first model of an attack tree, where the attack is driven by the intention of the attacker and its benefit. This kind of threat analysis has a weakness because unintended threats caused by a user, equipment accidents or natural effects are not taken into consideration. Nevertheless, such a weakness is not considered from the security point of view anyway, it belongs more to safety or reliability studies (see chapter 1). To cover the full issue, we should move to the study based on an asset threat analysis, which is usually accompanying the first model mentioned. As a matter of fact we can simplify this approach by introducing technological or sociological methods used to threaten a particular asset and by that create full attack analysis from the security point of view.

The attack tree methodology was introduced by Bruce Schneier [63] and provides a formal, methodical way of describing the security of systems, based on various attacks. The attack in the methodology is defined according to Def. 15.

Def. 15 *A threat exists only if an attacker has a benefit of the attack. Threats without any benefit for an attacker are no threats. Attack, as a result of execution of thread against a system, is represented in a tree structure as the root node, ways of achieving that goal as leaf nodes*

One can object to the definition above that it would be attacks executed just for fun, but then the fun is the attackers benefit. The attacker in the model is characterized primarily by its motivation, which defines the type of an attack performed and exploitations of the outcomes of those attacks. Formally we can distinguish among the following attacker types – User, Service Provider, Service Charger, Hacker, Cyber Activist, Communication Provider, Enterprise, Government and Foreign Power. It is obvious that the attacks where different classes of attackers are involved will overlap and a single attack may be attempted by several classes of attackers with different motivations. Another model of Telematic System, more closely describing elements of the system which could be involved in the attack, is in Fig. 15.

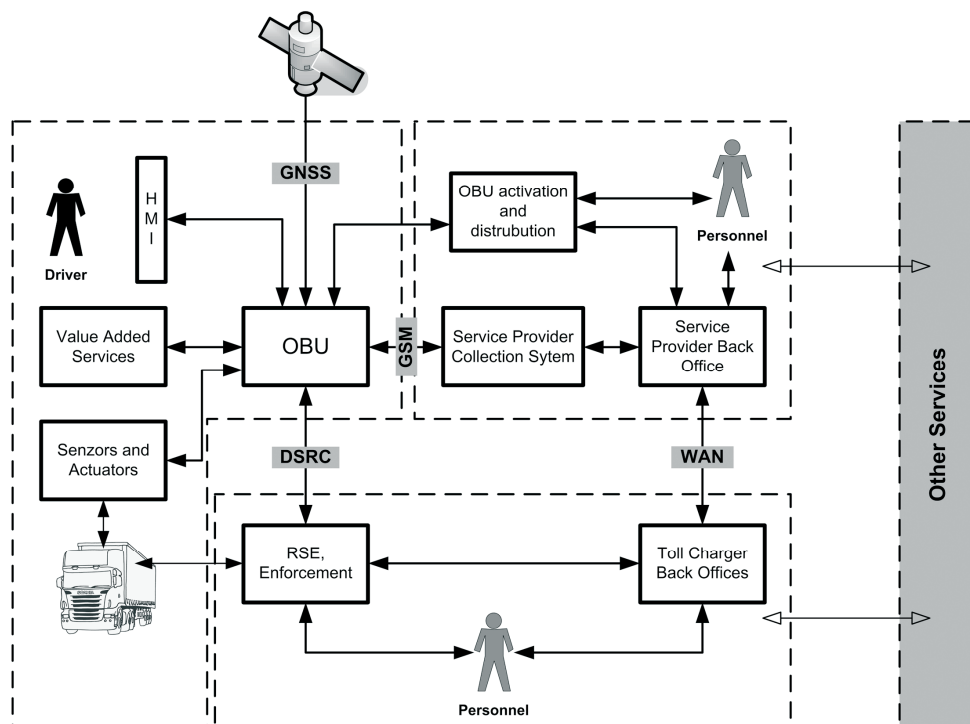


Fig. 15 Overview of EFC architecture

However even the arrangement of components in the system is largely irrelevant to the attack tree approach, since it is focused on the external elements of an attack, it provides a common decomposition of the system. Also an enumeration of the externally visible attack surfaces makes obvious, that some attacks are visible to certain attackers and not to the others, some of them could be accessed by anyone.

The interfaces and therefore most likely attack points are:

- OBU vehicle interface allowing connections to the vehicle as a connection to the power supply, CAN bus, tachograph signals, etc.,
- OBU data interfaces for value added services
- OBU tampering sensors,
- GNSS interface as a specific input of the localization information,
- OBU DSRC interface or OBU roadside equipment interface
- OBU cellular network interface as specific interface provided for communication of OBU data to central system, in the case, when OBU communicates to the Service Provider proxy server and the proxy communicates to Service Provider interface then these interfaces have to be dealt with separately from the security point of view (see the “Service Provider to Service Charger connection” below),
- OBU user interface, OBU personalization and maintenance interface
- Service Provider to Service Charger back office WAN connection,
- Road Side Equipment (RSE) interface to Service Charger back office or RSE interfaces itself, e.g. RSE compliance check interface for license number plate recognition (ANPR) subsystem,
- Service Charger personnel HMI and access to equipment,
- Service Provider personnel HMI and access to equipment and
- OBU distribution to Service Provider back office communication.

We also could speculate on delivery of equipment, e.g. OBU, and service provision, e.g. communication services, by suppliers and subcontractors from the security point of view. This is actually not a real interface, but attacks to be considered may be performed during equipment development, equipment manufacturing, service implementation or service operation.

4.1 Attacks by a User

The User is usually understood as a person who is using telematic services and liable for such services. It could be a physical person, a company or another legal entity. The User class includes e.g. drivers, truck owners or police. Unlike Activist attackers, the objective of the User is not publicity. The primary goal of the User is to avoid paying for services. The effect of the attack is twofold

- it represents a loss of income for the entity that is collecting payment for services, usually Telematic Service Charger
- if it becomes a wide-spread practice it undermines the belief that the telematic system is correct and fair.

To execute such an attack the user has to manipulate the system to not register usage of the service. There are several possibilities to conduct such an action.

4.1.1 Attacks on Sensors and OBU Input Data

The data used by OBU are sensed by a sensor and communicated to OBU for further processing. The sensor is an input to the OBU which can be used for **manipulating the input**. Typically it should be effective for usage sensors relevant in system where the service needs to be continually recorded, e.g. such as in GNSS-based systems, and it involves spoofing the signal that goes into the sensor.

Jamming the RF sensor is a specific case of attack described above when the input to the sensor is overdosed by an arbitrary signal. This type of attack is typical for GNSS road usage sensor which could be jammed e.g. with a portable device. Similar to jamming is **blinding the sensor**, when no measured entity is accessible to the sensor. This kind of attack is easily performed for telematic service which is dependent on the sensor data e.g. toll services using GNSS unit or a DSRC transponder which could be blinded by covering the antenna. These attacks do not require any modifications to the OBU and the method of manipulation is not specific to telematic services only, but it could happen as a part of attack against a moving vehicle itself.

When the attacker has an access to the sensor it can **manipulate the service sensors**, for example replacing them or filtering their output, to generate data that result in distorted information. This kind of attack is usually visible when an on-site inspection is done by an independent authority. In all cases the Service Charger or the Service Provider should be able to determine if a Service Declaration is based on correct and complete data or if factual service usage is represented by a corresponding set of Service Declarations.

4.1.2 Attacks on OBU itself

The attack of this class can be achieved by brutal force or by manipulating OBU itself. One of the soft attacks is **muting the OBU** when the OBU communication channel is separated from the service usage sensor, so the communication signal might be temporarily or permanently blocked. Another expected attack uses **manipulating the service data collection software**, when the software calculating the service usage on the sensor inputs is altered in such a way that a lower service usage will be resulting, stored and transmitted to the Service Provider back office. This attack is possible in autonomous systems only.

A simple attack by **disconnecting the OBU power supply** is another attack from the user, which could happen very often. That can be done permanently or only temporarily, e.g. insert a switch in the power supply. Much brutal attack will be **removing or destroying the OBU**, which is the one of the simplest yet most effective attacks performed by a user. Removal could be permanent or temporal. Unless some counter measures are embedded to the OBU, the OBU becomes “invisible” for the system in this case.

In all cases mentioned above when usage of OBU in a vehicle is obligatory and telematic service is dependent on the class of vehicle e.g. toll service, the Service Provider or Service Charger has to be able to determine if a vehicle is relevant to the service and it should be equipped with an operational OBU. Anyway, a driver should be notified of power drop and, if possible, OBU should have a short time internal backup to be able to detect movement without external power and report such an event¹. Also the Service Charger and the Service Provider shall be able to determine if the factual service usage is represented by a corresponding set of Service Declarations and based on correct and complete service usage data.

4.1.3 Attacks on OBU Data

The post collection attack remains in **manipulating the service usage data** after their collection is stored in the OBU. In the case where several items of service usage data remain under the control of the user before being reported to another party the User has the possibility to modify the service usage data taking the whole data set into account. Also **manipulating the usage data** when collected data are sent by the OBU would be attacked with a mechanism that allows detection of data and their modification or deletion when transmitted. The Service Charger and the Service Provider shall be able to determine, through a second source², if a Service Declaration is based on correct and complete Service usage data.

The higher level of attack remains in **manipulating the whole system** to lose service usage data, e.g. force an insufficient OBU data buffer by preventing the OBE from sending data back to the office as long as possible to produce insufficient memory that results in no longer collecting service usage or overwriting old service usage data. The Service Charger or Service provider should at least detect such an event or provide enough memory for data storage till next inspection. In this case an alternative procedure shall be available to retrieve service usage data from a muted OBU and also the driver shall be notified if the OBU is not working correctly e.g. out of memory event.

The attacker also can replace the data with **faked service parameters** or faked vehicle parameters if the price of service is dependent on these parameters. The User set vehicle parameters or service parameters to a

¹ And vice versa – OBU should report when comes back to ON condition.

² E.g. prior spot check observation, trusted hardware, completeness checks or collected data shall be stored in the OBU with a mechanism that allows detection of data modification and/or deletion of data.

value that does not reflect reality but that lowers the price of service. Also the User can set OBU identity parameters to a value that does not reflect reality but that lowers the service cost¹ or charges the toll to another user whose identity has been stolen. We recognize it as a faked OBU identity. The OBU should not allow the User to modify fixed vehicle parameters and limit the usage of manual vehicle parameters setting². Ideally, an OBU should have a mechanism to detect illegal parameter modification or tamper detection.

4.1.4 Specific User's Attacks

Under specific user's attack a high-end technology usage or regular criminal act could be understood. When a user uses an **OBU simulator** to produce the required service usage declaration, it is an example of using high end technology when profit could be less than fraud equipment cost. The simulator prevents the OBU from sending the service usage data back to the office and, on behalf of the OBU, produces a fake data set that is sent instead. Some mechanism on the Service Charger or Service Provider site has to be able to determine if Service Declarations data are based on data originating from a legitimate OBU, e.g. comparison of visual information from enforcement cameras with actual position of a vehicle in the case of toll service.

A regular criminal act when the User **bribes** Service Charger or Service Provider employee to manipulate the User account to pay lower service cost, to avoid a penalty, etc. is another way and it belongs to regular police investigation because of violation of criminal law. The problem will be to find relevant digital evidence which will not be repudiated in the investigation process and also which is correct and complete. Extensive logging with following analysis by IT security department could be helpful.

4.1.5 Foiling the System

A secondary goal is to foil the system out of discontent with its design or plain existence. It usually happens in large scale when a new system is introduced or starts the operation. This secondary goal might cause the User to perform attacks that due to their costs are not justifiable from an economic perspective. The effect of the attack is twofold

- it represents a loss of income for the entity that is collecting the fee for telematic services,
- if it becomes a wide-spread practice it undermines the belief that the telematic system is correct and fair.

All the attacks described in the sections above might also be performed without the economic incentive but motivated by spite.

Also there should be another secondary effect of the attack when users are misusing the democratic institutions, as courts, placing proceedings for damages caused by telematic system. If e.g. tolling system, Service Provider or Service User, is prosecuted then the quality of digital evidence will be decisive. Because of a low level of experience of courts with high end technology crimes, it is possible that some cases will be lost. When enough mass media popularity of these cases is achieved then Service User or Service Provider could incur reasonable losses.

4.1.6 Protecting the User Own Privacy

One of the most important features of telematic system is a User's privacy. Because every telematic system is storing and transmitting private information on a User, this particular issue will be extremely sensitive to the public. A User might be dissatisfied with the privacy protection features of a mandatory telematic system causing User not to disclose data that is crucial for the function of the system. The effect of the attack could be

- a loss of income for the entity that is collecting the service fees,
- if it becomes a wide-spread practice it undermines the belief that the telematic system is correct and fair.

¹ E.g. set reduced tariff for disabled person, if such a possibility exists.

² Actually, e.g. in tolling system there are parameters set by driver and only the mechanism how to check validity of these parameters is by comparison of parameter set with vehicle registration record or when enforcement inspection is taking place.

All the attacks described in sections above might also be performed without any economic incentive but motivated by a concern for the User's own privacy.

4.2 Attacks by Service Provider

The Telematic Service Provider is a legal entity providing his customers with telematic services on one or more service domains for one or more classes of vehicles. When a service provider is unsatisfied with his profit or other performance of its activity, it may perform some actions disturbing system parameters, operation or trust.

4.2.1 Attacks to Increase Revenue from Customer or Overcharging Customer

If this should be considered as an attack, the way to increase revenue from the user must involve over-charging. That means a charging for services which is larger than what is actual service usage. The motivation is a short-term financial profit.

Service Provider could charge a customer for a service usage that has never taken place faking service use. It is possible when Service Provider calculates the fake charge based on the service context data and tariffs of a Service Charger without involving them. Another possibility is using incorrect service context data when the Service Provider uses faulty or faked service context data to inflate the service charged to the customer. To use such inflated data not communicated to the Service Charger while using the correct data in communication with the Service Charger, the Service Provider is able to keep the difference.

The overcharging of the Customer happens when the Service Provider charges the customer a higher amount than calculated by customer OBU or by the Service Charger based on the billing details. The Service Provider then changes the invoice data received from the Service Charger increasing the fee.

To avoid such a situation, the Service Charger could require auditing invoices sent to customers for service in its service domain. Also a customer should be able to check the correctness of an invoice.

4.2.2 Attacks to Profile a Customer

The Service Provider could perform profiling of customers for its own gain or could be pressurized by a repressive government or a criminal organization to collect and provide customer's profiles. The attack could be directed towards the whole customer group or to an individual customer. When the whole group is profiled it could be used e.g. to target commercial offerings to a suitable customer¹. But political or criminal motives are also possible. If a single customer is profiled, the motivations could also be of a personal nature like stalking of celebrities, jealous spouses etc.

When profiling a customer the Service Provider accesses and compiles information on the customer profiles based on collected vehicle position data or other vehicle parameters in a way that is not allowed according to law or contract. To avoid such Service Provider behavior, the Service Provider should have the obligation to publish procedures of collecting and processing customer's data. On a request the Service Provider should have an obligation to allow an audit of compliance with these procedures by responsible national authorities.

4.2.3 Attacks to Resale Data on Customers

The Service Provider could also get financial gain from reselling data on a customer in a way that is not allowed according to law or contract. To avoid such a case the Service Provider should have an obligation to publish procedures of collecting and processing customer data as mentioned above. On a request the Service Provider should have an obligation to allow an audit of compliance with these procedures by responsible national authorities. To that extent a Service Charger can demand checking of compliance procedures with data protection law².

