Threats in Networks using Agent and Biometric Systems

Drahanský Martin, Hanáček Petr, Zbořil František sr., Zbořil František jr.,
Maros Barabas and Lukas Antal

[1]*Brno University of Technology, Faculty of Information Technology*
Božetěchova 2, CZ-612 66, Brno, Czech Republic

[1]*{drahan, hanacek, zboril, zborilf, ibarabas, iantal}@fit.vutbr.cz*

Abstract

This article is devoted to description of threats and actual possible attacks on networks (high-speed and wireless), where agent systems and biometric systems are in use.

Keywords: *wireless and high-speed network, agent system, biometric system, threat, attack*

1. Introduction

This article combines three related topics – networks with running agents and biometric devices in this network. Networks could be generally split up into two groups – wire or wireless networks. At the moment, wireless networks are more popular, because they enable mobility to users and their transfer rates are acceptable for the most users. All the networks could be exposed to any type of attack – there exist special types of attacks (threats), which could be found only in networks, nevertheless all devices used in the network should comply with criteria for trusted and secure device. In the second chapter, we describe all known specialized types of attacks, which could be realized in networks, where our focus is oriented on high-speed and wireless networks, because these two types are the widely used types of networks. In the network area, there could be used software agents, which could be used to different tasks within the network. Nevertheless, these agent systems could be attacked as well (see the third chapter) – in a list with threats we should consider a special type of possible attacks – to agent systems, because they have very special way of life in a network and many attacks differentiate from the known attacks on classic networks without agents. The last part of this paper (fourth chapter) is oriented on biometric systems, which are very often used in a network (data transfer to a central storage, *etc.*) – they serve to an authorization of a genuine user for granting access rights to a network, therefore we described special types of threats, which could be applied to biometric devices (systems) interconnected via a (wire or wireless) network. Agents and biometric systems can coexist in a network area and they should show such strong abilities that they can resist against attacks and do not decrease the security of the whole network.

2. Threats and Possible Attacks in Networks

In this section of wireless network attacks classification we present the chosen attacks on *Wired Equivalent Privacy* (WEP), *Lightweight Extensible Authentication Protocol* (LEAP), *Hole 196* attack on *Wi-Fi Protected Access II.* (WPA2), and one of the latest, attack on *Wi-Fi Protected Setup* (WPS). Following these sections we provide classification of attacks into five classes based on the final result achieved by a particular attack concluded with the table of classified attacks on wireless networks.

2.1 WEP vulnerabilities and attacks

Protocol *Wired Equivalent Privacy* (WEP) has become the first security mechanism for data encryption within wireless Wi-Fi connections since 1997. The WEP protocol uses symmetric stream Rivest Cipher 4 (RC4) for data encryption, which takes place on the L2 layer of ISO/OSI model. The protocol supports the use of 40-bit or 104-bit shared keys. The shared key is during the encryption or decryption concatenated with 24-bit value of initialization vector for creating 64-bit or 128-bit WEP key. By encrypting with WEP, a 32-bit control checksum (*i.e.*, Integrity Check Value – ICV) is created. The WEP key, composed of a shared key and initialization vector, is the input of stream cipher RC4 and the output is pseudorandom sequence called Keystream.

The first WEP vulnerability went public in 2001 in Intercepting Mobile Communications article – see [8]. Ian Goldberg warned against several deficiencies within the design of RC4 stream cipher, which allow to break integrity and confidentiality of encrypted communication. In the same year it was also published the statistical method based on the presence of weak initialization vectors and their repetition in the RC4 cipher, theoretically describing the possibility of finding the shared key [16].

This method, called *Fluhrer, Mantin, and Shamir* (FMS), was in 2002 practically used for compromising the WEP shared key. This method required the capture of more than one million packets [27]. In 2004 a security researcher with the nickname KoreK published an improvement of the previous method in which the compromising of the WEP keys suffices roughly 500,000 packets. In 2007 the trio of scientists Pychkine, Tews, and Weinmann provided optimizations, which requirement for a successful compromise has only about 60,000 packets [28]. Besides the improvements of statistical methods, a number of methods to generate traffic in order to speed up the collection of the required number of packets have been published. These attacks were named ARP Injection, Fragmentation Attack, KoreK Cochchop, Hirte and Caffe Latte. Currently, there are a number of tools that automate the attacks against WEP keys and allow the attack to make even less experienced individuals without the need to know the details or the principle of the attack.

The reaction to the weaknesses of WEP protocol was several adjustments to improve the encryption algorithms, increasing the IVs space to 128 bits and elimination of weak IVs [9]. None of this improvements and changes was standardized and it is currently recommended to use the WPA protocol as a replacement for WEP.

2.2 Hole 196 attack on WPA2

Hole 196 vulnerability affects the 802.1i standard, also known as WPA2. The attack is unique in the need of an attacker being authenticated within the network, WPA2 is currently considered safe as regards the resistance of an external attack. In the case of an attack within the network from other authenticated user, the risk already does exist.

