ATTACKS TO CRYPTOGRAPHY PROTOCOLS OF WIRELESS INDUSTRIAL COMMUNICATION SYSTEMS

Tomas ONDRASINA[1], *Maria FRANEKOVA*[1]

[1]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna 1, 010 26 Zilina, Slovak Republic

tomas.ondrasina@fel.uniza.sk, maria.franekova@fel.uniza.sk

Abstract. *The paper deals with problems of safety and security principles within wireless industrial communication systems. First safety requirements to wireless industrial communication system, summarisation of attack methods and the available measures for risks elimination are described with orientation to safety critical applications. The mainly part is oriented to identification of risks and summarisation of defensive methods of wireless communication based on cryptographic techniques. Practical part the cryptoanalytic's attacks to COTS (Commercial Off-The-Shelf) wireless communications are mentioned based on the IEEE 802.11 standards.*

Keywords

Safety and security issues, wireless industrial communication system, attack, safety integrity level, cryptographic techniques, wireless communications, cryptoanalysis.

1. Introduction

Industrial communication systems are important elements of automation systems which are used in wide variety of application, e. g. process manufacturing, electric power generation and distribution, gas and water supply, transportation and others.

In many cases the industrial communication systems is component part of system which partook in control of SRCP (*Safety- Related Critical Processes*). Undetected corruption of data transmission (e.g. control commands) can cause considerable substantially damages within equipments, environments or demands on human health and this is reason why system have to be designed so that guarantee required SIL (*Safety Integrity Level*) defined by generic standard IEC 61508 [1].

For this reason the safety-related wireless machines must have implemented a number of safety mechanisms located into special safety or security profiles distinct from the office system, so called COTS (*Commercial Off-The-Shelf*) systems [2]. Data integrity, user authentication and access control are very important services need for the safety critical operation of the industrial communication system mainly if system is based on the wireless technology.

In the last decade wireless technologies have been used for several industrial application for remote control, but for safety-related machine-to-machine applications are still rare [3], [4].

In area of standard measurement and control systems we can used many types of wireless technologies [5], [6]. Without GSM (*Global System of Management*) between the most recommended standards belong technology Wi-Fi, Bluetooth and ZigBee. Figure 1 shows examples of some wireless protocols, with comparison of their practical distance and rate [7].

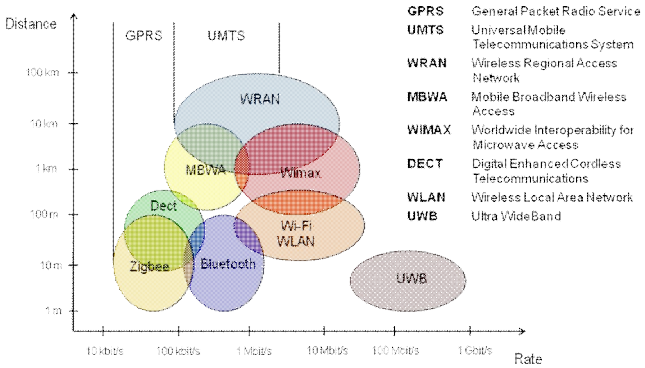

Fig. 1: Wireless protocols, their communication speed and operation range.

When we compare wire fieldbus systems and wireless communication systems many similar risks occur during transmission are relevant also in wireless communication systems, but wireless systems introduce also some new risks and the probability of failures is often higher than in wired systems.

Basic wireless communication threats we can summarised by the following points:

- the transmission fades because the distance between sender and receiver increases,
- the signal fades because of obstacles and of environment conditions,
- transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances,
- two or more signals interfere with each other and cause proper signal for another receiver,
- receiver is too sensitive,
- the nodes understand the network state or configuration differently at the same time,
- security; intentional penetration to wireless network,
- systematic failure, characteristics of wireless communication is not considered,
- sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower power consumption i.e. longer battery life.

These communication threats can effect the following consequences: signal level is low, bit error rate increases, data is corrupted or lost, the signal can be delayed, new messages may be inserted. There is no communication through a sleeping node until the node awakes and others.

Within communications between safety–related wireless machine all the risks or threats must be considered, safety requirements determined, adequate measures are applied to minimise risks and the system is validated, wireless communication can be relevant possibility in safety-related machinery applications.

Basic principles valid for safety a security profiles implemented within wireless communication system the following safety a security standards define [8], [9], [10].

In the paper safety analysis of standard Wi-Fi communication protocols based on IEEE 802.11 standard is mentioned only with orientation to cryptography mechanisms used in cryptography protocols WEP and WPA.