The Service Provider, while performing his duty, collects customer's and vehicle's position data and probably some other data as required for service charging purposes. At the same time, without the permission of the customer, Service Provider can transmit this information "in real time" to third parties. The third party pays for such a stolen data either on black market or regularly. The attack is either performed by the Service Provider himself or by staff of the Service Provider without his knowledge. To avoid such a case the Service

¹ The combination with reselling of data about tolled customers, as described further, is possible.

² E.g. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Provider has to implement appropriate monitoring procedures for its processes and systems and keep a history of the monitoring activities - logs.

4.2.4 Attacks on Reduction in Payments to Toll Charger

The intention of Service Provider is to pay the Service Charger less than it is entitled to due to the service usage by a customer. The motivation is usually a short-term financial gain.

To perform such an attack, the Service Provider could modify the service usage data sent to the Service Charger that the service usage is deflated, e.g. slightly shifting the time values to put the service in cheaper time class, while using the correct data to charge the customer¹.

The Service Provider could also refrain from reporting a service usage to the Service Charger, while using the correct data to charge the customer. Then the difference between these two amounts is a profit for the Service Provider.

In certain set-ups the Service Provider will have the ability to interpret the service usage data in a way that inflates the service that is due to the Service Charger, while using the correct data to charge the use of service to the customer. It could happen e.g. in the case where the service usage is evaluated against the template stored in Service Provider system. Service Provider then should modify the comparison algorithm or template in a way that service usage sensor is intentionally misinterpreted and less expensive service is reported².

If the Service Provider is in control of computing the final fee or some data on which the final fee is computed, it could use faulty fee context data to deflate the fee to be paid to the Service Charger while to use the correct data which results in a higher fee in communication with the customer and thus he can keep the difference. Also the Service Provider which has been requested by a Service Charger to enrich determined charge data may manipulate them to reduce the final fee, while using the correct data to charge the customer.

To avoid such a behavior it should be obvious that service declarations sent from the Service Provider to the Service Charger must be based on trusted data. Trusted in this sense means confidentiality, authenticity, integrity and non-repudiation ensured by cryptographic procedures or other technical and organizational means³. The Service Charger should also have a possibility to check the correctness of the charge data delivered by Service Provider e.g. by using some monitoring procedures. As a matter of fact, it would be helpful if the Service Charger has a possibility to recalculate the fee based on the agreed fee declarations. At least the Service Charger should require auditing of invoices sent to customers for fees in a relevant domain.

Last but not least the Service Provider could gain if he can lower its costs for equipment, primarily OBU, that does not fulfill certifications agreed or that cannot deliver requested quality of service. In this case, contract between Service Provider and Service Charger should be based on Service Level Agreement, which specifies requested technical data of the equipment under penalty. The Service Charger must have a right to audit the technical specification of the OBU and installation procedure to check if requested parameters of OBU and installation are fulfilled.

4.3 Attacks by Service Charger

The Service Charger is a legal entity charging services provided for vehicles in its service domain. The motivation of attack from the side of a Service Charger may be targeted to reduce the complexity of its operations or to make charges against a Service Provider or User which are not appropriate and this way to increase revenue of the Service Charger. They may also attempt to resell or otherwise profit from the data collected from Service Providers or Users.

¹ This is extremely dangerous when such a service is provided for law enforcement agency, e.g. average vehicle speed measurement with following conclusion on violation of speed limit. Even slight time difference in the time synchronization of distant parts of the system could cause incorrect measurement resulting in unlawful fine to the driver.

² E.g. in the Electronic Toll Collection system based on GNSS navigation system, if the comparison of positional data against the map, so called map matching, is provided by Toll Service Provider system, the Service provider could misinterpret the GNSS data from OBU and charge less expensive road usage.

³ E.g. independent second data sources for comparison of data or random evaluation of data by independent party.

4.3.1 Attacks to Increase Revenue

The malicious intention of a Service Charger might be to increase the revenue perceived from Service Providers or User for the usage of the services by their users. We can find several classes of an attack from Service Charger's side.

4.3.1.1 Attacks on Charge Data

During this attack Service Charger modifies the charge data acquired by itself, e.g. from his own road side equipment or from Service Provider's system, and reports them as billing details. The Service Charger can also insert faked charge data as acquired by Service Charger and report them as billing details. Another method allows a Service Charger to replay genuine charge data acquired by Service Charger and report them as additional billing details. The billing details presented by the Service Charger must be based on trusted data, so the data flowing through the system have to fulfill requirement on confidentiality, authenticity, integrity and non-repudiation achieved by cryptographic procedures or other technical and organizational measures.

4.3.1.2 Attacks on Billing Details

In this case the Service Charger modifies the billing details acquired and reported by the Service Provider and reports the aggregated value back to the Service Provider. The Service Charger can also insert faked billing details in the list of billing details acquired and reported by the Service Provider and report the aggregated value back to the Service Provider. To avoid this, the calculation of amounts in the billing details must be verifiable by Service Provider.

4.3.1.3 Data Repudiation Attacks

To perform data repudiation attack, the Service Charger has to repudiate illegally the correctness of billing details acquired through the Service Provider. The Service Charger could repudiate the origin or the update to new version of the service context data claiming payment for users according to different service context data. Also the Toll Charger can repudiate the reception of the exception list claiming payment for users who were on the list at the time of acquisition of the charging data by its.

Because a Service Charger can repudiate billing details regularly while communicating with Service Provider via trusted billing details, it needs to provide a reason for repudiation. Also a Service Charger must provide proof that the repudiation is legal or correct.

4.3.2 Reselling the Data and Specific Information

Reselling data or specific information to the third party is in principle a criminal act. But because the Service Charger manages a large database of users and user's related data, the temptation of employees will be high. Also some political issues or pressure from organized crime community could motivate high executives of Service Charger.

The Toll Charger could sell confidential and sensitive user data to other commercial parties operating data mining systems, for example to insurance companies, advertising industry or to governmental agency which are dealing with anti-terrorism. Also there should be an interest for the data from other state governments, usually from states surrounding the Service Charger domain or states having a specific interest in the territory.

The collected user's and vehicle's performance data could be sold and transmitted to a third party, by the Service Charger or by its staff without knowledge of the Service Charger. The Service Charger can collect user and vehicle position data in bigger details than it is required for charging purposes without the permission of the user. This data could be sold and transmitted in real time to third parties for specific data mining and statistics. The third party can commercialize the data mined and distribute them to interested parties.

4.4 Attacks by Hacker

A hacker is usually defined as an attacker who is attempting to penetrate the system without direct financial motivation, who is characterized by capable intellect, high tenacity and a desire to demonstrate relatively publicly the results of his efforts. This class of attackers may find the results of their actions exploited for commercial or criminal benefit by attackers of other classes. Their effects cannot be considered benign but are

likely to be technically sophisticated and may be time consuming in implementation or finding countermeasures.

4.4.1 Demonstration of System Vulnerability

This class of attack falls into a typical hacker's fields of activities. It simply shows that the system is vulnerable, but the attack itself does not necessarily achieve a perceivable benefit for the attacker. The most often seen type of hacker's attack is an attempt to confuse the OBU by fake input signal from the vehicle and push OBU to accept it as valid. In this attack a signal, that is required for the operation of the system, is emulated or modified to modify its semantics. Typical sources of signals are CAN bus, tachometer or odometer.

Another possibility in electronic toll collection systems is to fake signal from GNSS which swamps the real one and gives a different position for the OBU. Similarly, the fake signal emulating DSRC gantry could cause a change of the state of DSRC OBU unit and to confuse toll collection system or invoke court cases against Service Provider or Service Charger later¹.

The power source of OBU would be a challengeable part of hacker's activities. The simple attack when excessive noise is inserted on power supply lines can induce erroneous system operation or instability, when system randomly restarts with corresponding data loss. The hacker's trick when removing OBU from the vehicle while maintaining PSU connections would be obsolete while hackers use such an approach in some other activities performed on mobile computing services. Maintaining the fake power supply unit avoids the anti-tamper circuitry in OBU being triggered and allows the device to be removed from the vehicle safely without any notification to Service Provider site.

4.4.2 Exhibitionism

The act of exhibitionism, the exposure of private parts of his or her body with a tendency toward an extravagant, is understood as a psychiatric diagnosis. We are not going to use this term in such a hard meaning, but more than less as an extravagant behavior that is intended to attract attention to oneself within its community. This kind of social behavior is often observed among young people seeking for attention in their social environment.

Hacker's behavior, which is in the principle non-malicious, would have these signs to a certain extent. This class of attack is characterized by innate cleverness or complexity resulting in some observable effect². Again, it does not necessarily have a malevolent intent or result, but may be exploited by others for commercial gain.

Reverse engineering of firmware in the roadside device or OBU with intention to re-flash the own version of firmware is one of typical attacks of this class. The new version of firmware can

- be equipped with back door, allowing a hidden access to the OBU data for the purpose of manipulation or further investigation of the device;
- allow manipulation, e.g. modifying the input signals received by the charging application with intention of miscalculation of result;
- be prepared for an output state manipulation. The modification could be used e.g. to show ridiculous messages on traffic sign or OBU display or to modify the information that is recorded in respect of a charge event.

Replacing or modification of the security element with a fake element could be used for modification of the data recorded by respective secure element. For the purpose of charge manipulation a hacker can extract private keys from the OBU and thus allow a OBU fake to act as a regular OBU or extract secret keys from the road side equipment thus to allow a fake road side equipment to act as regular road side equipment for the purpose of charge manipulation. Also, in both cases mentioned above, the fake road side equipment can be misused for

¹ The attacker can fake user input according to sensed external state, for example automatically update the class of a vehicle before an audit-check event takes place or provide false configuration data to the OBU. Also fake adjusting an OBU in DSRC system is possible so that it is inappropriately set, e.g. telling that it is in a passenger car rather than in a truck.

² This is important sign of hacker's attack. Other classes of attack targeted on financial or other profit are rather hidden, so potential profit lasts for longer period of time.

the purpose of extracting data from regular OBUs as well as a fake OBU acting as a communication peer to remove information from regular road side equipment.

When a hacker obtains an access to the OBU hardware it can invalidate or incapacitate component on the printed board of OBU electronic e.g. by using a JTAG interface to switch a component into a testing mode (if there is any). Having full access, the hacker can provide additional service which interferes with the regular service application. When OBU supports secondary applications it can provide a secondary application which prevents the OBU from operating correctly by using most of system resources as memory, CPU etc., compromising input signals or output state reporting.

4.4.3 Research Attacks

A hacker is not only an attacker. One of his major goals is to gain detail knowledge of the system targeted. To improve the understanding of the system or to research its operation attacks leading to information leakage from the system or increasing, the level of knowledge outside of the implementer community¹ will be performed. For this purpose the hacker can intercept the communication between

- the OBU and the Service Provider back end,
- the OBU and Proxy or
- any two elements within the OBU.

When hacker has an access to OBU or any part of system, gained by impersonating maintenance or service crew member, it cannot observe the communication between any two components on the printed circuit board only and e.g. modify its configuration, but it can also clone an existing OBU and its private key on original OBU onto cloned hardware or design and build a fake OBU which is not easily detectable by roadside equipment or enforcement equipment. Removal of a component at regular OBU printed circuit board and its replacement with a similar component which offers a new or different functionality could be also achieved at this level of knowledge.

Also, intercepting DSRC interaction between roadside equipment and OBU would bring reasonable amount of knowledge to hacker community. To perform such attacks, a hacker should provide a fake OBU operating under its full supervision. These classes of attack also demonstrate cleverness and engineering capabilities of the hacker and finally may lead to financial profit by selling its faked OBU or the knowledge achieved by the hacker to a third party.

4.5 Attacks by Hactivist or Terrorist

Hactivism is the fusion of words “hacking” and “activism” – politics and technology. More specifically, hactivism is often described as a digital civil disobedience – hacking for a political cause or criminal activities to achieve its goals. A hactivist may be interested in abusing or manipulating the system in order to highlight or realize its political objective, even though that the objective may not have any relation to the system as such. To a hactivist, publicity is one of the main goals; therefore he is interested in large-scale disruptions of the systems that cannot be easily reconciled or hidden by authorities. The activist might not be interested in hiding its identity². The terrorist strokes are very often similar to hactivist actions, but with a larger impact on the system, society and people.

The cyberterrorism, the phenomenon of 21st century, is a product of interaction of classical terrorism, networks and dependency of a human society on information technology and communication infrastructure. One of basic motivations of terrorists, similar to hactivist, is to attract attention of media and to present their ideology this way. The large scale network of telematic services with connection to local infrastructures gives a lot of opportunities to cyberterrorist. Some terrorist organizations have their own specialized units developing and using infoware and other kind of malicious software to be implemented as a weapon against their enemy – hated part of the society. These specialized units are groups of highly skilled people operating in cyberspace, using electronic means to perform or support terrorist attack [32]. Attacks carried out by these special units are

¹ There is already some implementer knowledge which is never intended to be publicly known. This approach is often called “security by obscurity”.

² This behavior is similar to terrorist behavior where publicity is a primary part of effect of attack.

attacks of high quality difficult to distinguish from hackers attacks or attacks of military Information Operation Unit.

Despite groups formed by terrorists for special purposes there are individuals taking part in different cyberterrorist activities. These are formed by people sympathizing with the ideology of some political, religious, nationalistic or other movement and by taking part in the activity against the same enemy they express the sympathy for the particular movement. They usually work separately and the attacks are not too sophisticated. Also we cannot ignore the so called “thrill seekers”, who are individuals attracted by either real situation or conflict in the society. They are not led by any ideology, religion or any kind of the philosophical background and the major driver of thrill seekers is exhibitionism or internal satisfaction [31].

4.5.1 Social Destabilization through Manipulation of the Telematic System

Manipulation of telematic systems on a large scale might have destabilizing effects on the society as a whole. Hactivist groups as well as terrorist units may be intended to different size of attack motivated by anger or resentment against the political regime or way of living of one or more countries. The political, religious, nationalistic or other movement could be a source of hate, the driver of hactivist and terrorist movements.

Manipulation of telematic systems could have effects such as reducing the trust of users in the correct function of telematic systems or in extension of any high-tech system. Reducing trust of users in correct function of the system creates social tension, lack of trust in the telematic system management and by extension in any authority. Such social movement endangers the financial stability of enterprises, local or national governments and leads to reduction of revenues from telematic services offered. The terminal situation, when lack of funding disrupts the maintenance of infrastructure should bring a telematic system owner to bankrupt and to total end of telematic system operation.

One of the tools used by hactivist or terrorist would be a large-scale disruption of GNSS signal in tolling service or any service based on a localization of a vehicle. By jamming or different disruption of the GNSS signal in large areas, the OBU of a big number of users of system will stop working correctly. Also activists or terrorists may prevent the whole or parts of the charging system from operation by using denial of service or distributed denial of service method¹.

Breach of data integrity, data non-repudiation or its confidentiality or privacy will cause a large scale problem causing damage of trust to the system when becoming known in the public. Activists or terrorists may break into the system or into data communication between parts of the system and change the contents of messages including associated message authenticators. Also by breaking into the system they can get access to personal data of users. When the data are published and the attack becomes publicly known, there might be major loss of trust in the system in general public achieved.