Unlike the WEP, WPA2 has a hierarchy of encryption keys. On the top of this hierarchy is Pre-shared Key. Depending on the type of WPA network used (Home vs. Enterprise), the key is used to derive the Pairwise Master Key (PMK), which is then used to derive the Pairwise Transient Key (PTK). The PTK key is unique to each client. Unlike the WEP, communications between the AP and various clients are encrypted by different keys.

In case of broadcasting, it would be ineffective to forward the same communication to all clients, each encrypted with a different key. For this reason, standard 802.1i defines the Group Transient Key (GTK), which is shared by all connected clients. The standard specifies that the key is used for encryption of AP communication and for decryption on the client side. But the problem is, that the opposite situation is not explicitly defined and prohibited, it is

only mentioned on the 196th page of the standard, which is the reason for its name. An attacker with small wireless card driver adjustments can broadcast messages so they look like they are from access point [30].

This design flaw allows an attacker within the network to carry out attacks such as ARP Poisoning, Denial of Service, or DNS Spoofing, ultimately to become a man in the middle between the client and the access point transparently. This attack starts by an attacker, who sends to a broadcast (or to a particular user only) an ARP frame indicating that he became the default gateway on the network. This frame is encrypted by GTK key, therefore every client believes it is a frame sent by the AP. As soon as the victim starts sending packets encrypted by its PMK key, the communication is decrypted by AP and encrypted again by attackers PMK key. An attacker is in the middle of the communication able to eavesdrop all packets unencrypted. This attack is completely undetectable from the AP perspective.

The defense against this attack may be the use of the AP isolation functionality, where individual clients of wireless network are connected to a separate VLANs without seeing each other. Another method of defense may be the deployment of monitoring adverse changes in the ARP table on clients.

2.3 The LEAP Vulnerability

The LEAP method of EAP protocol within 802.11x standard is a proprietary method published by Cisco Systems. The clients are authenticated to the network with their username and password. The password is not transmitted in plaintext, but a modified MS-CHAPv1 protocol is used.

In August 2003, Joshua Wright presented susceptibility of LEAP method to offline dictionary attack. Almost every authentication method based on the credentials when using weak passwords are vulnerable to this attack, but the vulnerability in the LEAP protocol causes a significant reduction of time needed for this attack. For successful attack, the attacker must first capture the LEAP communication of authorized client. The process of authentication in the LEAP protocol works on the principle of challenge-handshake and it is based on the algorithm of Microsoft MS-CHAPv1. Description of this protocol follows [25]:

1. The authenticator sends 8-byte challenge string to the client.
2. The client creates 16-byte NT hash of the password used for 3DES key generation as follows:
   - Key 1 = NT1 – NT7
   - Key 2 = NT8 – NT14
   - Key 3 = NT15 – NT16 + ”\0\0\0\0\0”
3. Each of the keys is encrypted challenge string, the output are three 8-byte strings.
4. The client sends concatenation of these strings (24 bytes) to authenticator as challenge-response string.
5. The authenticator based on received challenge-response string decides whether the client is successfully authenticated.

The security problem is the way how the third DES key is created. The key is 7 bytes long, but the last 5 bytes are always constant (bytes with zero value). Brute force attack on DES with 16-bit key consists of only 65,536 options. By breaking the third encryption key, it is able to get the last two bytes almost in constant time (above labeled as NT15 and NT16) of

the NT password hash.

In the next phase it is necessary to convert the password dictionary to dictionary containing only NT hashes of passwords. Since there is no salting material within the NT hash, it is possible to have these dictionaries prepared. This file is then filtered by NT hashes ending with two characters that have been found in the previous phase. This will massively reduce possible matches as it is shown in Table 1. From each of the vocabulary was randomly selected one record and the dictionary was filtered by the last two bytes of the NT hash.

Table 1. Reduction of key state

Dictionary	Number of records	After filtering
darkC0de.lst	1,707,659	24
Ispell English Wordlist	74,158	2
AlphaNum 6char	308,915,776	267

The last step is the classic dictionary attack on MS-CHAPv1 algorithm only using passwords from a dictionary whose NT hash ends by two identified characters. The user password can be found by matching the NT hash with the main dictionary. The username is open as it is contained in the EAP-Identity-Response packet. It is recommended to use other methods like PEAP, EAP-TLS or EAP-FAST instead of LEAP [6].

2.4 Attacks on WPS

The WPS (WiFi Protected Setup) technology is used for an easy configuration of wireless clients. At the end of 2011 a serious vulnerability was discovered that dramatically reduces the time required to perform online brute-force attack on WPS [29]. The client authenticates using WPS to the AP by sending 8-digit PIN. If the PIN is correct, the client is sent WEP/WPA/WPA2 key to log on to the network. It is evident that the WPS vulnerability also applies to networks that use the recommended encryption using WPA2-CCMP.