2. Analyses of Cryptography Mechanisms used in Cryptography Wireless Communication Protocols

The basic requirements for all cryptosystem are so that cryptography mechanisms implemented within communication protocols were resistant against known cryptoanalytic attacks during all life time of system. For considering of safety and effectively of used cryptography algorithm can be used the method for expression of computationally complexity of algorithms, which are based on the principle of complexity theory. Operational demanding of algorithm is determined on the based on the asymptotic complexity, which is describes which way the behaviour of algorithm will be change according to input data of length *n*. Operational demanding is generally marked by notation *O* (called Landauov's notation or Bachmann-Landauov's notation) and is function *f* of input data $O(f(n))$. Computationally complexity determine generally three parameters: S (*Space)*, T (*Time*) and D (*Data*).

Nowadays as computationally safety algorithms are considered algorithms with exponential combinational complexity, which can be breakup in real time for small value of n input data only.

Basic specifications of communication Wi-Fi protocol defined according to standard IEEE 802.11 [11]. Nowadays series IEEE 802.11a to IEEE 802.11n exist. Original cryptography standard IEEE 802.11 is based on the WEP (*Wired Equivalent Privacy*) protocol, which has implemented the stream Rivest Cipher RC4 (for data confidentiality) and check sum on the base of CRC (*Cyclic Redundancy Check*) CRC-32 (for data integrity). Standard length of the key is 40 bits, to which is added 24 bits of initial vector (IV). The key is represented by the hexadecimal number. Expanded length of the key in WEP protocol is 104 bits with 24 bits of IV. Less safe kind of ciphering, which supported WEP protocol is in the present time replaced by cryptography protocol WPA (Wi-Fi Protected Access), which uses stream cipher RC4 too, but the length of cipher key is 128 bits and the length of initial vector is 48 bits. Fundamental increasing of safety is obtained with using TKIP (*Temporary Key Integrity Protocol*), what is protocol for dynamic change of keys.

The use of this type of protocol is based on the server RADIUS, this solution is way for assuring of company. For private sector simpler implementation exists via PSK (*Pre-Shared Key*), in which the keys in all equipment are set forwards. Protocol WPA MIC (Message Integrity Code) has implemented (for integrity check) so called MICHAEL. This method uses the check of the frames counter, what eliminates against replaying attacks. Nowadays in recommendation IEEE 802.11i advanced cryptography protocol WPA2 is defined, which replaced protocols WEP and WPA.

In this protocol the stream cipher RC4 is replaced by cipher AES (Advanced Encryption Standard) [12], which is in the present time computationally safety cryptography standard, which symmetric cipher DES (*Data Encryption Standard*) replaced. Assuring by protocol WPA2 contents authentication according to IEEE 802.1x and definition of new protocol CCMP (*Counter Mode Cipher Block Chaining MIC Protocol*).The main characteristics of the cryptography protocols used in wireless networks are illustrated in Tab.1.

Tab.1: The main characteristics of the cryptography protocols used in the wireless networks.

Protocol	WEP	WPA	WPA2
Encryption	Rivest Cipher 4 RC4	Rivest Cipher 4 RC4	Advanced Encryption Standard AES
Key length	104 bits 40 bits	128 bits (encryption) 64 bits (authentication)	128 bits 192 bits 256 bits
Length of IV	24 bits	48 bits	48 bits
Data integrity	CRC-32	Michael	Counter with CBC-MAC (Cipher Block Chaining of Message Authentication Code)
Header integrity	None	Michael	Counter with CBC-MAC (Cipher Block Chaining of Message Authentication Code)
Key control	None	Extensible Authentication Protocol (EAP)	Extensible Authentication Protocol (EAP)

3. Practical Realisations of Attacks

WEP protocol is based on the RC4 encryption algorithm, with the secret key of 40 bits or 104 bits being combined with a 24 bits of IV (*Initialisation Vector*). The encryption of message *C* is determined using the following formula:

$$C = [M \parallel ICV(M)] + [RC4(K \parallel IV)], \quad (1)$$

where || is a concatenation operator, ICV is integrity check value and + is a XOR operator. Clearly, the initialisation vector is the key to WEP security, so to maintain a decent level of security and minimise disclosure the IV should be incremented for each packet so that subsequent packets are encrypted with the different keys. Unfortunately for WEP security, the IV is transmitted in plain text and the IEEE 802.11 standard does not mandate IV incrementation, leaving this security measure at the option of particular wireless terminal (access point or wireless card) implementations.