The security issues of the technology are important while hactivist or terrorist are searching for methods of breaking into telematic system. Hidden manipulation of the internal data like exception list status or malicious handling a large population of OBU can cause OBU to malfunction subsequently causing inability to access the system or unjustified enforcement to users.

4.5.2 Raise in Profile of the Activists Cause

Activists or terrorists may try to manipulate the system for the sole purpose of drawing attention of the public. This will be often achieved by claiming responsibility for a successful attack afterwards even though the attack could be virtual, performed by other body or causing low or no damage to telematic system. In general there will not be very much difference in the attack methods employed, compared with the attacks described above in 4.5.1.

4.5.3 Direct Furthering of Activists Cause

Activists or terrorists may try to manipulate the system in order to direct further their cause. This might e.g. be a reduction in the number of total service events count in the case when activists or terrorists are motivated by green issues. A key factor here is influencing the behavior of any party in the system, but especially the users. One of the ways to achieve that is to reduce the trust of users in the system, such that they will be less inclined

¹ The DoS or DDoS principle remains in generation of large amount of random data targeted to overload system resources.

to use it. In general there will not be very much difference in the attack methods employed, compared with the attacks described above in 4.5.1.

4.5.4 Reduction in Credibility of the System

One of the activists' motivations may be the service charging environment itself, e.g. if it is opposed to the idea of telematic as such. To discredit the system in the eyes of users or politicians, it might try to end the use of existing telematic systems or to prevent establishing of new ones. In general there will not be very much difference in the attack methods employed, compared with the attacks described in 4.5.1.

4.6 Communication Provider Attacks

The communication provider is the entity providing the communications infrastructure for the operation of the telematic system. The different communication services of the system may be provided by several providers, e.g. cellular network operator, internet provider etc. Using one specific service may involve several Service Providers at the same time.

4.6.1 Change in Network Utilization

The communication provider is trying to optimize network utilization for the purpose of achieving higher remuneration from Service Providers or Service Chargers. In this intent it can deliberately corrupt the data flow leading to retransmission of packets and thus to an increased aggregate data flow.

On the contrary to this approach the communication provider may try to reduce the use of the network by flat rate communication user, what is usually a case of telematic systems having flat rate contracts for the whole fleet, to increase income from time or volume metered communication users. Also, by preventing data transfer from the OBU for an extended period of time, it is possible to make the OBU data buffer overflow and the data to be lost. Thus data are not being transferred over the network with a resulting decrease in network utilization.

The contracting parties involved in telematic system operation should have proper service levels agreement with communication providers. The contract should be specifically focused on agreed monitoring procedures in place that are able to detect any non-compliant behavior.

4.6.2 Collecting the Travel Behavior

One of the possible acts of the communication provider is to establish individual user tracking profiles selling them to interested third parties. The attack collects the user data e.g. vehicle position and next service requested using data communication interception. To extend the attack, communication provider can provide analysis the data communication traffic, i.e. the connection, location, duration and frequency of the communications, to generate the user profiles.

To prevent such a behavior contracting parties of communication providers should have proper privacy protection agreements in place.

4.7 Attacks by Enterprise

Under the attacker class "Enterprise" any kind of organizations with certain financial, technical and personnel resources should be understood. This class includes general commercial enterprises of either a legitimate or illegitimate nature using their resources to make profit while performing the attack against the telematic system.

4.7.1 Movement Tracking

To know where a vehicle at a certain time is or what trips a vehicle makes within a certain period of time could be important information for any kind of an enterprise. This might have several reasons, e.g.

- knowing the position of a vehicle or its freight of special value can e.g. help to organize and plan stealing of the vehicle;
- tracking an individual, in the case of the vehicle the driver of vehicle, would give information on the position of an individual for whatever reasons, e.g. compared the traveling salesman plan to his actual position;

- tracking the vehicle to discover business behavior of a competitor executive or fleet will give reasonable information to enterprise business intelligent unit to discover business activities of the competitor.

The main attack for criminal enterprises may be to get an access to data by bribing an employee to act like a 'spy'. The bribed employee may install a bypass data connection to allow an online access for the criminal enterprise. Less often, a qualified person hired by an enterprise can install and operate data interception device. This solution is more expensive but less vulnerable to disclosure to the authorities when intercepting device is in a passive mode.

Access control concept and a logging concept, security policy of the company and special contracts with important personnel could be used as countermeasures. To reduce the possibility of interception, the data sent via different communication interfaces must be trusted. That means confidentiality, authenticity, integrity and non-repudiation by cryptographic procedures or other technical and organizational measures should be used.

4.7.2 Creation and Distribution of Cloned Equipment

Some results of hacker's investigation could be used by a criminal enterprise, which clones OBUs and sells them to users. Cloning or faking an existing OBU and its credentials or accounts, which are trusted objects, should be a subject of selling the OBU to users allowing them knowingly to avoid paying for telematic services. To avoid such a criminal offense the trusted objects like cryptographic keys must be stored and used securely in the OBU. Also fraud detection measures should be implemented to detect cloned or faked OBUs.

4.7.3 Attack to Disable or Compromise System Encryption

An enterprise demonstrates the vulnerability of the system encryption to discredit a competitor's implementation. There are many methods how to attack encryption system and to use decrypted key to intercept data communication. During that process the data should be replaced, the certificates, hashes or other key information could be changed to disable data decryption or verification of signatures. One way how to get information on cryptographic procedures implementation is the exchange receiver certificate or encryption session key with a fake or a wrong OBU. A major role is given to disabling cryptographic procedures implementation, correct encryption or electronic signing of the data or just receiving encrypted information.

The countermeasures in this case remain in storing cryptographic keys securely in the OBU or roadside equipment or other mobile equipment. Also confidentiality, authenticity, integrity and non-repudiation by cryptographic procedures should be anchored into company security policy and technical or organizational measures should be taken.

4.7.4 Stealing Equipment

The simplest act of criminal enterprise is to steal OBUs, road side or other equipment either for analyzing and cloning or for reselling the equipment. Both actions can be done by stealing equipment from the stock of telematic system provider or dismounting equipment from premises.

The equipment could be designed in a way that it is hard to steal them¹ or set of measures has to be taken on the Service Provider or Service Charger side as remote monitoring, asset tracking etc.

4.7.5 Racketeering

A criminal enterprise could try to break into several parts of a telematic system to obtain sensitive data. The data can be used either to extort money from targeted individuals, or to extort money from the involved Service Provider or Service Charger by threatening to disclose this information about their clients. To get the data the enterprise should bribe Service Provider or Service Charger employee to intercept the data communication. Data interception could be done on the communication provider to Service Provider interface, Service Provider to Service Charger interface or on the open air interface².

¹ E.g. by self-deactivating or self-blocking feature.

² E.g. OBU GSM interface.

To avoid such a situation the Service Providers and Communications Providers systems should be designed in a way that the access to stored or processed data is only possible within the legal context of a respective country. Monitoring procedures shall be in place to detect any unauthorized access.

4.8 Attacks by Government

The sovereign entity within whose domain the Service Charger operates includes all government departments and governmental organizations, e.g. police and military forces, intelligence services, etc. The government is characterized by significant resources, technical and financial capability.

4.8.1 In Theatre Commercial Advantage

This class of attack gives a commercial advantage to companies involved in telematic services, e.g. Service Providers or OBE manufactures, or other business in the domain of the government. The main target is to collect information that provides an advantage to local companies. The information could cover

- collection of information about how particular OBU is used may be interesting for OBU manufacturer and Service Providers;
- tracking commercial vehicles to discover business behavior and relationships may give an advantage to local hauliers;
- tracking private vehicles to discover its commercial behavior and whereabouts may give an advantage to local companies

The government can obtain direct access to data through authorities' power or through direct contact with the state-owned Service Charger or Service Provider, which provides the data on request of the government after appropriate data mining.

The Service Chargers system should be designed in a way that the access to stored or processed data is only possible within the legal context of a respective country and monitoring procedures shall be in place to detect any unauthorized access.

4.8.2 Political Targeting of Individuals and Organizations

Governmental organizations are able to control movements or discrediting individuals or organizations based on their travelling behavior. This should be done by collecting travelling data of visited locations or travelled distance of individuals or members of organizations or more precisely collecting travelling data of their vehicles. The data should be collected by communication interception or by using an appropriate installation to obtain an identifier of the vehicle OBU. Data can also be read-out from the OBU through one of its interfaces – cellular network interface, user interface or maintenance-interface.

It is unavoidable that the government can decide to implement visual detection of vehicles including automatic number plate recognition. If such a telematic service is implemented as an independent system it is the responsibility of the telematic service provider. It can only prevent unauthorized direct short-range or long-range communication with the OBU, relying fully on automatic number plate recognition. The current EETS decision [2] and corresponding architecture do not allow direct access to the OBU by any other party than the Toll Service Provider¹. If a government forces Telematic Service Provider to implement such kind of access, a check of legal compliance within current legislation should be required.

4.8.3 Tracking of Individuals

This class of attacks allows the government tracking of individuals for several reasons. For example to catch criminals, supervise suspicious individuals, collect traffic information, etc. The tracking of users and vehicles is carried out by data collected by data communication interception.

Direct access to data can be obtained through authorities' power including detailed charge or location data obtained through direct contact with the state-owned Service Charger or Service Provider, which provides the data on request of the government. Also data can be obtained by communication interception on the

¹ It is called OBU/Proxy concept. The EETS decision mentioned is Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements known as Decision 2009/750/EC

communication provider to Service Provider interface, the Service Provider to Service Charger interface or direct interception of data on the open air interface.

The Toll Service Providers and Communications Providers systems should be designed in a way that the access to stored or processed data is only possible within the legal context of a respective country (lawful interception). Monitoring procedures shall be in place to detect any unauthorized access.

4.9 Attacks by Foreign Power

A foreign power is defined as a foreign sovereign entity with independent political, social or military objectives on the service operator domain. The foreign power is characterized by significant resources, both technical and financial.

4.9.1 Social Destabilization

Social destabilization is already covered under hacktivist and terrorist activities in chapter 4.5. The methods used are similar, maybe more sophisticated due to a better finance support of the activity and mechanisms already built into foreign power e.g. state structure.

4.9.2 Movement Tracking

The foreign power may be interested in tracking certain persons, e.g. political activists or government officials, in the service domain. A main attack avenue for foreign powers may be to get access to data by bribing an employee to act like a spy. A major reason why a foreign power can use this attack while e.g. activists cannot is that it potentially has a big amount of money and power at its discretion. In principle, all kinds of data can be collected, for example the movement and mileage data of targeted vehicles and user personal data.

The movement tracking even individual could not be accepted as jeopardy to the stability of the state, province or government administering the territory where telematic service is implemented creates a hidden threat when cumulated. E.g. knowing the details of traffic on the territory of adjacent state at normal conditions, the foreign government can control the traffic¹ on its own territory during oil crisis such a way, that the neighbor's oil reserve will be exhausted while its own oil reserve remains.

Another way of attacking the system to obtain the desired data is to hire hackers, using the money in its possession. Although these hackers then cease to be ethical hackers, many of the attacks listed above, especially those related to the interception of communication, will be still usable.

To avoid such a situation the Service Providers or Toll Chargers should implement procedures for vetting personnel and monitoring systems activities. A security policy should be in place for implementing appropriate security procedures. Even there is no direct measure against the possibility for hackers trying to access systems and data a general security policy and appropriate security measures should be implemented to reduce the risk of successful attacks.

4.9.3 Racketeering

A foreign power could try to break into several parts of a telematic system to obtain sensitive data or to take control over the system. It could use these data either to extort targeted individuals, or to extort the involved government by a threat to disclose information about their citizens on a large scale. This is very close to the intention of movement tracking described above.

Alternatively the foreign power could extort the government, Service Providers or Service Chargers by showing its control over some part of the telematic system and threatening to use this power in a way which is disadvantageous for the party involved. In contrast to extortion by a criminal enterprise, its object will not usually be money, but some form of collaboration with the foreign power's goal. However this does not change the methods used by the foreign power.

As an example we can mention the case of electronic system for toll collection which depends on a satellite system. If the foreign power in question is in control of the satellite system used by the telematic system in question, it might threaten to disable the use of the system for that particular system if it is generally possible. The jamming of the satellite signal on larger territory will be less effective and technologically difficult because

¹ The control could be achieved e.g. by setting higher toll fee or placing traffic signs such a way, that heavy vehicles will prefer to use neighbor country road network.

of nature of signal and antennas. The attacks used for achieving these goals will largely be the same as described in the sections above.

The Service Providers system should implement some backup procedures that enable a limited operation of the toll system even in the case of unavailable satellite positioning signals as a measure protecting the system and users from such a threat¹. Also the Service Providers system should implement monitoring procedures, probably in the OBU, to detect jamming of the satellite signal.

The Service Providers and Service Chargers should implement procedures for vetting personnel and monitoring systems activities. A security policy should be in place for implementing appropriate security procedures.

4.9.4 International Prestige

A foreign power could try to enhance its own internal prestige by showing it is able to disrupt large-scale telematic systems operated by other governments. Alternatively it could seek for diminishing the prestige of other governments by disrupting their telematic systems. In this respect, the foreign power comes very close to the motives of hackers described in section 4.4.

5 Asset based threat analysis

The threat analysis based on attack trees has one weakness – unintended threats resulting from user behavior and accidents caused by equipment failure or by natural cause e.g. climatic phenomenon are not covered. Therefore an asset based threat analysis done in parallel is recommended resulting in exhausting list of existing threats. In asset based threat analysis for every identified asset the possible threats will be listed with a description on possible damages. The threat analysis does not assume any existing or recommended countermeasure. Therefore an attack can exploit any imaginable vulnerability. One of the main targets of asset based threat analysis is the identification of realistic threats without a benefit for the threat agent, especially if the threat agent is no person or organization.

5.1 Threatened Assets

The threatened assets define objects subject to attacks in a telematic system which requires protection by certain countermeasures. The main types of threatened assets are

- information objects, usually described in standards or in implementation;
- software, such as OBU firmware and computer software;
- physical entities, e.g. OBU, road side equipment and back office equipment;
- services, e.g. data collection service, data communication service;
- privacy of service users and
- intangibles, such as service chargers and service providers reputation and image.

It has to be stated while security architecture covers all information on objects and interfaces, not all interfaces fully rely on technical implementations. Furthermore, technical standards are not available for every interface and most of the interface-related assets have been derived from the EFC architecture standard which describes information objects.

From the point of countermeasures the most important step is to describe common features of threats where we can use relation between threat and the agent, who is able to perform the threat. The relationship was widely covered in the Chapter 4, even we do not deal with additional causes arising from third party or force majeure. As a matter of fact, these two last mentioned reasons are out scope of security issue and should be specifically reflected in the safety analysis of the system even original cause of failure could be situated outside of the system. The good reason for such a conclusion could be found in analysis of the existence of attacker. In the case above, “the attacker” is the “force majeure” or third party, no one volitional to cause the failure of the

¹ This could be e.g. a manual booking system.

system. Because human is an integral part of the system, so failure of the system could be also caused by the non-volitional human action and as it, all this issues are more close to safety analysis than security study¹.