The worst case of online brute-force attack on 8-digit PIN takes 10^7 combinations (8^{th} digit is a checksum). If we take into account that the online PIN verification lasts about 1 second, it will take approximately 115 days to exhaust the entire space. But the vulnerability lies in the fact that before sending, the entire PIN is divided into two four-digit numbers, and these numbers are sent and verified separately. This vulnerability reduces the space to 10^4+10^2 possibilities which is practical reduction to couple of hours.

For a secure deployment of SOHO Wi-Fi network it is recommended in addition to using WPA2 also to disable WPS.

2.5 Summary

In this section we provide a brief description of wireless attacks categorization principles we used for the classification (see Table 3). The section is concluded with the table of existing wireless attacks classified to describe the categories based on achieved results of the particular attack and its principles (see Table 2).

Table 2. Classification of attacks on wireless networks

Attack	Target	Classification	Mitigation
ARP Injection	WEP	Traffic generation	Use WPA instead
Fragmentation attack	WEP	Traffic generation	Use WPA instead
KoreK Cochchop	WEP	Traffic generation	Use WPA instead
Hirte	WEP	Traffic generation	Use WPA instead
Caffe Latte	WEP	Traffic generation	Use WPA instead
FMS	WEP	Obtaining secrets	Use WPA instead
Handshake brute-force	WPA-PSK, WPA2-PSK	Obtaining secrets	Use strong pass-phrase
Teck-Bews, Ohigashi-Morii	WPA-PSK	Others	Use WPA2 with CCMP instead
Hole 196	WPA-PSK, WPA2-PSK	Man in the Middle	In multiuser environment use Enterprise WPA
WPS vulnerability	WPS	Obtaining secrets	Disable WPS
EAP brute-force	LEAP, EAP-MD5	Obtaining secrets	Use PEAP or EAP-TLS instead
Wi-Fi Deauthentication & DoS	All	Deauthentication / DoS	Employ WIDS
Rogue AP (AP impersonalization)	All	Man in the Middle	Employ WIDS

Table 3. Category of results achieved by a particular attack

Threat	Description
Traffic generation	A threat / category which goal is to obtain the largest set of communication packets for further analysis and attacks. This set is can be used for offline statistical attacks on the WEP protocol.
Obtaining secrets	A type of attacks that lead to obtaining shared passphrase or user specific key which results in full access to a wireless network.
Man in the Middle	An attacker can sniff and decrypt data from other authorized users within the network.
Deauthentication / DoS	An attempt to make a machine or network resource unavailable to its intended users or isolated from resources [2].
Others	This category contains theoretical attacks and proof of concepts of security vulnerabilities.

3. Threats and Possible Attacks on Agent Systems

Threats and possible attacks on multi-agent systems (MAS), as on many other systems, come out from possible exploitation of vulnerabilities of these systems and they are similar to these mentioned in the previous chapter. Threats and attacks on MAS can be categorized from different points of view, *e.g.*, good three-layer taxonomy was proposed by Bijani and Robertson [3]. The main threats are there categorized to those that relate to agent's integrity, confidentiality of agent code, and authenticity of agents, their services and roles. In this paper, we will focus on three problems: problem of secure interpretation of mobile agents at a host platform, communication between guarding agent and control center, and possible malicious attacks to the intention based agents on a FIPA platform.

3.1 Security threats in mobile agent systems

As a special point of view let us examine usage agents as mobile codes in a distributed system. We may, for example, take wireless sensor networks as the referencing systems and put agents there. Which threats may appear in such systems was discussed in [31]. In general agents work on a platform where they are interpreted and both, agent and platform may mean threat to another. If we consider agent in the form of an interpretable agent code to be possible threat to the platform, we may find three such threats.

- *Resource wasting* – proper interpretation of agent code may lead to unfair usage of platform resources by the agent.
- *Spying* – agent tries to discover information that is private to the platform and agent does not provide these data to possibly unreliable platform.
- *Agent masquerade* – agent pretends that its purpose is different than it really is.

By contrast an agent that resides on a platform may be endangered by invalid or malicious platform. These threats may be described as follows:

- *Eavesdropping of Agent Code* – platform may analyze the agent code and capture agent private data.
- *Modification of Agent Code* – platform substitutes part of agent code and changes its behavior.
- *Improper Execution of Code* – an interpreter that executes agent code on a platform may improper execute some agent actions that may cause improper agent behavior.
- *False Service Outputs* – platform may provide service that produces incorrect results. Agent is then confused by these results and consequently to behave irrationally.
- *Incorrect Transport* – agent is not transported to a desired node or platform as it requests and then behaves as it was the originally intended platform.