Security weaknesses of WEP can be summarised as follows:

- the weaknesses of RC4 algorithm due to key construction,
- the use of static key (maximum of 4 keys), change only IV,
- IVs are too short (24 bits) and IV reuse is allowed (no protection against message replay, cycle only 224), ICV encryption with data,
- the use the same algorithm for encryption and authentication,
- no proper integrity check (CRC32 is used for error detection and isn't cryptographically secure due to its linearity),
- no built-in method of updating keys.

These weaknesses are used within the active and the passive attacks against WEP protocol. The main attracts are the following: brute-force attack (distributed and dictionary attacks), FMS attack, KoreK, Klein's attack, Man-in-the-middle attack and others.

The attacks can be realised via different SW tools as AirCrack, Airbase, AirSnort, Chopchop, Sorwep, WepAttack, WEPcrack, WepLab and others, which are generally supported by Linux. In the paper FMS attack is descript in detail.

FMS attack (the name according to authors Scott Fluhrer, Itsik Mantin, Adi Shamir) is based on the three basic principles:

1. Some IVs form the cipher RC4 in the manner in which information about the key in input bytes can be disclosed.
2. The weak invariant allows the use the output bits for choosing the most probably bits of key.
3. The first output bits of key we can discover always, because they include the head - line of SNAP (*SubNetwork Access Protocol*).

On the base of catching the couple (weak IV, the first byte of RC4 stream) is able to determinate the secret key.

In the paper the application Aircrack-ng was used for implementation of FMS attacks. AirCrack is WEP and WPA-PSK cracker, which is based on the passwords attack after summarisation of the sufficient number of packets.

The application Aircrack contains three main utilities, used in the three attack phases required to recover the key:

- *airodump*: wireless sniffing tool used to discover WEP-enabled networks,
- *aireplay*: injection tool to increase traffic,
- *aircrack*: WEP key cracker making use of collected unique IVs.

4. Results of Safety Analyses

For testing purpose the network which is illustrated in the Fig. 2 was realised.

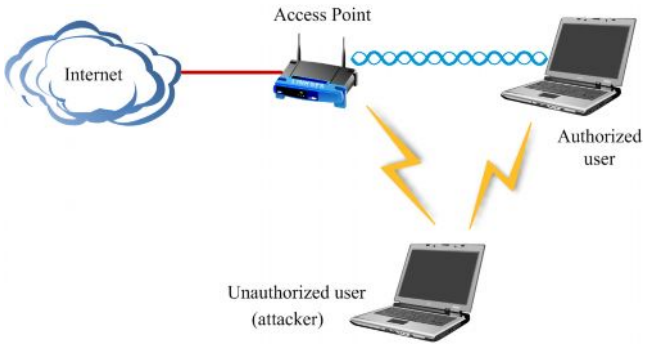

Fig. 2: Realised wireless network.

The testing was realised in the monitoring mode of attacker wireless card. The attack can be specified as passive attack, because it is no able to observe on the authorised network operation side. The attack was realised in the following steps:

1. Initialization of wireless network interface card to monitor mode by tool Airmon-ng:

```
root@bt:~# airmon-ng start wlan0
```

2. Find all the wireless networks via application Airodump-ng from package of programme Aircrack-ng (see the Fig. 3):

```
root@bt:~# airodump-ng mon0
```

3. Determining the network for breaking of WEP password. Wireless network iWLAN was created for this test (the name of tested network was iWLAN):

```
root@bt:~# airodump-ng -w wep -c
11 --bssid 00:02:72:64:7B:74 mon0
```

Testing was realised for two examples:

- the use of 64-bits WEP security with 40-bits secret key (see the Fig. 4),
- the use of 128-bit WEP security with 104-bits secret key (see the Fig. 5).

4. The increase of network traffic in network iWLAN by using tool Aireplay-ng:

```
root@bt:~# aireplay-ng -1 0 -a
00:02:72:64:7B:74 mon0
```

```
root@bt:~# aireplay-ng -3 -b
00:02:72:64:7B:74 mon0
```