As far as we are concerned, the threatened assets remain the same – telematic system, only character of the thread could be different. Before we continue in specific asset analysis of telematic system, we should describe the basis of the threat taxonomy itself.

5.2 Taxonomy of Threats

It cannot be said there is some universal taxonomy of threats because their existence and meaning is changed according to environment where threatened process is in progress. Nevertheless, we have to accept some kind of taxonomy to be able to describe roles of security elements in the system and entities bound to the threatened process. On the highest level of abstraction we can recognize three groups of threats

- basic threats,
- activation threats,
- underlying threats.

5.2.1 The Basic Threats

The basic threats could be distinguished in four categories reflecting four aspect of the security of information system

- **leakage of information**, the case when secret or confidential information is disclosed to unauthorized subject or is revealed by the one,
- **violation of integrity** of the information which could be understood as breach of data consistency when new data could be created or existing data modified or deleted by unauthorized subject,
- **denial of service**, when the access to the information or to the system resources by legitimate users is intentionally blocked or disabled. As an example we can introduce well-known DoS attack, when illegitimate or void requests produce a high load on the network resource which consequently disables system services to regular authorized users²,
- **illegitimate usage**, when the network resource is used by unauthorized subject or by inadequate manner. As an example we can introduce system penetration and using commercial services without payment or on others account.

5.2.2 The Activation Threats

The activation threats importance is corroborated by their characteristic where implementation of activation threat leads to immediate formation of the basic threat. Consequently, security parameters of system are threatened. The term activation threat is deducted from their ability to activate other threats, not to become the threat itself. We can recognize two categories of activation threat further fragmented as

- penetration threats
 - **masquerading** – the case when one entity, the person or system, impersonates other entity. This kind of threat is one of the most common way of violation of security perimeter of the system, e.g. “login perimeter”, In this case unauthorized entity “convince” the security mechanism of its relevancy as another authorized entity using all privileges fictive authorized entity. The masquerading is very often and efficiently used by hackers,

¹ This is more legal aspect of the failure; if it has been caused intentionally and the attacker behaves volitionally else the failure was caused by unintentional behavior of the human. As a matter of fact, these two issues „safety“ and „security“ are often mixed and e.g. in [22] the theft of the device is counted as security aspect of the system not as a safety aspect.

² The DoS attack today is usually realized as DDoS (Distributed Denial of Service) attack which allows attacker to create higher load on the target by using many sources of attack in the network. At the same time, the origin of the attack is much better hidden than when classical simple DoS attack is used.

- **bypassing of control** – in this case the attacker misuses system or security weakness to obtain privileges of regular user,
- **violation of authorization** process remains in misusing of already authorized access to resource for unauthorized purpose. This kind of attack has to be conducted from inside of system by user, who already has an access to the system¹, so it should be said that in this case it is more personal failure than system malfunction,
- implantation threats
 - **Trojan horse** threat is historically the most common case of implantation threats, when system contains code or data invisible during regular operation. The piece of code or data affects security elements of the system when operation is started. As an example we can introduce a program supporting ordinary activities of user, e.g. text editor, but at the same time it allows to save the information created by the user into hidden part of the system. Then, Trojan horse can read this information and send it over to the attacker who implements the Trojan horse. There is a lot of free downloads on the internet, programs providing a simple services to the user but, at the same time they provide an information on the user activity to the third party,
 - **back-door** is a part of system allowing bypass security policy when specific data string is applied to the input of back-door program. The example could be login procedure where all common procedures of authorization are omitted for specific username.

Implantation threats are usually not used immediately, but they are woken up by implementer some time later, when they were hidden in the system for some time.

5.2.3 The underlying threats

When we analyze basic and activation threats in some system environment, we can identify a threat allowing implementation of several basic threats, e.g. if leakage of the information belongs to basic threat as shown above, then we can find several threats implementing the information leakage – link eavesdropping, analysis of communication traffic or employee indiscretion. Such a threat which is essential for implementation of several basic threats is called “underlying threat”. The relationship between basic threats and underlying threats is shown in figure Fig. 16.

¹ Such kind of users called „insiders“ create majority of security problems and they could be an important focus of the security manager when security policy of the company is designed.

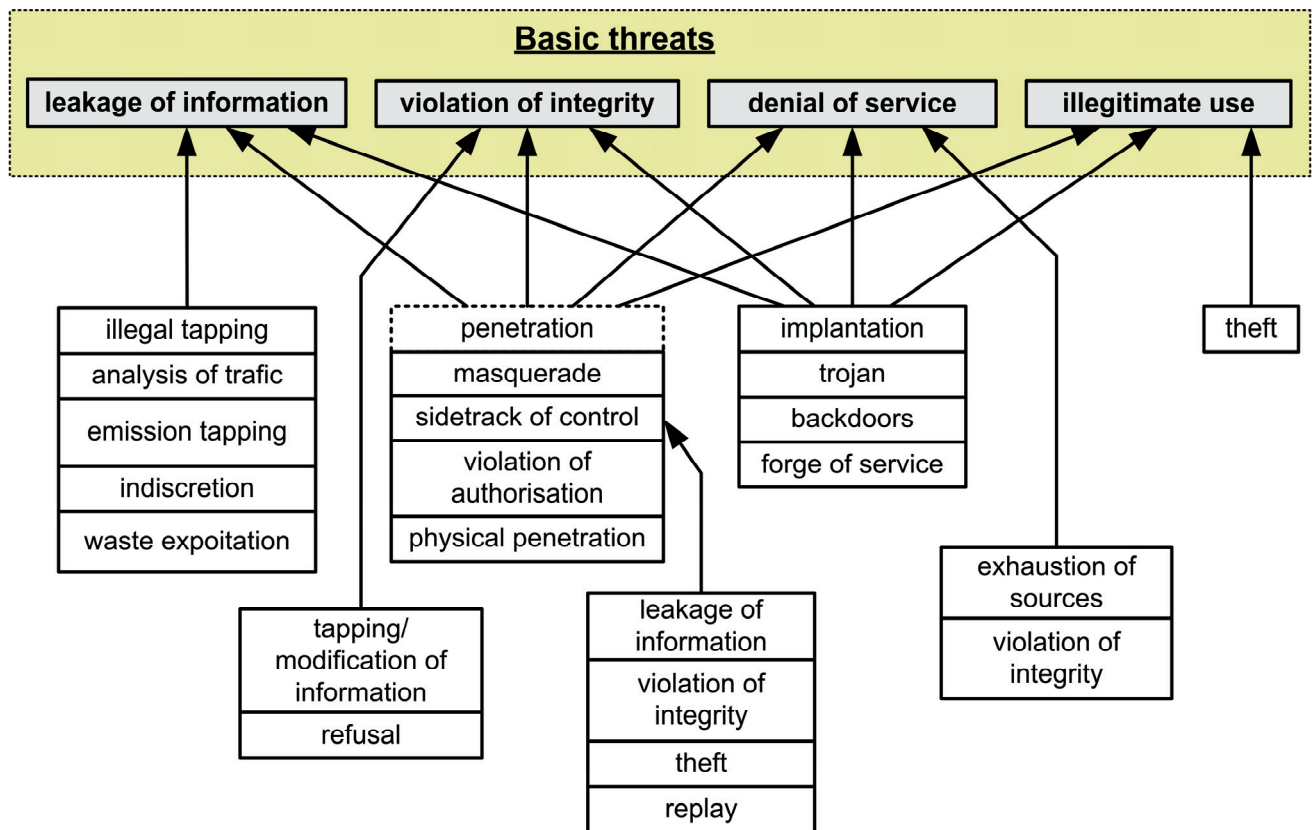


Fig. 16 The relationship of basic threats and underlying threats

The existence of such threats could be supported by statistic in [54] reflecting over 3000 of misuse of computer system. The most often found threats are, in top down list, violation of authorization, masquerading, bypass of control, Trojan horse, back-door and exploitation of garbage media.

Table 8 Typical threats

Threat	Description
Violation of authorization	Person authorized for using of resource for some purpose will use the resource for some other purpose (unauthorized).
Bypass of control	The attacker uses the security hole or vulnerability of the system.
Denial of Service	The attacker limits the legitimate access to the resources or information in the network.
Illegal monitoring	The information is acquired by non legitimate eavesdropping of the communication channel.
RF emission monitoring	The information is extracted from the electromagnetic emission of system elements, e.g monitors, when operated.
Illegitimate use	The resource is used by unauthorized person or in unauthorized manner.
Indiscretion	Authorized person discloses the information to unauthorized person either by incautiousness or for consideration.
Leakage of information	Acquiring of the information by unauthorized person or system
Violation of integrity	The breach of data consistency when new data are created or existing data are modified or deleted by unauthorized subject.
Modification of data during transmission	The data are modified by unauthorized subject during transmission.
Masquerading	One entity, the person or system, impersonate other entity.

Exploitation of garbage media	Information is obtained from magnetic or paper media found in garbage.
Physical penetration	The attacker gains the control over the system by physical penetration and presence at the installation site where system control elements can be directly accessed.
Replay	The illegally recorded copy of legitimate transaction is replayed by attacker with criminal or malicious intent.
Repudiation of activity	The party involved in mutual communication denies the communication act afterwards.
Exhausting of resources	The particular resource is intentionally overloaded such a way that regular service bound to the resource is impossible to use.
Service forgery	The forged subsystem or system element presenting itself as a regular part or functionality serves as an instrument to gain sensitive information.
Theft	A critical part of the system e.g. access card or sensitive information is stolen.
Analysis of traffic	Unauthorized person gains the sensitive information by monitoring communication traffic filtering its specific parts.
Back door	The feature or part of system is inserted into regular system with intention to be used later, evoked by specific information presented by attacker.
Trojan horse	The part of software installed contains hidden code which, when running, could threaten the regular user

Even Table 1 looks like an incomplete list of threats, all known ways of an attack have been covered, but not their methods. As an example, viruses or worms belong to the categories of “bypass of control” and “masquerading” and they are an implementation of such a combined form of attack only. On the other hand some of these attacks can request specific supporting information, e.g. masquerading expects either indiscretion or some other way of acquiring password.

5.3 Threats, Objects and Assets

The security view of the system uses different decomposition of the system as we have seen above. The taxonomy of threats had been described in Chapter 5.2 in common. Objects, generally said, are well defined parts of the telematic system, usually understood as information objects, described in standards or in implementation¹ documents. An example of information objects is in Table 9. All remaining entities could be generally covered as assets of the telematic system such as software, OBU firmware and computer software or physical entities like OBU’s, road side equipment or back office equipment. These assets are well defined by their position in the system and functionality. To complete the list of assets we have to add intangibles influenced by threats, like services provided by different parts of the system or privacy of service users, providers reputation etc. Even it is difficult to describe value of intangibles, they may play important role in the estimation of providers benefit or risk analysis.

Table 9 Typical threats

Information object	Description
Contract	Contract with the user including all parameters relevant for service, the way the service is handled and parameters of Service Level Agreement
Operational rules	Rules governing the telematic system, e.g., identifiers, Service Level Agreements, security rules etc.
Trust objects	Certificates, signatures etc.
OBU interrogation	OBU attribute list for compliance check

¹ As an example we could introduce the information objects as described in ISO 17573, i.e. the information objects in the EFC rules class.

Exception lists	To indicate that some contracts, users or services are no more supported
OBU status	Status of the OBU read from the device to check if defined parameters of operation are met or if specific services are requested.
Customization	Customization info specifying parameters out of default set up like communication language, specific exception etc., including updated software
Billing details	Refined charge report of the OBU based on provided services up to the level of details requested in the user bill including the payment claim
Financial objects	Objects exchanged to manage a selling/buying process or taxation process
User privacy	The right of the user to control or influence what information related to them may be collected and stored, by whom and to whom that information may be disclosed etc.

While security architecture covers all information objects and assets, it will be important to define external exposure of the object into its environment. This is done via object interfaces. Most of interfaces related to assets have been derived from the telematic system architecture standards which describes information objects¹. We can define matrix matching the interfaces and assets according to the system model in Fig. 15 where

- OBU interfaces which have to be covered in OBU threat analysis OBU tampering sensors
 - OBU user interface, HMI interface, also covering
 - OBU data interface(s) for value added services,
 - OBE vehicle interface like connections to the vehicle, e.g. power supply, CAN bus, tachograph signal, etc.
 - GNSS interface
- DSRC interface covers
 - OBU interrogation,
 - charging identification,
 - transfer charging information,
 - user identification and transit information etc.
- OBU personalization and maintenance interface, should be covered in OBU and Service Provider system analysis
- OBU cellular network interface, should be covered in OBU and Service Provider system analysis, comprising customization, OBU status, context data and charge data
- OBU proxy to Service Provider interface should be covered in OBU and Service Provider central system analysis comprising similar items like above – customization, OBU status, context data and charge data
- Service Provider to Service Charger back office WAN connection has to be covered in the Service Provider and Service Charger central system analysis comprise contractual conditions, trust objects, exception lists, context data and billing details,
- Road Side Interface to Service Charger back office is covered in the Service Charger central system and Road Side Equipment analysis,
- Road Side Equipment compliance check interface for license number plate recognition is a part of Road Side Equipment analysis,
- Service provider and Service Charger personnel HMI and access to equipment have to be covered in the provider's central system analysis,

¹ It must be mentioned, that not all interfaces fully rely on technical implementations. Furthermore, technical standards are not available for every interface.

- OBE distribution to Service Provider back office communication is part of Service Provider central system analysis.

Delivering of equipment (e.g. OBU) and service provision (e.g. communication services) by suppliers and subcontractors is not a real interface, but attacks to this part of the system may be performed during equipment development, equipment manufacturing, service implementation or service operation and have to be covered in the Service Provider and Service Charger system analysis.

Individual threats in asset based threat analysis will be realized by its actors. Possible actors are

- Data transmission failure, caused by accident or environmental incident,
- IT equipment failure, i.e. hardware or software failure caused by accident or environmental incident,
- Service user,
- Toll Service Provider as entity or a single employee,
- Toll Charger as entity or a single employee,
- Any entity responsible for performing interoperability management functions,
- Outsider, e.g. fun hacker or terrorist.

The following chapters deal with technologies and methods used to implement individual threats.

6 Technology of Wireless Attacks

The main role, when attack is performed, belongs to the technology or method implemented. Even the social engineering is having high impact on the security, the technology knowledge and virtuosity is necessary part of attack against the telematic system. With view of the basic decomposition of the system in figure Fig. 2 we can distinguish between two parts of the system – wired part and wireless part. While attack technology in wired part of the telematic system is “technologically” similar to the known internet attacks, wireless attacks are having their own specifics different from known e.g. WiFi attacks.

A great number of information systems is concerned about protection of transmitted data, but in the case of telematic system we have to consider additional objectives protected such as tracking the source or source manipulation. As in any other mission critical system it is important to minimize all threats to keep “security big triple” safe – the confidentiality, integrity and availability of data and resources. However, not all of these conditions have to be fulfilled on the same level, e.g. not all systems need the four nines¹ of availability or not all the transmitted information have to be “strictly confidential”. The risk analysis of the information assets or system as whole would create necessary decision rules for acceptable limits of individual security measures and, naturally, it also produces basic level for cost of the design and implementation.

6.1 Eavesdropping

The wireless part of the telematic system mostly communicates via radio channels and communication can be surreptitiously overheard. The possible distance, at which attacker can listen to the communication traffic, depends on the radiated power and the directionality of antennas used. The situation is showed in figure Fig. 17, which is an example of eavesdropping range in the case of DSRC electronic fee collection gantry.