Some of these points relate together. Transportation of agent is a kind of platform service and execution of agent code may be understood as a modification of agent code at the agent platform. But after the agent code is transformed to another, possibly reliable platform, agent is then interpreted correctly. So although its code has not been modified, the new hosting platform may exploit agent for a purpose that is not intended by the agent.

In [13] the security issues and their solutions were classified as possible, impossible, and hardly possible. Among impossible tasks to solve belong correct agent code interpretation, confidentiality of agent data and transport of agents. Other threats may be solved but some of them like authorization of an agent etc.

3.2 Security threats in communicating agent system

As an illustration of possible threats in an agent system let us considered a group of agents, *e.g.*, intelligent sensors, whose task is a protection of boundaries of some locality (building, field, forest, region, etc.). An enemy may be either agent or a group of agents, and these agents may be as fake technical or program objects so persons (from pilferers of fruits or Christmas trees to terrorists).

Structure of such system is simple. Agents monitor a boundary of guard locality and each of them is responsible for given part of this boundary. If some agent detects that the boundary is violated it sends information about this to the control center, only. The center thereafter solves this situation, but countermeasures are not objects of this paper.

Complexity and intelligence of agents may be various. Simplest of them may have motion detectors and very simple communication algorithm for communication with the center only, on the other hand complex intelligent agents may use special sensors as cameras for night vision, thermo-cameras, shake sensors, *etc.* and they can themselves interpret detected object. They can, *e.g.*, distinguish between wild animals and persons or cars.

From the first point of view may be seen that it is a simple problem, but contrary is true. Enemies can do many various hostile actions. Most important threads and attacks are as follows:

- *Eavesdropping of formerly eavesdropped messages*. Eavesdropping is the basic activity of an enemy. From messages he/it can probe a technique and range of the protection of the given region boundary, i.e. what (motion, temperature, sound, *etc.*) and within what range the individual agent detect, as well how the center react and which counter-measures are made. The main task of this attack is the localization of usually stationary guarding agents.
- *Repetition of formerly eavesdropped messages*. Repetition of formerly eavesdropped messages is usually used when the enemy cannot decode eavesdropped messages. Then he/it can reason to the technique and range of the given boundary protection from activities of the center on repeated messages. The enemy can provoke the communication between the agent and the center by pseudo-disturbing of guarded boundary.
- *Jamming* is the next and relatively simple way, how knock out the protection of the given region. If the agent cannot communicate with the center, the probability of the attack successfulness increases
- *Masquerading/Faking* (passing itself off as proper agent). Faking assumes that the enemy infiltrates into principles of the protection (*e.g.*, on the basis of eavesdropping) and it knocks out some guarded agent – then it can fake that he/it is proper agent and confuse center by fake messages.
- *Theft or destroying of agent*. Theft or destroying of agent is the simplest way, how to knock out protection of (part of) the region/boundary. This attack evidently assumed that some guarded agent was localized (*e.g.*, again on the basis of eavesdropping). Next threat of the theft of the agent is the possibility that the enemy by analysis of the stolen agent obtains algorithms and cryptographic keys. Then he/it is able pursue next attacks, first of all next eavesdropping and faking.

3.3 Security threats in FIPA based and intention-based agents

Because agents are mostly a complex reasoning system, we may identify some threats that are common to them. We may consider an agent to be a social element inside a multiagent system which behavior might be modified by interaction with other agents. In this section we suppose that the agents are interpreted on a FIPA compliant platform and interaction is made in the form of communication among agents in the Agent Communication Language specified by the FIPA [15] according to a mutually shared communication protocol. In general a threat is that a message is false, that correspond to the taxonomical approach of Bijani and Robertson. So the threat is, in general, to send a message that carries false content. As the communication is passed on speech acts, then these messages may have different impacts on receiver mental states. We explain possible threats as possible wrong behavior of a participant in a communication process.

As the main problems we have identified the following agent protocols – contract net, brokering, subscribing, English auction and Dutch auction. With respect to these protocols we may identify following unfair behavior of agents that are part of the communication processes.

- *Making a false auctions* – illegal usage of "call for proposals" speech act as a starting act of the contract net protocol or some auction protocol may cause that participants waste a time on doing a communication that may have no effect.
- *Proposal of unfair bid* – auctions and contract nets are basic protocols of multiagent systems. These protocols are used during negotiating about resources, services and conflict solving agreements. Making false proposals may lead to invalid result of the negotiation process.
- *Provision of false service offers* – an agent may register a service that it is not willing to perform. Such registration may lead to incorrect brokering efforts and that the agreed deal between service provider and the client leads to wrong or none service performance.
- *Provision of false service results* – an agent had completed successfully or unsuccessfully requested service but then provides wrong information about the service results.
- *Invalid brokering* – a broker informs incorrectly a recruited agent about real demands of the client agent. Both, client and recruited agent are then doing and expecting different services.