5. To break WEP password is possible after catching of sufficient number of frames with different IV only (via application Aircrack-ng):

```
root@bt:~# aircrack-ng wep-01.cap
```

```
CH  3 ][ Elapsed: 3 mins ][ 2010-02-08 08:20

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:02:72:64:7B:74  -49      876      269    0  11  54   WEP  WEP         iWLAN
00:16:B6:DA:0E:3C  -59      352      159    0  13  54   WEP  WEP         KRIS_WiFi
00:18:39:18:71:6B  -65      939      533    7   5  54   OPN              utc-wifi
00:18:39:0B:DA:63  -65      505      820    4  11  54   OPN              utc-wifi
00:4F:62:25:93:C8  -69      899        0    0   6  54   WEP  WEP         UKaI-KPI23
00:18:39:0B:DD:F0  -67      853      535   10   7  54   OPN              utc-wifi
00:16:B6:D9:DF:6B  -73      258      134    0   1  54   WEP  WEP    OPN  KRIS_WiFi
08:10:74:60:EC:9E  -75      321        0    0   6  54   WPA2 CCMP   PSK  default

BSSID              STATION            PWR   Rate    Lost   Packets  Probes

(not associated)   00:21:63:E6:F1:6E  -77    0 - 1      0         1  KRIS_WiFi
(not associated)   00:25:D3:6D:3E:93  -75    0 - 1    104       497  TP-LINK
(not associated)   00:15:00:3B:FB:A7  -82    0 - 1      0        13  KRIS_WiFi
(not associated)   00:22:FD:15:0C:7F  -75    0 - 1      0         4
00:02:72:64:7B:74  00:25:BC:28:64:B1  -33   54 -36      0       295
00:18:39:0B:DA:63  00:1F:5B:C9:38:56  -75   54 - 1      0       549  utc-wifi
```

Fig. 3: The results of the network scan via application Airodump-ng.

```
CH 11 ][ Elapsed: 2 mins ][ 2010-02-08 08:24 ][ 140 bytes keystream: 00:02:72:64:7B:74

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:02:72:64:7B:74  -41  96     1484    21269    0  11  54   WEP  WEP    SKA  iWLAN

BSSID              STATION            PWR   Rate    Lost   Packets  Probes

00:02:72:64:7B:74  00:25:BC:28:64:B1  -38   54 - 1      0     14457  iWLAN
00:02:72:64:7B:74  00:1A:73:6B:9E:CF    0    0 - 1      0     17404
```

Fig. 4: Scan of wireless network iWLAN with 64-bits key.

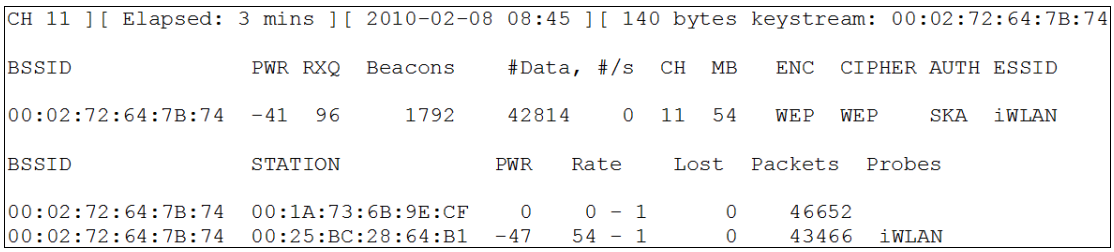

Fig. 5: Scan of wireless network iWLAN with 128-bits key.

Within realisation of FMS attack about hundred frames with weak initialisation vector (IV) was catching. In network with low traffic we can accelerate this by using active reinjection frames or fragmentation attack.

For successful breaking of 64 - bits WEP password (password *kris5*) 21212 frames was catching. In this reason was decryption realised with successful 100 %. The list from application Aircrack-ng is illustrated in Fig. 6.

The practice of breaking 128 - bits WEP password was the similar. In the first the number of catching frames was 25000 and the experiment was unsuccessful. The experiment was repeated and the successfully breaking of WEP password was realised with 42335 frames (password *unizafelkris5*). Decryption was realised with successful 100 %. The list from application Aircrack-ng is illustrated in Fig. 7.

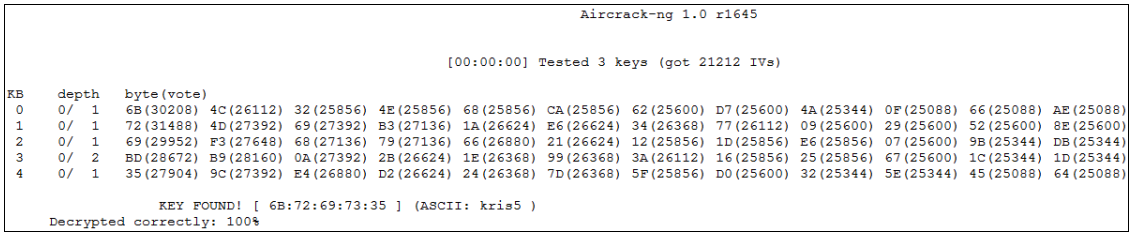

Fig. 6: The successful breaking of 64-bits WEP password via application Aircrack-ng.