¹ By term „four nines“ is meant value with four numbers „9“ in fractional part of the value, e.g. 99,9999%.

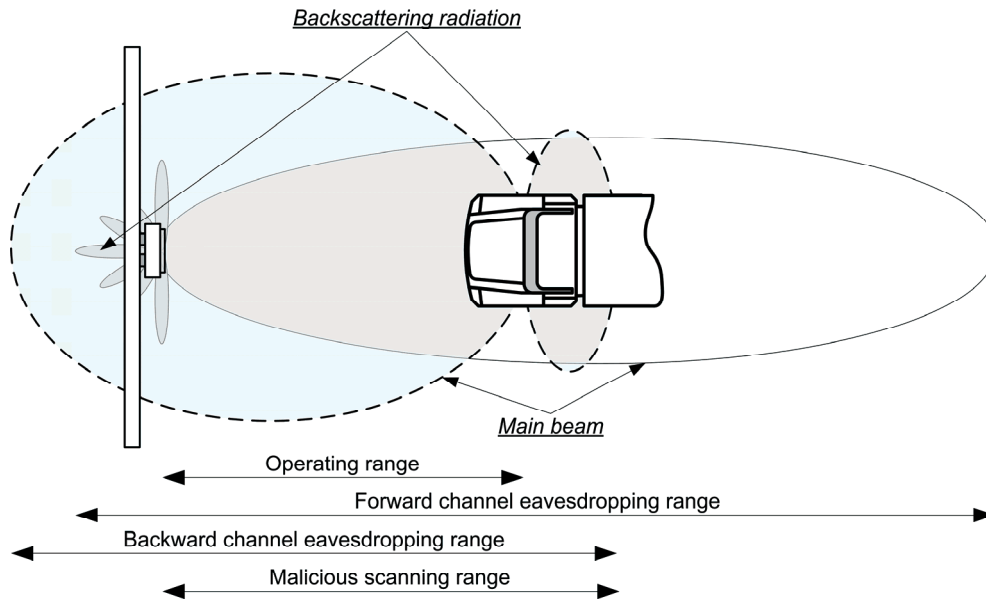


Fig. 17 Eavesdropping range classification

As one can observe the major drivers of the eavesdropping range is radiated power of transceiver and directional characteristic of antennas. The categorization is similar to the categorization of RFID communication channel, which as a matter of fact is the case [58].

The forward channel eavesdropping range is defined as transceiver to responder channel, where the transceiver transmits a strong signal, allowing long distance monitoring. In contrary, backward channel eavesdropping range, when much weaker signal is transmitted from responder to transceiver, can be monitored in close proximity of the responder only¹. The operating range is usually characterized as an intersection of main beams of radiation of transceiver and responder while malicious scanning range lies in the intersection of both radiation beams including backscattering pattern.

The eavesdropping is particularly problematic specifically from two reasons

- feasibility – it can be accomplished from long distance;
- purely passive attack, so the detection of such an attack is difficult.

Eavesdropping attack is a serious threat mainly when sensitive information is transmitted during transaction, like personal data or company sensitive data.

6.1.1 Security on Physical Layer of the System

The eavesdropping attack starts on physical layer, so physical-layer qualities play important role in the study of information-theoretic security in communication systems used in wireless communication which creates substantial part of intelligent transport system. For better understanding of the eavesdropper the fundamental security limits are introduced. This part is based on the study [18], where quasi-static fading channels and secret key agreement protocol are considered. In this case, to secure communications four steps of the protocol are studied

- establishing common randomness via an opportunistic transmission,
- performing message reconciliation,
- establishing a common key via privacy amplification and
- using of the key.

¹ In both cases we cover main radiation beam as well as the backscattering radiation.

The performance analysis has to be done in the case of perfect knowledge of the eavesdropper's channel as well as if this knowledge is imperfect or partial.

First of all, we have to separate the problems of security and reliability of communication as had been shown in introductory chapter at page 2. Very often exaggerated cryptographic security is typically handled at the upper layers of the protocol stack expecting that once the physical layer connection has been established the communication between the friendly parties will be error free. The fundamental notion of perfect secrecy was introduced by Shannon [65], who showed that an infinitely powerful attacker can extract precisely zero information from the encoded stream. This result is very pessimistic while reducing problem to secure key distribution. It was widely believed that perfect secrecy is not achievable in practical systems. However there exists the idea that extra security and especially information theoretic security¹ can be obtained by exploiting the physical layer. The secrecy capacity of the Gaussian wiretap channel representing the maximum transmission rate at which an eavesdropper is unable to decode any information, was characterized later in [45].

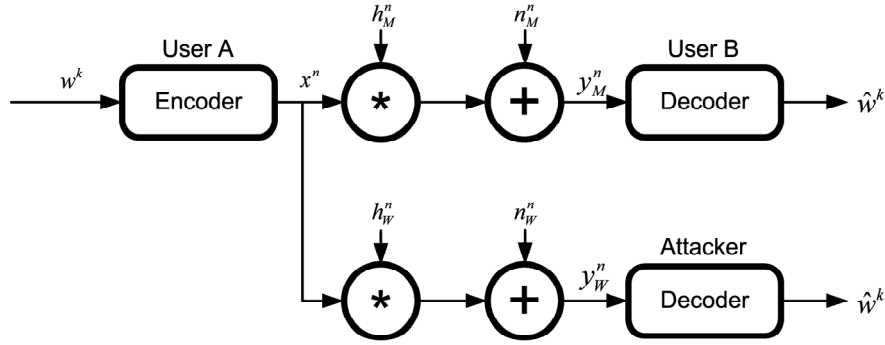


Fig. 18 System setup

All methods of secrecy are based on the key agreement protocol, which is the process for the legitimate partners to share common randomness. Let consider the system setup described in Fig. 18, where a legitimate user *A* wants to send secure messages *w* to another user *B*. Each *k*-bit message w_k is encoded into a *n*-bit codeword x_n before transmission. In this system the user *B* observes the output of a discrete-time Rayleigh fading channel, which is considered to be the main channel, given by

$$y_M(i) = h_M(i) \cdot x(i) + n_M(i) \quad (14)$$

where

$h_M(i)$ - denotes the main channel complex Gaussian fading coefficient with zero-mean and unit variance, and,

$n_M(i)$ - denotes a zero-mean circularly symmetric complex Gaussian noise.

Likewise, an attacker is capable of eavesdropping user *A* transmissions, and observes the output of an independent discrete-time Rayleigh fading channel, the wiretap channel, given by

$$y_w(i) = h_w(i) \cdot x(i) + n_w(i) \quad (15)$$

where

$h_w(i)$ - is the wiretap channel complex Gaussian fading coefficient with zero-mean and unit variance,

$n_w(i)$ - a zero-mean circularly symmetric complex Gaussian noise.

¹ Sometime this kind of security is called “perfect security”.

Both the main and the wiretap channels are assumed to be quasistatic fading channels, meaning that the fading coefficients are random but constant during the transmission of an entire codeword, and independent from one codeword to another. This setup is a good model for network applications with mobile units moving at slow speed, where the channel response varies slowly with time.

One of the main roles is played by average transmission power. In this case we denote average transmission power by P , and the average noise powers in both channels are respectively denoted by N_M and N_W . The instantaneous Signal-to-Noise Ratio (SNR) at user B receiver is therefore

$$\gamma_M = \frac{P|h_M|^2}{N_M} \quad (16)$$

and its average value is

$$\bar{\gamma}_M = \frac{PE[h_M^2]}{N_M} = \frac{P}{N_M} \quad (17)$$

Likewise, the instantaneous and average SNR at attacker receiver are respectively

$$\gamma_W = \frac{P|h_W|^2}{N_W} \quad \text{instantaneous Signal-to-Noise ratio} \quad (18)$$

$$\bar{\gamma}_W = \frac{PE[h_W^2]}{N_W} = \frac{P}{N_M} \quad \text{average Signal-to-Noise ratio}$$

Since the channel fading coefficients $\mathbf{h}$ are zero-mean complex Gaussian random variables, the instantaneous SNRs γ and $|\mathbf{h}|^2$ are exponentially distributed. The transmission rate between user A and B is

$$R = \frac{H(W^k)}{n} \quad (19)$$

with error probability

$$P_\varepsilon^k = P(W^k \neq \hat{W}^k) \quad (20)$$

where

$\hat{W}^k$ - denotes messages estimate for user B .

To provide users A and B with secure communication, the goal is not only to maximize the transmission rate, but also the attacker's equivocation rate

$$\Delta = \frac{H(W^k | Y_W^n)}{H(W^k)} \quad (21)$$

Then we should define secrecy capacity C_s of the system as the maximum transmission rate R at $\Delta = 1$. In the model discussed, for any pair of $(\mathbf{h}_M, \mathbf{h}_W)$ of fading realizations, the wiretap fading channel is strictly

equivalent to a complex valued wiretap Gaussian channel with main channel SNR equal to γ_M and wiretapper's channel SNR equal to γ_W . When the output of the wiretapper's channel is a degraded version of the output of the main channel, that is, attacker's SNR is lower than user "B" SNR, then the secrecy capacity of the real valued Gaussian wiretap channel is given by

$$C_s = C_M - C_W \quad (22)$$

where C_M is the capacity of the main channel and C_W denotes the capacity of the attacker's channel according to the following equation

$$C_M = \frac{\log_2(1 + \gamma_M)}{2} \quad C_W = \frac{\log_2(1 + \gamma_W)}{2} \quad (23)$$

The secrecy capacity of complex valued AWGN¹ channel follows straightforwardly from the previous result by noting that each use of the complex AWGN channel corresponds to two uses of the real-valued one, yielding

$$C_s = \begin{cases} \log_2(1 + \gamma_M) - \log_2(1 + \gamma_W) & \dots \text{ if } \gamma_M \succ \gamma_W \\ 0 & \dots \text{ if } \gamma_M \leq \gamma_W \end{cases} \quad (24)$$

This equation corresponds to the secrecy capacity of a single realization of a wiretap fading channel. In the case of wiretap quasistatic fading channel the secrecy capacity is a random variable, therefore the system in this case can be characterized either in terms of outage probability or in terms of average secrecy capacity².

All presumptions above have been based on perfect knowledge of eavesdropper's channel, but there is necessary to introduce an assumption, that user *A* does not know the eavesdropper's channel state perfectly. Nevertheless, we still assume that user *A* as well as user *B* has perfect CSI³ on the main channel. Also eavesdropper has perfect knowledge of the channel between user *A* and the eavesdropper.

Suppose now that user *A* sets the instantaneous information transmission rate R_s to be equal to the instantaneous secrecy capacity estimate $\hat{C}_s$ of the channel where

$$\hat{C}_s = \begin{cases} \hat{C}_M - \hat{C}_W & \dots \text{ if } \hat{C}_M \geq \hat{C}_W \\ 0 & \dots \text{ if } \hat{C}_M < \hat{C}_W \end{cases} \quad (25)$$

and, in the case of imperfect knowledge of the CSI, we had introduced instantaneous channel capacity estimate for each channel according to Eq. (26)

¹ AWGN - Additive White Gaussian Noise Channel

² It would be instructive to characterize the secrecy capacity of a quasi-static fading channel averaged over every possible main channel. It could be proven that the average secrecy capacity of a wiretap fading channel is either higher than or close to the secrecy capacity of a wiretap Gaussian channel.

³ CSI - Channel State Information.

$$\hat{C}_M = \frac{\log(1 + \hat{\gamma}_M)}{2} \quad \text{instantaneous main channel capacity estimate}$$

$$\hat{C}_W = \frac{\log(1 + \hat{\gamma}_W)}{2} \quad \text{instantaneous wiretap channel capacity estimate}$$
(26)

As could be proven from previous equations, the transmission in perfect secrecy is guaranteed if and only if Eq. (27) is valid. However, if none of these relations are valid, the transmission in perfect secrecy cannot be guaranteed.

$$\hat{C}_s \prec C_s \quad \text{or} \quad \hat{C}_W \succ C_W$$
(27)

As had been stated, the user can ensure perfect secrecy of the transmission only when instantaneous secrecy capacity estimate of the channel is lesser than secrecy capacity of the system as the maximum transmission rate or if instantaneous wiretap channel capacity estimate is higher than capacity of the attacker's channel.

6.2 Attack on Authentication

Verification of identity of one entity by another is known as an authentication. Some aspects of authentication, specifically role of cryptography in authentication process, had been described in chapter 3. Usually subjects act on behalf of some other, external entity. The identity of entity controls the action that its associated subjects may take. Hence, the subject must bind to the identity of that external entity.

Def. 16 *Authentication is the binding of an identity to a subject.*

As matter of fact, the external entity must provide some useful information to enable the system to confirm its identity. This information comes from one or more of the following

- something what only the entity knows (e.g. password or other secret information),
- something what only the entity has (e.g. identity card or badge),
- some exceptional characteristic belonging to the entity only (e.g. fingerprint),
- some place where only the entity can be (e.g. particular terminal).

The authentication process consists of obtaining the authentication information from entity, analyzing the obtained data and determining if it is associated with that entity. This means that the authenticating entity, the server or computer, must store some information about the entity to be authenticated. To store the entire data of the entity to be authenticated could be dangerous, so numerous mechanisms for managing the data stored are required. These requirements in an authentication system [16] could be represented by five major components

- (v) The set of **authentication information** as the set of specific information with which entities prove their identities.
- (vi) The set of **complementary information** as the set of information which is stored by system and used to validate authentication information.
- (vii) The set of **complementation functions** that generate the complementary information from authentication information.
- (viii) The set of **boolean authentication functions** that verify identity.
- (ix) The set of **selection functions** that enable an entity to create or alter the authentication and complementary information.

The authenticity of the claimed entity can only be ascertained for the instant of authentication exchange. To provide authenticity of the subsequent data exchanged, a secure means of communication has to be used, usually with some time variant parameters to prevent reply attack¹. Depending on the level of authentication, at least one authentication token has to be exchanged for unilateral authentication and at least two tokens from mutual authentication. Also, when challenge response protocol is used, additional token has to be exchanged to initiate the protocol.

6.2.1 Passwords and attack on passwords

The password is an example of very common authentication mechanism based on what people know: the user supplies password and computer verifies it. If the password is the one associated with the user that user's identity is authenticated. If not, the password is rejected and authentication process fails. So we can use Def. 17 could be used as definition of password.

Def. 17 *A password is information associated with an entity that confirms the entity's identity.*

The simplest password is some sequence of characters. In this case so called **password space** is narrowed to set of all possible or allowed sequences of characters. The set of complementary information can contain more or fewer elements than authentication information, depending on the nature of complementary information. The most often, the complementary information is stored in the computer as encrypted file or, by using one way hash function, the computed hash value of the original password is stored².

The goal of the authentication system is to ensure that entities are correctly identified. If one entity can guess another password, or find the sequence of characters generating the same hash (collision), then the attacker can impersonate the other. The authentication model has to provide a systematic way to analyze this problem. Using this approach we have to find such authentication information from whole set that for every complementation function we can find unique complementary information for relevant authentication information. Because one can determinate whether authentication information is associated with the entity only by computing its complementation function or by authenticating via authenticating function, we have two possible approaches for protecting password used simultaneously

- Hide enough information so that authentication information, complementation function or complementary information cannot be found.
- Prevent access to authentication functions.