Intelligent agents are mostly based on mental-state principles and their main representatives are the BDI agents [23] together with agents based on Agent Oriented Programming [26]. Because the second are not supported much today we put focus on the BDI systems and we study possible wrong behavior of such agent when it accepts a message that's content is not correct.

Behavior of such systems is driven by an intention that has been chosen as a goal that is achievable. The intention is selected on the basis of the actual belief of the agent. If a sender sends a false message then any of the mental state of the agent may become incorrect. In the following point we summarize how particular mental states can be corrupted when agent accepts an incorrect message.

- *Provision of false belief* – a speech act type "inform" adds a belief to an agent base with a notation of sender's identity. If false belief is accepted by the re-

ceiver, then it may cause selection of unusable plans as applicable means and thus cause an irrational behavior of agent.

- *Pursuit of non-desired intention* – if an agent receives a false goal to achieve it may consequently find a plan as a mean for that goal. Such mean is then a part of new intention of the agent and agent then behaves toward this false goal.
- *Provision of incorrect know-how* – each intention is followed by perforation of a plan. In BDI-based systems like JASON [5] agents may send their plans as a knowledge how to reach a goal. Receiver may then use such plans when it is suitable means for goal achievement.

3.4 Summary

Security threats in multiagent systems may be observed from several different points of view. Agents are mobile codes as well as autonomous communicating entities, entities that communicate with protocol described in FIPA standards as well as they often are systems based on mental states and reasoning on BDI principles. In this chapter we described main security issues in these systems and presented main threats to agent's security.

4. Threats and possible attacks on biometric systems

Biometric systems [18, 4] are based on recognition of different human physiological or behavioral characteristics. The most often used technologies are the following: fingerprint, face, eye iris, hand geometry, voice, gate and some others. These systems are generally connected to any kind of a network (LAN, WLAN, BlueTooth, *etc.*) and could be attacked like all other devices used in the network – therefore all these devices have to meet the criteria for secure network devices (trusted device). Anyway, the threats to biometric systems have some special possibilities, which are listed below.

The functionality of such systems is influenced not only by the used technology, but also by the surrounding environment (including, *e.g.*, skin or other diseases). Biased or damaged biometric samples could be rejected after revealing their poor quality, or may be enhanced, what leads to the situation that samples, which would be normally rejected, are accepted after the enhancement process. But this process could present also a risk, because the poor quality of a sample could be caused not only by the sensor technology or the environment, but also by using an artificial biometric attribute (imitation of a finger(print)). Such risk is not limited just to the deceptional technique, but if we are not able to recognize whether an acquired biometric sample originates from a genuine living user or an impostor, we would then scan an artificial fake and try to enhance its quality using an enhancement algorithm. After a successful completion of such enhancement, such fake fingerprint would be compared with a template and if a match is found, the user is accepted, notwithstanding the fact that he can be an impostor! Therefore the need of careful liveness detection, *i.e.*, the recognition whether an acquired biometric sample comes from a genuine living user or not, is crucial.

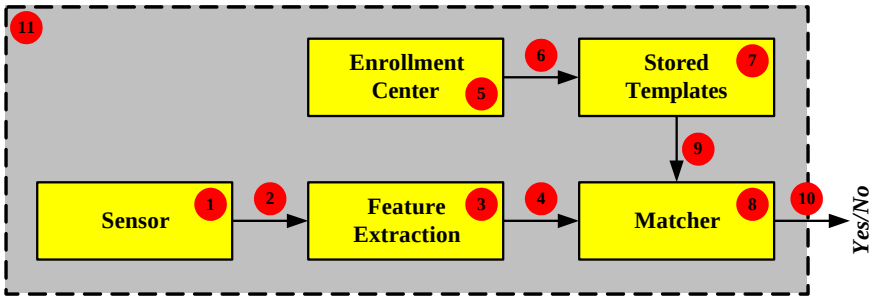

Figure 1. Basic components of a biometric system.

Each component of a biometric system presents a potentially vulnerable part of such system. The typical ways of deceiving a biometric system are as follows (Figure 1) [11, 19, 1, 17]:

1. *Placing fake biometrics on the sensor*. A real biometric representation is placed on the device with the aim to achieve the authentication, but if such representation has been obtained in an unauthorized manner, such as making a fake gummy finger, an iris printout or a face mask, then it is considered as a deceiving activity.
2. *Resubmitting previously stored digitized biometric signals* (*replay attack*). A digitized biometric signal, which has been previously enrolled and stored in the database, is replayed to the system, thus circumventing the acquisition device.
3. *Overriding the feature extraction process*. A pre-selected template is produced in the feature extraction module using a Trojan horse.
4. *Tampering with the biometric feature representation*. During the transmission between the feature extraction and matching modules, a fraudulent feature set replaces the template acquired and processed by the device.
5. *Attacking the enrollment center*. The enrollment module is also vulnerable to spoof attacks such as those described in the previous points 1 to 4.
6. *Attacking the channel between the enrollment center and the database*. During the transmission, a fraudulent template replaces the template produced during the enrollment.
7. *Tampering with stored templates*. A template, previously stored in the database (distributed or not), can be modified and used afterward as corrupted template.
8. *Corrupting the matcher*. A pre-selected score is produced in the matching extraction module using a Trojan horse.
9. *Attacking the channel between the stored templates and the matcher*. During the transmission between the database and the matching module, a fraudulent template replaces the template previously stored.
10. *Overriding the final decision*. The result of the decision module can be modified and then used for the replacement of the output obtained previously.
11. *Attacking the application*. The software application can also be a point of attack and all possible security systems should be used to reduce the vulnerability at this level.

From the above list of possible attacks we can deduce that most security risks or threats are quite common and could be therefore resolved by traditional cryptographic tools (*i.e.*, encryp-

tion, digital signatures, PKI (*Public Key Infrastructure*) authentication of communicating devices, access control, hash functions etc.) or by having vulnerable parts at a secure location, in tamper-resistant enclosure or under constant human supervision [20].

Now we can described some troubles in biometric systems based on fingerprint recognition, because they are the most widely spread systems. When a legitimate user has already registered his finger in a fingerprint system, there are still several ways how to deceive the system. In order to deceive the fingerprint system, an attacker may put the following objects on the fingerprint scanner [22, 1, 24]:

- *Registered* (*enrolled*) *finger*. The highest risk is that a legitimate user is forced, *e.g.*, by an armed criminal, to put his/her live finger on the scanner under duress. Another risk is that a legitimate user is compelled to fall asleep with a sleeping drug in order to make free use of his/her live finger. There are some deterrent techniques against similar crimes, *e.g.*, to combine the standard fingerprint authentication with another method such as a synchronized use of PINs or identification cards; this can be helpful to deter such crimes.

- *Unregistered finger* (*an impostor's finger*). An attack against authentication systems by an impostor with his/her own biometrics is referred to as a non-effort forgery. Commonly, the accuracy of authentication of fingerprint systems is evaluated by the false rejection rate (FRR) and false acceptance rate (FAR) as mentioned in the previous chapters. FAR is an important indicator for the security against such method (because a not enrolled finger is used for authentication). Moreover, fingerprints are usually categorized into specific classes [7]. If an attacker knows what class the enrolled finger is, then a not enrolled finger with the same class (*i.e.*, similar pattern) can be used for the authentication at the scanner. In this case, however, the probability of acceptance may be different when compared with the ordinary FAR.

- *Severed fingertip of enrolled finger*. A horrible attack may be performed with the finger severed from the hand of a legitimate user. Even if it is the finger severed from the user's half-decomposed corpse, the attacker may use, for criminal purposes, a scientific crime detection technique to clarify (and/or enhance) its fingerprint.

- *Genetic clone of enrolled finger*. In general, it can be stated that identical twins do not have the same fingerprint, and the same would be true for clones [22]. The reason is that fingerprints are not entirely determined genetically but rather by the pattern of nerve growth in the skin. As a result, such pattern is not exactly the same even for identical twins. However, it can be also stated that fingerprints are different in identical twins, but only slightly different. If the genetic clone's fingerprint is similar to the enrolled finger, an attacker may try to deceive fingerprint systems by using it.

- *Artificial clone of enrolled finger*. More likely attacks against fingerprint systems may use an artificial finger. An artificial finger can be produced from a printed fingerprint made by a copy machine or a DTP technique in the same way as forged documents. If an attacker can make then a mold of the enrolled finger by directly modeling it, he can finally also make an artificial finger from a suitable material. He may also make a mold of the enrolled finger by making a 3D model based on its residual fingerprint. However, if an attacker can make an artificial finger which can deceive a fingerprint system, one of the countermeasures against such attack is obviously based on the detection of liveness.

- *Others*. In some fingerprint systems, an error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. Some attackers may use such error to deceive the system. This method is well known as a "fault based attack" (*e.g.*, denial of service), and may be carried out by using one of the above mentioned techniques. Furthermore, a fingerprint image may be made protruding as an embossment on the scanner surface, if we spray some special material on such surface.

Many similar attacks are documented in the literature, including all the above mentioned types. One example of the attack on fingerprint technology has been presented in [21]. Hackers in the club-magazine "Die Datenschleuder" (4,000 copies in one edition) have printed a fingerprint of the thumb from the right hand of the German minister of the interior – Dr. Wolfgang Schäuble, and invited readers to make a fake finger(print) of the minister and to try to pretend that their identity is those of the minister. This could be considered as a bad joke, as a fingerprint also serves as a conclusive proof of a person's identity. A hacker has acquired this fingerprint from a glass after some podium discussion. Nevertheless, biometric travel documents (issued in Germany starting from 2007, issued in the Czech Republic from 2009), enforced not only by Dr. Schäuble, should be protected just against this situation. The implementation of fingerprints into the travel documents was prescribed by a direction of the European Union in 2004.