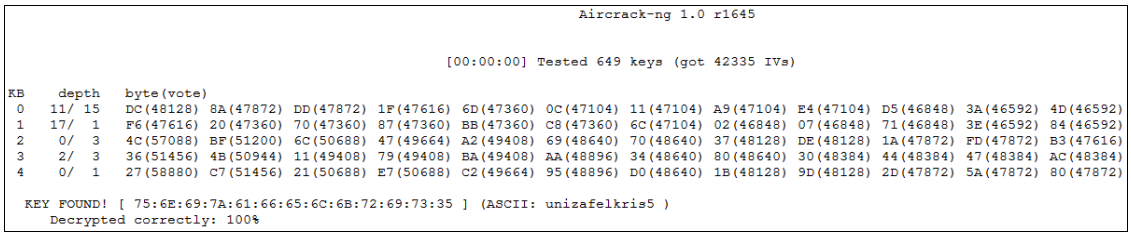

Fig. 7: The successful breaking of 128-bits WEP password via application Aircrack-ng.

5. Conclusion

Resulting from realized cryptanalytic attacks to standard wireless communication we can establish that this system without implementation of additional safety layer does not fulfill the requirements to safety-related communications with increasing value of safety integrity level (SIL 1 – 4). In this system it is necessary to implement the safety mechanisms according to norms relevant for open transmission systems and validate additional safety layer of wireless machine in consideration in required SIL using method illustrated e. g. in [7]. The other solution is Zigbee communication standard [13] using on the base of AES cryptographic standard.

Acknowledgements

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0023/08 “Theoretical apparatus for risk analysis and risk evaluation of transport telematics systems”.

References

[1] IEC 61508. *Functional safety of electrical / electronic / programmable electronic safety-related systems*, 1989.

[2] DZUNG, D.; NAEDELE, M.; VON HOFF, T. P.; CREVATIN, M. Security for Industrial Communication Systems. In: *Proceedings of the IEEE*, VOL. 93, NO. 6, JUNE 2005, p. 1152-1175. ISSN 0018-9219.

[3] LOPEZ, E. E.; MARTINEZ-SALA, A.; VALES-ALONSO, J. Wireless communications deployment in industry: A review of issues, options and technologies. *Computer in Industry* [online], p.29-49. Available at WWW: <www.elsevier.com/locate/compind>. ISSN 0166-3615.

[4] WILLIG, W.; MATHEUS, K.; WOLISZ, A. Wireless Technology in Industrial Networks. In: *Proceedings of the IEEE*, VOL. 93, NO. 6, JUNE 2005. ISSN 0018-9219.

[5] VIEGAS Jr., R.; PORTUGAL, P.; GUEDES, L. A.; VASQUES, F. A Proposal of Real-Time Publish-Subscribe Scheme Compatible with 802.11e Wireless Networks, *IECON 2009*, p. 2393-2398. ISSN 1553-572X.

[6] MACEDO, P.; AFONSO, J. A. Simulation Analysis of IEEE 802.15.4 for Wireless Networked Control Systems. *IECON 2009*, p. 2482-2487. ISSN 1553-572X.

[7] MALM, T.; HÉRARD, J.; BOEGH, J.; KIVIPURO, M. *Validation of safety - related wireless machine control systems.* TR 605, 2007. ISSN 0283-7234.

[8] IEC 61 784-4. *Digital Data Communications for Measurement and Control-Profiles for Functional Safe and Secure Communications in Industrial Networks*, 1998.

[9] *System protection profile for industrial control systems (SPP-ICS) version 1.0*. [online]. 2004. Available at WWW: <www.isd.mel.nist.gov/projects/ processcontrol>.

[10] ISA SP100.11a. *Wireless Systems for Industrial Automation: Process Control and Related Applications*, APRIL 2009.

[11] IEEE 802.11. *IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area network.* Specific requirements. - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[12] *AES* [online] Available at WWW: <http://www.fips-197.com>.

[13] SASTRY, N.; WAGNER, D. *Security considerations for IEEE 802.15.4 networks*. In: *Proceedings 3rd ACM workshop on wireless security*. Philadelphia. USA, p. 32-42. ISBN 1-58113-925-X.

About Authors

Tomas ONDRASINA was born in 1983 in Zilina (Slovakia). He is PhD student in the study programme "Control Engineering". The topic of his PhD. thesis is Safety mechanisms of wireless networks for use in industrial automation.

Maria FRANEKOVA was born in 1961 in Brezno (Slovakia). She received her Assoc. Prof. in 2004 in the field of “Information and Safety-related Systems”. Her research interests include safety data transmission, analysis of safety communication on the base of coding and cryptography tools within safety related applications.