Each of these approaches leads to different types of attacks and defenses. The most known attacks are dictionary attacks based on guessing of passwords. We can recognize two versions of dictionary attack

- attack type 1, when the complementary information and complementation function are known. The dictionary attack then takes each guess and computes value for each known complementation function for this guess. If the value corresponds to the complementary information for particular entity, then respective guess authenticates this entity using complementation function yielding this complementary information;
- attack type 2 used when either complementary information or complementation functions are not available. Then the attack is based on the plain guessing or, correctly said, on the using authentication function. If the guess goes through it means that authentication function results in true and the particular guess is valid password.

Password guessing requires either the set of complementation functions and complementary information or access to authentication function. In both approaches, the goal of the defender is to maximize time needed to guess password. We can estimate the time on the general basis of the Anderson's formula

¹ Usually some kinds of time stamp, sequence number or challenge message are used.

² The hash function has to be carefully designed with respect to the collision (the case when two different sequences of original produce the same hash value). Very simple algorithms used e.g. for storing a BIOS password are susceptible to collision.

$$P \geq \frac{T \cdot G}{N} \quad (28)$$

where

P – probability that attacker guesses the password in specified time,

T – number of time units during which guessing occurs,

G – number of guesses that can be tested in one time unit,

N – number of possible passwords.

For this formula several assumptions had been made. First, the time required to test individual password is constant and second, all passwords are equally likely to be selected. The first assumption is reasonable, because the algorithms used to validate passwords are fixed and either the algorithms are independent of password's length or variation is negligible. Second assumption is a function of the password selection mechanism. Usually the password selection is purely random. The random selection, based on pure math, yields some typical problems like overlooking human factors etc. Also, random sequence of letters and numerical characters is not easily memorable, so large set of unmemorable passwords could be abandoned, just because of human psychic.

The compromise between using random, unmemorable passwords is to use pronounceable passwords, which are based on unit of sound called **phoneme**. So we can construct such a string of vowels and consonant, which is pronounceable even not having any meaning¹. The advantage of pronounceable passwords is that fewer phonemes need to be used to reach some limit, so that the user must memorize “chunks” of characters instead of individual characters themselves.

6.2.2 Challenge-Response Method

The main disadvantage of passwords is that they are reusable. If attacker sees a password it can later replay the password. Because system cannot distinguish between password from attacker and password from legitimate user, it allows an access. There is an alternative – authenticate such a way that transmitted password changes each time. Then, if attacker replays the password, system will reject it. The challenge-response algorithm is good way to do it and it is similar to the IFF² technique used by military airplanes to identify allies and enemies.

Let's consider there will be a challenge response authentication system in which function F is the secret. The function F is called a “pass algorithm function”. To succeed with login the user has to know an algorithm. Haskett [29] suggests using this scheme in combination with a standard password scheme. When user supplies the reusable password, the second prompt is given, which could be the same as the standard system prompt to confuse the attacker? At this point, the user must enter some string based on the secret algorithm. For example, if algorithm is based on “every other letter of prompt beginning with second letter” and prompt sent after reusable password is “abcdefg” the response to the prompt will be “bdf”³.

Other method expecting ultimate form of password aging is one time password, when password is valid for exactly one use. In some sense, challenge response mechanism uses one time passwords. A one-time password could be defined as a password that is invalidated as soon it is used. The problem in any one-time password scheme is the generation of random password and synchronization of the system and user. This problem is usually solved by using a special time dependent password calculator or more simply by delivering of list of one-time passwords to the user.

Challenge response algorithms are naturally less vulnerable to dictionary attack than regular passwords. But, in general, if the attacker knows the challenge and the response, a dictionary attack proceeds as for a reusable password.

¹ E.g. “retogelan” or “lojutten” are memorable and pronounceable passwords with no meaning while similar construction not based on qualified phoneme structure like “xrfdsm” is not pronounceable.

² IFF – Identification – Friend or Foe.

³ This is actually most simple explanation, the real function would be more complex and difficult.

Example 12:

In the authentication system Kerberos an authentication server enciphers data consisting of name, a timestamp, some random data and a cryptographic key. An attacker does not see the original data sent to the server, but by knowing the form and contents of the data sent back, the attacker can try cryptographic keys until the known parts of the enciphered data decipher correctly. From this it can derive the cryptographic key to be used in future communications.

Many different techniques using challenge response technique had been designed. Beside already mentioned Kerberos [69] we can mention Bellovin and Merrit encrypted key exchange technique [12], Windows challenge/response protocol (NTLM) etc.

6.3 Skimming

The skimming is usually understood as a method of eavesdropping used with identification card based on RFID or other techniques (magnetic strip etc.). In the case of telematic system the skimming point toward the method of reading of the information stored in telematic equipment e.g. OBU without owner's knowledge or consent. Under such circumstances an unauthorized transmitter interacts with responder to obtain data targeted.

The adversary, not obeying regulation, may build its own transceiver with higher output power and higher sensitivity, which could be used to invoke response from responder independently of existing channels. Nevertheless, the knowledge necessary to invoke regular transaction can not be easily obtained and one of the sources of this knowledge is interception of regular transactions.

6.4 Hiding and jamming

The element of telematic technology when using electromagnetic waves could be insulated using the physical laws of propagation of electromagnetic signal. The easiest way of insulation uses Faraday cage, container made of conducting material. In this case propagation of electromagnetic signal is blocked or reasonably reduced at the cage boundary. If the cage is made of solid material, all frequencies are blocked at the edge while if conductive mesh is used, the attenuation of the signal is frequency dependent according to size of mesh eye.

Another method of suppression of information transfer through electromagnetic media misuses the interaction of electromagnetic waves in a different way – the jamming. Two methods of jamming can be used

- active jamming when radio channel is disturbed by other source of electromagnetic waves of the same frequency or spectrum. This disturbance may be achieved with an adversary device that actively broadcasts radio signal, so as to completely disrupt the radio channel. However in the most cases, the regulations on radio emissions are violated.
- passive jamming when each time a transceiver wants to interact with particular responder, the responder has to be singulated from the population of responders¹. A collision-avoidance protocol may be employed in this case and the adversary can conceal the presence of particular responder by simulating the full spectrum of possible responders, such a way hiding its presence;

The key point in successful active jamming is signal-to-noise ratio (SNR), which is defined as ratio of useful signal to all environmental signals commonly designated as “noise”.

¹ It is not true when transmitter and responder communicate on peer-to-peer basis.

$$SNR = \frac{P_{signal}}{P_{noise}} = \frac{\left(\frac{U_{signal}}{Z_{ant}}\right)^2}{\left(\frac{U_{noise}}{Z_{ant}}\right)^2} = \left(\frac{U_{signal}}{U_{noise}}\right)^2 \quad (29)$$

The “P” indicates average power and term “noise” simply represents the undesirable accidental fluctuation of electromagnetic spectrum collected by antenna. Jamming in this sense could be considered effective if $SNR < 1$. Depending on the character of jamming we can distinguish among

- **spot jamming** wherein the attacker directs all its transmitting power on single frequency that the target uses with the same modulation and enough power to override original signal. This kind of jamming is usually very effective, but since it jams a single frequency, each time it may be easily avoided by changing the target frequency;
- **sweep jamming** overcomes disadvantage of jamming method described above when jammers full power shifts rapidly from one frequency to another. While this method of jamming has the advantage of being able to jam broad frequency spectrum, even it doesn't affect them all at the same time and thus limits the effectiveness of this type of jamming. However in the packet data transmission environment it could cause considerable packet loss and retransmission making this kind of jamming effective;
- **barrage jamming** happens when a range of frequencies is transmitted at the same time. Its main advantage is that it is possible to jam multiple frequencies at once with enough power to decrease SNR of targeted receiver. Because limited spectrum density of transmitter output amplifier, as the range of jammed frequencies grows the output power per frequency is reduced proportionally;
- **deceptive jamming** simulates live traffic when signal emitted by the adversary is not random but resembles network traffic. Deceptive jamming is used when adversary does not want to reveal its existence. By flooding the telematic network with fake data it can deceive the network defensive mechanism and complete its task without leaving any traces. The deceptive jamming is very dangerous type of attack as it cannot be easily detected and has the potential to flood the network with useless data, occupies the available bandwidth used by legitimate users and could mislead the other part of system or its operator.

According to previous definitions of jamming we can also define a type of jammer. Actually we can introduce three types of jammers – constant jammer, deceptive jammer, random jammer and reactive jammer [76]. The constant jammer emits continuous radio signal any way – on one frequency, sweeping range of frequencies or using barrage method. The information emitted is totally random it does not follow any underlying protocol and it is just random stream of bits. In this case, jammer keeps the communication channel busy disrupting network communication by e.g. causing interference to the signal that is already being transmitted thus corrupting communicated packets.

While deceptive jammer uses deceptive jamming technique described above, the random jammers cycle between random sleep time t_s and random transmitting time t_j . By changing relation between t_s and t_j we can achieve desired level of effectiveness of jamming and acceptable power consumption. The reactive jammers listen to the network traffic in low power mode. When any activity is detected, reactive jammer sends out a random signal to collide with existing signal on the channel. As a result, transmitted packets are corrupted.

There are several classes of countermeasures against jamming. These classes are distinguished by the layer where countermeasures take place – the countermeasures at physical level and security schemes at higher layers of the system

6.4.1 Antijamming techniques at physical layer

The jamming is very powerful and easy achieved way of disturbing communication channel by adversary. The important knowledge for adversary is to find out start of the communication activity in tracked channel. The continual transmission of jamming signal has no reason because tracked channel could be inactive or should

move to another frequency. So, for the adversary would be important to know that there is an activity in tracked communication channel hence it has to monitor the respective channel for its activity. It gives a chance to the regular user to cover its activity by decreasing the level of the signal under detectable level and in that way to confuse the jammer monitoring device. From this point of view there are two controversial conditions

- to use high power transmitter which implies higher resistance against jamming because a stronger jamming signal is needed to overcome the original signal;
- to use low transmitted power to decrease probability of discovery ongoing transmission in the channel and by that way hide the communication from adversary.

The decreasing of power of transmitted signal could be also achieved by using antenna polarization or directive antenna. The polarization of antenna determines the orientation of electric and magnetic component of the electromagnetic field with respect to earth surface. The one is determined by physical structure of antenna and its orientation. For line of sight communication widely used in telematic application it could make a significant difference in signal quality to have the transmitter and the receiver using the same polarization¹. There will be significant difference in linearly polarized signal and circularly polarized signal reception. The antenna with circular polarization will not receive signals which are circularly polarized as for the opposite direction. Furthermore, there will be 3 dB loss from a linear polarized antenna that receives signal circularly polarized and vice-versa. As a result of this discussion we can conclude that by changing the polarization of the antenna we can defend the telematic nodes from jamming.

The other possibility would be the use of directional type of antenna. In general, directional antennas provide better protection against eavesdropping, detection and jamming than omnidirectional antennas. The example of radiation diagram of directional antenna is shown at Fig. 19. While directional antenna has one main beam in the specific direction with side lobes significantly smaller, the radiation diagram of omnidirectional antenna is usually circular or with two mirrored flat lobes.

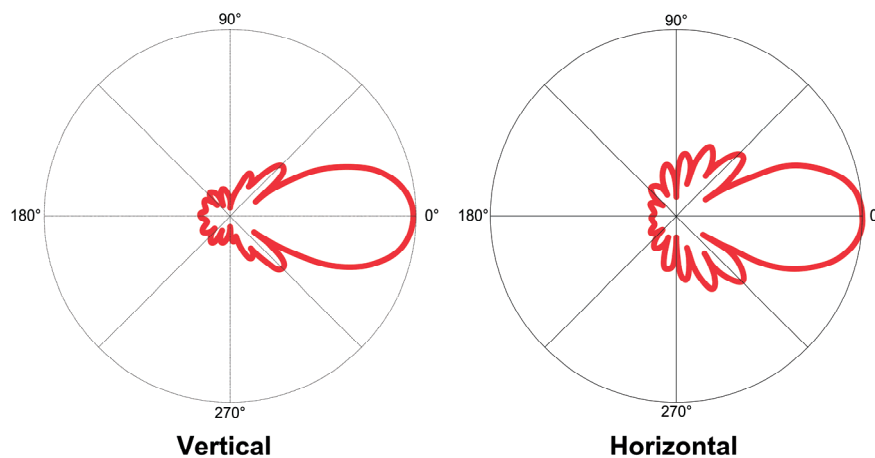


Fig. 19 Radiation diagram of directional antenna (Yagi)

There are two main problems with directional antenna when used in the network

- there is a requirement of more sophisticated MAC protocol [11] and
- more complex multipath routing protocol has to be used [60].

Typically, there are two types of directional antenna usually used in telematic network – sectored and beam forming. Sectored antenna has multiple fixed antenna elements, pointed in different directions that can often operate independently. On the other hand beam forming antennas have multiple element antennas that work in tandem to transmit or receive in different directions. The elements of beam forming antennas can be electronically switched or phased. When switching mechanism is used, antennas can select from set of

¹ It is not usually the case that polarization is either pure vertical or pure horizontal. In many cases the influence of environment and reflections adds other components and final polarization on the receiver side is circular. Also, presuming this situation, the standards as e.g. DSRC recommend circular polarization at transmitter side already.

predefined beams by shifting the phase of each antenna element's signal by precalculated amount. On the other hand so called steered beam forming antennas are more dynamic in their nature since main lobe of the antenna can be moved to any direction by linear shifting the signal phase of individual elements.

Such an antenna is usually called antenna array. In the telematic application using higher frequencies, like DSRC 5.8 GHz or higher, antenna array formed by patch antennas and microstrip lines on laminate are often used to form specific beam geometry. An example of antenna array using microstrip lines for phasing of patch antennas is on Fig. 20. This antenna design using Butler matrix with four inputs/outputs has been designed to excite a phased antenna array to steer the beams in different directions. The Butler matrix is fabricated together with the patch antenna array on high frequency laminate for frequency band 5.25 GHz.

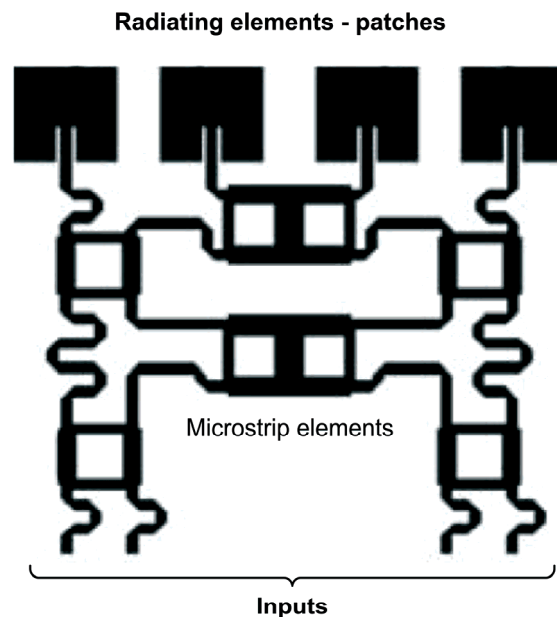


Fig. 20 Layout of patch antenna array with microstrip phasing elements (Butler matrix") [55]

The antijamming methods could be also based on manipulation of signal's spectrum. The method using frequency hopping spread spectrum (FHSS) transmits radio signals by rapidly switching carrier frequency among many frequency channels using shared algorithm known to both parties – transmitter and receiver. Using frequency hopping spread spectrum brings forward many advantages, as

- minimizes unauthorized interception and jamming of radio channels,
- SNR required for the carrier relative to background noise decreases as wider range of frequencies is used for transmission,
- it deals effectively with multipath effect, the phenomenon observed when radio signals reaches the receiving antenna through two or more paths due to reflections of original signal,
- multiple telematic systems can share the same frequency band without causing interference problem.