It is clear from [22] that the production of a fake finger(print) is very simple [12]. Our own experiments have shown that to acquire some images (*e.g.*, from glass, CD, film or even paper) is not very difficult and, in addition, such image could be enhanced and post-processed, what leads to a high-quality fingerprint. The following production process of a fake finger(print) is simple and can be accomplished in several hours. After that, it is possible to claim the identity as an impostor user and common (nearly all) fingerprint recognition systems confirm this false identity supported by such fake finger.

Therefore, the application of liveness detection methods is a very important task, and should be implemented (not only) in all systems with higher security requirements, such as border passport control systems, bank systems, *etc*. The biometric systems without the liveness detection could be fooled very easily and the consequences might be fatal.

References

[1] P. Ambalakat, "Security of Biometric Authentication Systems", In: 21st Computer Science Seminar, SA1-T1-1, **(2005)**, pp. 7.
[2] B. Aslam, M. H. Islam and S. A. Khan, "802.11 disassociation DoS attack and its solutions: A survey", Proceedings of the First Mobile Computing and Wireless Communication International Conference, **(2006)**, MCWC, IEEE, pp. 221-226.
[3] S. Bijani and D. Robertson, "A review of attacks and security approaches in open multi-agent systems", Springer, **(2012)** May 16.
[4] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha and A. W. Senior, "Guide to Biometrics", Springer-Verlag, **(2004)**, pp. 364, ISBN 0-387-40089-3.
[5] R. H. Bordini, R. F. Hubner and M. Wooldridge, "Programming Multi-Agent Systems in AgentSpeak Using Jason", John Wiley and Sons, **(2007)**.
[6] Cisco Response to Dictionary Attacks on Cisco LEAP. 2003, [online-cit. 2011-05-02]. http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html.
[7] C. G. Collins, "Fingerprint Science", Copperhouse/Atomic Dog Publishing, **(2001)**, pp. 192, ISBN 978-0-942-72818-7.
[8] N. Borisov, I. Goldberg and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11", In Proceedings of the 7th annual international conference on 81 Mobile computing and networking, biCom '01, New York, USA, ACM, **(2001)**, pp. 180-189, ISBN 1-58113-422-3,

http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.
[9] S. Chandramathi, K. V. Arunkumar, S. Deivarayan, *et al.*, "Modified WEP key management for enhancing WLAN security", International Journal of Information Communication Technology, vol. 1, no. 3/4, **(2008)**, pp. 437–452, ISSN 1466-6642.
[10] Y. Demchenko, L. Gommans, C. de Laat and B. Oudenaarde, "Web Services and Grid Security Vulnerabilities and Threats Analysis", Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, **(2005)**.
[11] D. Dessimoz, J. Richiardi, C. Champod and A. Drygajlo, "Multimodal Biometrics for Identity Documents", Research Report, PFS 341-08.05, Version 2.0, Université de Lausanne & École Polytechnique Fédérale de Lausanne, **(2006)**, pp. 161.
[12] M. Drahanský, "Fingerprint Recognition Technology: Liveness Detection", Image Quality and Skin Diseases, Habilitation thesis, Brno, CZ, **(2010)**, pp. 153.
[13] W. M. Farmer, J. D. Guttman and W. Swarup, "Security of mobile agent: Issues and requirements", In Proceedings of the 19th National Information Systems, **(1996)**.
[14] FIPA Abstract Architecture Specification, http://www.fipa.org/specs/fipa00001/SC00001L.html.
[15] FIPA ACL Message Structure Specification, http://www.fipa.org/specs/fipa00001/SC00001L.html.
[16] S. R. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", In Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, SAC '01, London, UK, Springer-Verlag, **(2001)**, pp. 24, ISBN 3-540-43066-0, http://aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf.
[17] J. Galbally, J. Fierrez and J. Ortega-Garcia, "Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection", Biometrics Recognition Group, Madrid, Spain, **(2007)**, pp. 8.
[18] A. K. Jain, P. Flynn and A. A. Ross, "Handbook of Biometrics", Springer-Verlag, **(2008)**, pp. 556, ISBN 978-0-387-71040-2.
[19] A. K. Jain, "Biometric System Security", Presentation, Michigan State University, **(2005)**, pp. 57.
[20] M. Kluz, "Liveness Testing in Biometric Systems", Master Thesis, Faculty of Informatics, Masaryk University Brno, CZ, **(2005)**, pp. 57.
[21] LN: Němečtí hackeři šíří otisk prstu ministra (German Hackers Distribute the Minister's Fingerprint), Lidové noviny (newspaper), **(2008)** March 31.
[22] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems", In: Proceedings of SPIE, vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, **(2005)**, pp. 11.
[23] A. S. Rao and M. P. Georgeff, "BDI Agent: From Theory to Practice", In: Proceedings of the 1st Conference of Multiagent Systems, **(1995)**.
[24] C. Roberts, "Biometric Attack – Vectors and Defences", **(2006)**, pp. 25.
[25] B. Schneier, D. Wagner, "Mudge: Cryptanalysis of Microsoftİs PPTP Authentication Extensions (MS-CHAPv2)", In Proceedings of the International Exhibition and Congress on Secure Networking – CQRE (Secure), London, UK, Springer-Verlag, **(1999)**, pp. 192-203, ISBN 3-540-66800-4.
[26] Y. Shoham, "Agent Oriented Programming", In: Artificial Intelligence, vol. 60, **(1992)**, pp. 51-92.
[27] A. Stubblefield, J. Ioannidis, A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", In NDSS, The Internet Society, **(2002)**, ISBN 1-891562-14-2, 1-891562-13-4.
[28] E. Tews, "Attacks on the WEP protocol", Cryptology ePrint Archive, Report 2007/471, **(2007)**.
[29] S. Viehböck, "Brute Forcing Wi-Fi Protected Setup", **(2011)**, http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.
[30] WPA 2 Hole196 Vulnerability, **(2010)**, http://www.airtightnetworks.com/fileadmin/pdf/WPA2-Hole196-vulnerability-FAQs.pdf.
[31] F. Zbořil, M. Drahanský, P. Hanáček and J. Horáček, "Security in Wireless Sensor Networks with Mobile Codes", Threats, Countermeasures, and Advances in Applied Information Security, Hershey, US, IGI Global, **(2012)**, ISBN 978-1-4666-0978-5.