Unfortunately the overall bandwidth required by frequency hopping spread spectrum systems is much broader than that required to transmit same information using single carrier frequency. However, transmission on each specific lasts for very short time and then this frequency is released, so it could be used by another FHSS system which balances this disadvantage.

Another method, direct sequence spread spectrum (DSSS) transmission is performed by multiplying the data (the carrier frequency) being transmitted and pseudo-noise digital signal¹. This process causes the radio frequency signal to be replaced with very wide bandwidth signal with spectral equivalent of a noise signal. However this noise can be filtered out at receiving side to recover original data through multiplying the

¹ Pseudo-noise is digital realization of pseudorandom sequence of values +1 and -1 at much higher frequency than that of original signal, so called "chip rate".

incoming radio frequency signal with the same pseudo-noise modulated carrier. In direct sequence spread spectrum modulation technique is most of the FHSS modulation advantages still kept. Furthermore DSSS is difficult for adversary to descramble transmitted carrier and recover original signal mainly because high chip rate¹. Also, because DSSS received by regular receiver resembles white noise, radio direction finding of transmitting source is a difficult task.

The most promising antijamming technique is a combination of FHSS and DSSS modulation. In general terms, direct sequence spread spectrum systems achieve their processing gains through interference attenuation using wider bandwidth for signal transmission while frequency hopping spread spectrum systems do the same through interference avoidance. The hybrid system compared to individual FHSS or DSS modulation decreases probability of detection and probability of interception. It has to be stressed that both, the frequency sequence and pseudorandom sequence should be known to recover original signal.

The last but not least antijamming technique is called ultra wide band modulation scheme. This modulation technique is based on transmitting very short pulses on a large spectrum of a frequency band simultaneously [27]. This makes the transmitted signal very hard to be intercepted or jammed as well as it is resistant to the multipath effect. In some research papers had been shown that ultra wide band modulation promises low power and low cost wide deployment of communication network².

To use antijamming technology in telematic system is not always possible. Some systems like e.g. DSRC use more simple modulation method either because of saving power necessary for battery equipped devices³ or just for economy of the system. Broadband technologies, FHSS, DSSS or UWB are not widely deployed days. Some experiments had been made to design reliable and secure backscatter⁴ node using low power baseband processor with spread spectrum encoding circuit. Achieved results show that, compared with BER performances of conventional telematic node system using FM0 encoded signal in the backscatter chain, DSSS enhanced backscatter system has distinct advantages to resist noise, interference, and interceptions [57].

6.4.2 Antijamming Security schemes

Securing telematic system against jamming is not a simple task and it is issue of immense importance. We already had analyzed the physical layer methods of antijamming but there should be also other methods on higher layers which could be used to secure the communication. We can propose three categories of approach

- proactive measures,
- reactive measures,
- and mobile agent based measures.

The proactive and reactive measures could be further understood as software countermeasures and combined software/hardware countermeasures. The role of proactive countermeasures is rather to make telematic system immune to jamming than to react in the event of incident. The main characteristic of reactive countermeasure is that they enable reaction only upon the incident sensed by node.

6.4.2.1 Proactive countermeasures

The major role of software proactive countermeasures remains in using software methods to help a node to survive attack or when attack is detected, the software initiate other defensive mechanism. The nature of attack will be the major parameter for differentiation in accepting proactive countermeasures. We can distinguish among following approaches

- creating and analyzing models of attack to verify feasibility of launching and detecting jamming attack. In this case we can present four different jamming attack models according to [77]. To improve detection the notion of consistency checking is introduced. The packet delivery ration is used to

¹ E.g. in 802.15.4 network the chip rate is 2 Mchip/s.

² IEEE 802.15.3a was an attempt to provide a higher speed UWB PHY amendment to IEEE 802.15.3 for applications which involve imaging and multimedia. The members of the task group were not able to come to an agreement and topic was withdrawn in January 2006. From that time further some other moves are continuing separately, e.g. IEEE 802.15.4a Includes a C-UWB physical layer.

³ In the case of DSRC it would be OBU, which is in principle semi-passive RFID element.

⁴ Backscatter node is just different term for semi-passive or passive OBU.

classify radio link and then consistency check is performed to classify whether the poor link quality is due to jamming. In the model mentioned above, two enhanced detection algorithms are designed: one employing signal strength for consistency check and one employing location information for consistency check;

- examination of link layer protocols, as in the reference [44], where authors had examined three representatives of MAC protocols, S-MAC, L-MAC and B-MAC. Based on the analysis several methods of jamming attack were derived that allow adversary to jam above the MAC protocols in energy efficient manner. These attacks could be subdivided into attacks
 - effective on encrypted packets,
 - effective as constant/deceptive/reactive jamming,
 - more energy efficient than random jamming or reactive jamming.

Unfortunately, main conclusion of mentioned work had shown that with the typical telematic system used today there are not effective measures against link layer jamming. We should state at this point that to increase security of link layer would be possible either through physical level antijamming methods like FHSS or DSSS or through using specific link control strategy¹. Also encryption of packet at link layer would be some of help;

- detection radio interference and radio interference protocol are discussed in [80]. The basic idea of radio interference detection protocol is that a transmitter broadcasts a high power detection packet and subsequently normal power detection packet. The receiver uses this sequence to estimate the transmitter's interference strength. While high power carries transmitter's ID, the receiver estimates possible interference by sensing the power in normal power packet. When this process is finished, the node propagates detected interference information to all neighbor nodes and uses this information to figure out all possible collision cases within the system. The information acquired is then used to control the process of packet delivery. It has been proved, if the information is used for control of TDMA² protocol, the packet delivery ration reaches nearly 100% while uncontrolled TDMA itself has packet loss about 60%. Even this approach looks hopefully, actual usage is doubtful because only interference from adjacent nodes are effectively addressed. Jamming for external sources is not considered hence radio interference detection protocol remains highly vulnerable to jamming attack;
- defeating energy efficient jamming by specific MAC layer protocol as it had been designed e.g. in [73] by Wood et al. The general design approach of this protocol is to hide a message from jammer, evade its search and reduce the impact of messages that are corrupted anyway. The DEEJAM protocol proposes countermeasures for four different jamming attacks as
 - interrupt jamming as type of reactive jamming, where jammer starts jamming activity in the case when Start of Frame Delimited (SFD) is monitored in tracked channel. The defense proposed for this time of jamming is "masking the SFD". For this purpose the sender and receiver node has to agree on secret pseudorandom sequence for SFD in each packet. In such a case, the SFD is not detected and jamming will not be started. Naturally, this method cannot defend effectively against constant jamming;
 - activity jamming which is also type of reactive jamming when attacker periodically samples the radio channel looking for radio activity. When signal strength in tracked channel goes over programmable threshold, jammer initiates attack. Only proposition made for this type of attack is to use some lower layer method as FHSS;
 - scan jamming is appropriate attack against frequency hopping spread spectrum modulation technique, however attacker must use significantly higher hopping rate from the victim. During the course of attack, adversary samples each channel as briefly as possible to determine if there is any activity present³. If activity is discovered, jamming is immediately initiated. Because of

¹ Such a strategy could use Time Division Multiplexing technique or randomization of the interval of channel usage.

² Time Division Multiplexing Access

³ It is the same method as in the case of activity jamming, but with much higher sampling rate.

time necessary for change from discovery mode to jamming mode, this attack would be efficient when long packet is used. One of the countermeasures recommended is to use short packets and packet fragmentation. Using packet fragmentation a node breaks the transmitted packet into fragments which are transmitted separately on different channels and with different SFD's. If the fragments are short enough an attacker's reactive jamming message does not start until after the sender has finished transmitting and hopped to another channel;

- pulse jamming happens where attacker is blindly jamming on short pulses on a single channel. This will corrupt the fragments of a packet that would use the current channel and taking into account that corrupting even one fragment is sufficient to cause the drop of entire packet. The pulse jamming can achieve excellent results in system with limited number of communication channels for frequency hopping. As a countermeasure redundant encoding of a packet is proposed.

The DEEJAM protocol utilizes all above mentioned defensive mechanisms to protect telematic system against jamming from adversaries that use hardware with same capabilities as deployed nodes. The main advantage of this approach is that it is compatible with most of existing nodes' hardware.

The software proactive measures are limited by using standard hardware, so some measures, which should be easily and effectively implemented in hardware, are not possible. Combined proactive measures are focused on the design of innovative antijamming hardware along with proposal of algorithms that will utilize the new properties of hardware. The hardware features implemented in combination with software improvement usually use different types of spread spectrum modulation or controlled TDMA with respective software algorithm for control.

Gavalas et al. introduce outline the design of prototype node named Hermes which effectively defends jamming attacks [26]. Authors propose to use 5 GHz band where is enough bandwidth for spread spectrum modulation is available. Hermes uses hybrid FHSS/DSSS scheme as the main countermeasure against jamming. The core modulation is O-QPSK¹ with 55 frequency channels for FHSS and 5 MHz for DSSS available in each channel. Each channel uses DSS modulation scheme with 270 kHz pre spreading bandwidth reaching total 5 MHz two sided spread spectrum signal bandwidth. Hermes nodes are able to perform up to 10^5 frequency hops per second, so it is rather difficult for jammers to hop along and jam at the same time. The sequence of hopping is determined by generation algorithm which uses secret key as a seed. For the synchronization of communicating nodes the flooding synchronization protocol running on predefined frequency channel is used [48]. It uses low communication bandwidth and exhibits proven robustness against node and link failures. The main advantage of Hermes project is that it deals with the problem of jamming using a powerful hardware scheme capable of defending a telematic network against the most sophisticated and with unlimited power resources jammers. However, all these advantages come with an increased cost.

The physical layer and data link layer are considered as a major driver in the combined antijamming architecture. Law et al. [43] deal with many security aspects including jamming on these two bottom layers. They suggest the use of FHSS instead of DSSS because later requires more complex hardware circuits, power consumption is higher and whole system is more sensitive to environmental process [56]. The hop rate in FHSS system is typically much lower than the chip rate in DSSS system resulting in lower energy usage. Authors also discuss lowest acceptable rate of channel switching with conclusion of 500 to 1000 hops per second as a practical compromise. For transceivers that do not support spread spectrum it is recommended to use channel surfing method, changing the transmission frequency to a range where there is no interference from the adversary, as sufficient defense against DoS by jamming [78]. Finally for jamming on data link layer using TDMA protocol is recommended in absence of effective countermeasures.

¹ Offset Quadrature Phase-Shift Keying (O-QPSK) is a variant of Phase-Shift Keying modulation using four different values of the phase to transmit. Difference of the phase between ordinary QPSK and O-QPSK **remains** in the maximum phase shift when the phase in ordinary QPSK can change by 180° at once, while in OQPSK the changes are never greater than 90° .

6.4.2.2 Reactive countermeasures

The main characteristic of reactive countermeasures is that they enable reaction only upon the incident of jamming attack sensed by the node. These countermeasures can be also classified into two subcategories – software and combined software/hardware countermeasures, similarly to proactive countermeasures.

Main attribution of clean software reactive countermeasures is a functionality called jammed area mapping service. The algorithm JAM enables the detection and mapping of jammed regions to increase network efficiency [74]. Data is then simply routed around the jammed regions. The problem is that the jammed node itself would not be able to send any message, since almost all MAC protocols require a carrier sense to indicate a clear channel for broadcasting. The author of JAM algorithm proposes to use specific state of the node when carrier sense is overridden to allow broadcasting of a short high priority unacknowledged message. However, this action could lead to energy exhaustion of jammed nodes in the case of link layer jamming. Some benefits of mapping of jammed regions are

- feedback to routing and directory services,
- an effective abstraction at higher level than local congestion, failed neighbors and broken routes,
- support for avoiding the region by network controlled vehicles, military assets and emergency personnel,
- reports to a base station for further jamming localization and eventual offensive action against jammer,
- aid to power management strategies for nodes inside and around jammed region.

In cases that jamming attacks are restricted to small portion of network, JAM has beneficial results for robustness and functionality of the network. However, this method exhibits also several shortcomings – it cannot practically defend in the scenario that the attacker jams the entire telematic network or significant percentage of nodes and this technique fails to protect attacked nodes.

Combined software/hardware countermeasures use specialized hardware with proposed software solution. In previous section we have mentioned work [78] where one important feature – spatial retreat is presented. Spatial retreat can be applied only upon nodes that have a capability of mobility. It is an algorithm according to which two nodes move in Manhattan distances to escape from jammed region. The key to success of this strategy is to decide where the participants should move and how should they coordinate their movements. The main shortcoming of the mentioned strategy is that it is effective only against constant jammers and they have no results against more intelligent or follow-on jammers.

Çagalj et al. [21] proposed a reactive antijamming scheme using wormholes. The basic idea is that jammed nodes use channel diversity to establish a communication with another node outside the jammed area. There could be recognized two types of proposed wormholes¹

- frequency hopping pairs which is achieved by creation of pairs by using frequency hopping scheme similar to Bluetooth technology. All pairs are being deployed by synchronized wireless links affording longer links between pairs. Despite of the fact that frequency hopping spread spectrum is not an effective countermeasure against fast follower jammers, there are also two other problems of the technique
 - synchronization of pairs. It could be solved by using specific protocol, like time synchronization protocol like in [24], but this technique could be easily attacked as well [47];
 - some nodes (OBU or terrestrial stations) must be equipped by more sophisticated transceivers which can significantly increase the cost of the network. Also, the deployment of the network would be more complex and time consuming.
- uncoordinated channel hopping, where nodes are able of hopping among radio channels spanning large frequency band and creating probabilistic strategy of “hopping wormhole”. Nevertheless, in this case, individual packets are transmitted over a single channel allowing more time to adversary to recover channel in use and jam it. The common problems of frequency hopping also apply to this solution.

¹ Actually, authors proposed three methods in [21], but only two should be used in system with many degrees of freedom. The wiring of nodes of networks is not acceptable in ITS where OBU has to have freedom of movement.

Based on the discussion above, we can conclude that the wormholes techniques may be interesting to defend against jamming attacks, but a different approach must be taken. Unfortunately, proceeded reactive countermeasures will not be sufficient and effective defense in the case of the large scale attacks or sophisticated fast follower jammers attacks.

7 Conclusion

Telematic system as any other system has its own vulnerabilities and strength. The rationale behind this is the recognition of increasing vulnerability of organizations using telematics systems. Within organizations the awareness grows that information security is an important concern to consider. The management of those organizations wishes their telematics systems to be more secure but unfortunately, adding safeguards to operational systems leads to increase of complexity of the system and last but not least to operational problems and not to secure systems.

To avoid operational problems of information security in telematic system there should be an issue throughout the entire design of the telematics system. However, it is not common practice to take information security into account as a relevant design concern. In general the difficulties to embed information security in a traditional design process are

- The design focuses on the must-functionality of the system.
- Implicit requirements, which include most information security requirements, are left in the mind of the users.
- It is unclear how information security requirements proliferate throughout the design process.

Embedding information security in the design should be based on general information security requirements (confidentiality, integrity, availability) and the threats for the system. The set of information security requirements consists partially of functional requirements and partially of quality aspects of the functional requirements. The environment of the system has a large impact on the requirements, and should therefore already be considered in the definition of the design project. Context knowledge of the system is essential to make appropriate assumptions about the elements in the environment that are taken into account.

Standard technical safeguards should be used carefully in design of telematic system because they slightly differ in functionality and external behavior from the desired safeguard. By implementing only technical safeguards system itself cannot fulfill the specifications of its external behavior. The system must operate in a real-life environment with real threats and organizations that tend to change.

The project leader has to have on the mind that every design phase possibly includes conflicts among requirements and behavior specifications. Decisions as to which requirements prevail over others should be guided by a strategy, at least partly based on the security policy of the organization. Proliferation of the information security requirements throughout the design phase without extra measures to guide them through the whole design process should be avoided, because

- Even it sounds paranoiac, we should expect potential malicious behavior of the system architect and system builder.
- There is already tension between a certain level of abstraction in a design phase and the desired level of detail that makes it difficult to deliberately select among safeguards.

Considering the above difficulties and observations, we can recommend to develop methods to gather implicit requirements and treat threats as actions and their behavior as interactions with the system. The development of a framework for system's boundaries has to be in relation to threats and first of all we have to specify a set of principles to guide the structuring of a system, including information security.

References:

- [1] - : Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements, Brussels 2009
- [2] - : Commission Decision of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements 2009/750/EC, Brussels 2009
- [3] - : Data Encryption Standard (DES), National Institute of Standards and Technology, October 1999
- [4] - : Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Brussels 2002
- [5] - : Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003, Brussels 1995
- [6] - : EU Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community, Brussels 2004
- [7] - : Federal Standard 1037C, Glossary of Telecommunication Terms, Alliance for Telecommunications Industry Solutions, Washington DC, 2008
- [8] - : IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, Institute of Electrical and Electronics Engineers, New York, NY, 1990
- [9] - : Technical Committee CEN/TC "CEN TC278 WG1 "Electronic Fee Collection (EFC) — Security Framework", NEN, October 20, 2009
- [10] Ballare, M., Canetti, R., Krawczyk, H.: Keyed Hash Function and Message Authentication, Advances in Cryptology – Proceedings of CRYPTO'89, pp. 547-559, 1989
- [11] Bandyopadhyay S., Hasuik K., Horisawa S., Tawara S.: An adaptive MAC and directional routing protocol for ad hoc wireless network using directional ESPAR antenna, in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing 2001, Long Beach CA, pp. 243-246, October 2001
- [12] Bellare S., Merritt M.: Limitation of Kerberos Protocol, Proceedings of the 1991 Winter USENIX Conference, pp 253-267, January 1991
- [13] Biham, E., Dunkelman O., Keller N.: A New Attack on 6-Round IDEA, in Fast Software Encryption, FSE 2007, Lecture Notes in Computer Science 4593, Springer-Verlag, pp. 211-224, 2007
- [14] Biham, E., Shamir, A.: Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer, Advances in Cryptology, Proceedings of Crypto'91, pp. 156-171, August 1991
- [15] Biham, E.: New Techniques for Cryptanalysis of Hash Functions and Improved Attacks on Snefru, Fast Software Encryption, Lecture Notes in Computer Science, Volume 5086, Springer Berlin/Heidelberg, 2008
- [16] Bishop M.: Password management, in Proceedings of COMPCON'91, pp. 167-169, February 1991
- [17] Bishop, M.: Computer Security: art and Science, Pearson Education, Inc., New Jersey, March 2009
- [18] Bloch M., Barros J., Rodrigues M. R. D., McLaughlin S. W.: Information-Theoretic Security for Wireless Channels: Theory and Practice, Proc. Inform. Theory and Applications Workshop, San Diego, USA, Feb. 2007.
- [19] Brown, L., Kwan, M., Pieprzyk, J., Seberry, J., Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI, Advances in Cryptology, Proceedings of Asiacrypt'91, pp. 36-50, 1991
- [20] Brown, L., Pieprzyk, J., Seberry, J., Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI, Advances in Cryptology, Proceedings of Auscrypt'90, pp. 229-236, January 1990
- [21] Cagalj M., Capcun S., Hubaux J.P.: Wormhole based antijamming technique in sensor networks,

IEEE Transaction on Mobile Computing, 6(1), pp. 100-114, May 2006

- [22] Cusdick, T., Wood, M.: The REDOC-II Cryptosystem, *Advances in Cryptography, Proceedings of Crypto'90*, pp. 1 – 16, August 1990
- [23] Diffie, W., Hellman, M.: New Directions in Cryptography, *IEEE Transaction on Information Theory* 22 (6), pp. 644-654, November 1976
- [24] Ganeriwal S., Kumar R., Srivastava M.: Timing-Sync Protocol for Sensor Networks, in *The First ACM Conference on Embedded Networked Sensor Systems (SenSys)*, p. 138-149, 2003
- [25] Garfinkel, S.: PGP: Pretty Good Privacy, O'Reilly Media, pp. 101–102, December 1, 1994
- [26] Gavalas D., Mpitiopoulos A.: Countermeasures against radio jamming attacks in wireless sensor networks, *International Journal of Computer Research*, 15(1), pp. 5-22, March 2007
- [27] Ghavami M., Michael L.B., Kohno R.: *Ultra Wideband Signals and Systems in Communication Engineering*, Wiley, 2004
- [28] Guo J., Ling S., Rechberger, Ch., Wang H.: Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2, <http://eprint.iacr.org/2010/016.pdf> (Downloaded February 7, 2011)
- [29] Haskett J.: “Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms, *Communication of the ACM* 27(8), pp. 777-781, August 1984
- [30] <http://www.activism.net/cypherpunk/manifesto.html>, downloaded January 2011
- [31] Jirovsky, V.: The Society in Virtual World, in *Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management*, ed. Alan Rea, IGI Global 2011
- [32] Jirovský, V.: Virtual communities and cyber terrorism, Paper presented at Security and Protection of Information Conference, Brno 2007, Czech Republic
- [33] Kahn, D.: On the Origin of a Species. *The Codebreakers: The Story of Secret Writing*, Simon & Schuster, 1999
- [34] Kasiski, F. W.: *Die Geheimschriften und die Dechiffir-Kunst*, E. S. Mittler und Sohn, Berlin 1863
- [35] Knudsen, L. R.: Block Ciphers— a survey, in Preneel B., Rijmen V.: *State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptograph*, Leuven Belgium, June 1997
- [36] Knudsen, L. R.: Block Ciphers— a survey, in Preneel B., Rijmen V.: *State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptograph*, Leuven Belgium, June 1997
- [37] Konheim, A.: *Cryptography: A Primer*, John Wiley and Sons, New York, 1981
- [38] Konheim, A.: *Cryptography: A Primer*, John Wiley and Sons, New York, 1981
- [39] Lager, A.: Implementation of DES Algorithm Using FPGA Technology, Semestral project EPFL Lausanne, Lausanne 2001
- [40] Lager, A.: Implementation of DES Algorithm Using FPGA Technology, Semester project EPFL Lausanne, Lausanne 2001
- [41] Lai, X., Massey, J., Murphy, S.: Markov Ciphers and Differential Cryptanalysis, *Advances in Cryptology, Proceedings of Eurocrypt'91*, pp. 17-38, 1991
- [42] LaMalachia, B., Odlyzko, A.: Computation of Discrete Logarithms in Prime Fields, *Design, Codes and Cryptography* 1, pp. 46-62, May 1991
- [43] Law Y., Havinga P.: How to secure a wireless sensor network, in *The Proceedings of the 2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp.

- [44] Law Y., Hoesel V., Doumen J., Hartel P., Havinga P.: Energy efficient link layer jamming attacks against wireless sensor network MAC protocols, in Proceedings of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SANS 2005, ACM Press, pp. 76-78, 2005
- [45] Leung-Yan-Cheong S. K., Hellman M. E.: The Gaussian Wire-Tap Channel,” IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, July 1978
- [46] Liddell G. H., Scott R.: Greek-English Lexicon, Oxford University Press, USA, 1996
- [47] Manzo M., Roosta T., Sastry S.: Time Synchronization Attacks in Sensor Networks, in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks SASN, 2005
- [48] Maroti M., Kusy B., Simon G., Ledeczi A.: The flooding time synchronization protocol, Technical report ISIS-04-501, Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN. 2004, available at <http://www.eecs.harvard.edu/mdw/course/cs263/papers/ftsp-sensys04.pdf> (Downloaded November 8, 2010)
- [49] Merkle, R.: Fast Software Encryption Function, Advances in Cryptology, Proceedings of Crypto’90, pp. 476-501, August 1990
- [50] Meyer G.: The PPP Encryption Control Protocol (ECP), RFC 1968, June 1996
- [51] Miyaguschi, S.: The FEAL Cipher Family, Advances in Cryptography, Proceedings of Eurocrypt’90, pp. 6277-638, 1991
- [52] Naito, Y., Sasaki, Y., Kunihiro, N., Ohta K.: Improved Collision Attack on MD4 with Probability Almost 1, Information Security and Cryptology - ICISC 2005, Lecture Notes in Computer Science, pp. 129-145, Volume 3935, Springer Berlin/Heidelberg, 2006
- [53] National Bureau of Standards: Data Encryption Standard, FIPS PUB 46, January 1977
- [54] Neuman P.G., Parker D.B.: A Summary of Computer Misuse Techniques, in Proceedings of the 12th National Computer Security Conference, October 1989, Baltimore, USA
- [55] Pham N. T., Lee G. A., Flaviis F.: Microstrip Antenna Array with Beam Forming Network for WLAN Applications, <http://www.ece.uci.edu/rfmems/publications/papers/antenna/C104-APS05.pdf> (Downloaded March 12, 2011)
- [56] Pottie G. J., Clare L. P.: Wireless integrated network sensors: toward low-cost and robust self-organizing security networks, in Sensors, C31, Information and Training Technologies for Law Enforcement, ser. SPIE Proceedings, vol. 3577, pp. 86-95, 1999, available at <http://wins.rsc.rockwell.com/publications/spie3577-12.pdf> (Downloaded October 22, 2010)
- [57] Qiuling Z., Chun Z., Xiaohui W., Ziqiang W., Zhihua W.: VLSI Design of Spread Spectrum Encoding Low Power RFID Tag Baseband Processor, 2009 International Symposium on VLSI Design, Automation and Test, Hsinchu, Taiwan, April 27-30, 2009
- [58] Ranasinghe D.C., Cole P.H.: Confronting security and privacy threats in modern RFID systems, in Proceedings of ACSSC06, pp. 2058 – 2064, Pacific Grove, CA, 2006
- [59] Rosenheim, S. J.: The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet, Johns Hopkins University Press, Baltimore, 1997
- [60] Roy S., Bandyopadhyay S., Ueda T., Hasuike K.: Multipath routing in ad hoc wireless network with omnidirectional and directional antenna: A comparative study, in Proceedings of 4th International Workshop of Distributed Computing, Mobile and Wireless Computing, IWDC 2002, Calcutta, India pp. 184-191, December 2002
- [61] Sasaki, Y., Aoki K.: Finding Preimages in Full MD5 Faster Than Exhaustive Search, Advances in Cryptology, Lecture Notes in Computer Science, pp. 134-152, 2009, Volume 5479, Springer Berlin/Heidelberg, 2009
- [62] Scheider, B.: Applied Cryptography, John Wiley and Sons, New York 1996

- [63] Schneier, B.: Attack Trees - Modeling security threats, Dr. Dobbs' Journal, December 1999, <http://www.schneier.com/paper-attacktrees-ddj-ft.html> (Downloaded February 20, 2011)
- [64] Scott, R.: Wide Open Encryption Design Offers Flexible Implementation, Cryptologia 9 (1), pp. 75-90, January 1985
- [65] Shannon C. E.: A Mathematical Theory of Communication, The BellSystem Technical Journal, vol. 27, pp. 379-423, 623-656, July, October 1948.
- [66] Shimizu, A., Miyaguschi, S.: Fast Data Encipherment Algorithm FEAL, Advances in Cryptography, Proceedings of Eurocrypt'87, pp. 267-278, 1987
- [67] Simmons, G.: Forward Search as a Cryptanalytic Tool Against a Public Key Privacy Channel, Proceedings of the 1982 IEEE Symposium on Security and Privacy, pp. 117-128, April 1982
- [68] Singh, S. : The Code Book, Anchor Books, Random House, 1999
- [69] Steiner J., Neuman C., Schiller J.: Kerberos: An Authentication Service for Open Network Systems, Proceedings of the 1988 Winter USENIX Conference, pp. 191-202, February 1988
- [70] Thomsen, S.: An improved preimage attack on MD2, <http://eprint.iacr.org/2008/089.pdf>, (Downloaded February 7, 2011)
- [71] Vincenzetti D., Taino S., Bolognesi F.: STEL : Secure TELnet, in Proceedings of the 5th USENIX UNIX Security Symposium, pp. 75-83, June 1995
- [72] Wang X., Lai X., Feng D., Chen H., Yu X.: Cryptanalysis of the Hash Functions MD4 and RIPEMD, Advances in Cryptology, Lecture Notes in Computer Science, p. 551, Volume 3494, Springer Berlin/Heidelberg, 2005,
- [73] Wood A.D., Stankovic J.A., Zhou G.: DEEJAM: Defeating energy efficient jamming in IEEE 802.15.4 based wireless networks, in Proceedings of the 4th annual IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 60-69, San Diego, CA, June 2007
- [74] Wood D., Stankovic J. A.: Denial of Service in Sensor Network, Computer, 35(10), pp. 54-62, 2002
- [75] Xie T., FengHow, D.: To Find Weak Input Differences For MD5 Collision Attacks, <http://eprint.iacr.org/2009/223.pdf>, (Downloaded February 7, 2011)
- [76] Xu W., Trappe W., Zhang Y., Wood T. : The feasibility of launching and detecting jamming attack in wireless networks, in Proceedings of the 2004 ACM workshop on Wireless security, pp. 80-89, New York, 2004
- [77] Xu W., Trappe W., Zhang Y., Wood T. : The feasibility of launching and detecting jamming attacks in wireless network, Proceedings of the 6th ACM international symposium on Mobile Ad Hoc Networking and Computing, pp. 46-57, 2005
- [78] Xu W., Wood T., Trappe W., Zhang Y.: Channel surfing and spatial retreats: Defenses against denial of service, in Proceedings of the 2004 ACM workshop on Wireless Security, pp. 80-89, New York, 2004
- [79] Zhanshan Ma: Towards a Unified Definition for Reliability, Survivability and Resilience: the Conceptual Framework Inspired by the Handicap Principle and Ecological Stability, Aerospace Conference 2010, pp. 1 – 12, 6-13 March 2010
- [80] Zhou G., He T., Stankovic J. A., Abdelzaher T. F.: RID: Radio interference detection in wireless sensor network, in Proceedings of the IEEE INFOCOM' 2005, pp. 891-901, 2005