Acknowledgements

This research has been realized under the support of the following grants: "*The IT4Innovations Centre of Excellence*" – IT4I-CZ 1.05/1.1.00/02.0070 (CZ), "*Security-Oriented Research in Information Technology*" – MSM0021630528 (CZ).

Authors

Martin Drahanský graduated in 2001 at the Brno University of Technology, Faculty of Electrotechnics and Computer Science in Czech Republic. He achieved his Ph.D. grade in 2005 at the Brno University of Technology, Faculty of Information Technology. In 2010 he achieved his Associate professor grade at the Brno University of Technology, Faculty of Information Technology, Department of Intelligent Systems. His research topics include biometrics, security and cryptography, artificial intelligence and sensoric systems. For more information – see please http://www.fit.vutbr.cz/~drahan.

Petr Hanáček is an associate professor at the Faculty of Information Technology at Brno University of Technology. He concerns with information system security, risk analysis, applied cryptography, and electronic payment systems for more than ten years. He is an independent consultant in this area. He is a member of Security@FIT security research group at Brno University of Technology. For more information – see please http://www.fit.vutbr.cz/~hanacek.

František V. Zbořil is an associate professor at the Department of Intelligent Systems, Faculty of Information Technology, Brno University of Technology, Czech Republic. He received his M.Sc. grade in 1968 and Ph.D. grade in 1978 (both in Computer Science) at the same university. His research activities started on analogue and hybrid computers, his next research was focused on classical artificial intelligence and robotics, and now the main objects of his professional interests are soft computing problems. For more information – see please http://www.fit.vutbr.cz/~zboril.

František Zbořil jr. is an assistant professor at the Department of Intelligent Systems, Faculty of Information Technology, Brno University of Technology, Czech Republic. He achieved his Ph.D. grade in 2004 at the Brno University of Technology, Faculty of Information Technology. His major interests include artificial agents, their application in the area of modeling of distributed systems and applications for wireless sensor networks. For more information – see please http://www.fit.vutbr.cz/~zborilf.

Maros Barabas obtained his master's degree from the Faculty of Information Technology, Brno University of Technology in 2009 in the field of computer security. He is currently a Ph.D. student under the supervision of doc. Petr Hanacek. In 2006, he joined the emerging Czech branch of Red Hat, from 2008 he worked in the team aimed at security of Linux systems up to 2011. Since the beginning of 2012, he works as IT Security Consultant at AEC, part of Cleverlance group. In 2009 he joined the Security@FIT security research group at Brno University of Technology. His research is centered on development of malware detection, computer and network security.

Lukáš Antal graduated at the Faculty of Information Technology, Brno University of Technology in 2012. He continues with his studies at Faculty of Information Technology, Brno University of Technology as Ph.D. student under the supervision of doc. Petr Hanáček. His research topics include network security, attack detection and prevention. From 2012 he is a member of Security@FIT security research group at Brno University of Technology. From 2010 he works as IT Security Consultant focused on enterprise penetration testing, security assessment and audit at AEC, spol s .r.o.