Trust in Security of Identification Devices - Feeling of Unity

Břetislav Endrys

bretislav.endrys@monetplus.cz

Monet+, a.s.
Za Dvorem 505
763 14 Zlín-Štípa, Czech Republic

Petr Hanáček

hanacek@fit.vutbr.cz

FIT BUT Brno
Božetěchova 2
612 66 Brno, Czech Republic

Abstract

The article deals with the issue of electronic identity, means for proof of user identity, and means for performing serious personal or legal activities in the electronic world. Even though modern technical means are available, the problem of non-existence of universal user identifier makes the situation unclear. The progress in the area of functionality of present-day technology does not always mean the increasing of security of this technology. In reality it is often on the contrary. Therefore we will show some examples of the impact of increasing capability of new identification devices on their security and that less is often more.

Keywords: identity, smart cards, tamper resistant devices

1 Introduction

When providing security for information system, the issue of user's unique identity often plays a major role. The identity of an entity (typically a person) generally means expressing their identification in the sense of its correlation, i.e. its demarcation towards other entities ([1]). Identification is seen as determining which entity the name specified in a certain context determines and what profile the entity has in the given context. If we talk about the digital identity, we understand it as an electronic record of attributes defining the identity. Identity Management (IDM) is a set of tools for defining entity identity, secure storing of entity information and providing access to this information using standardized interfaces. Nowadays, the basic features of identity management includes:

- centralized administration
- capability of delegating administrative tasks based upon defined roles and rules
- capability of self-handling of users' passwords, without the central administration intervention
- automated activating of the user's environment
- availability of auditing mechanisms and mechanisms for automated generation of reports

Industrial interest groups, such as World Wide Web Consortium (W3C) develop standards which are targeted at identity management in global terms, in which each subject is identified uniquely. Accourding to the W3C Program Statement, identity management must satisfy portability and interoperability requirements ([1]). The ID card holder must be enabled to use such ID card in any application, services and domains. There must be a service displaying generally used identifiers (first names and surnames, birth registration numbers, telephone numbers, e-mail addresses, etc.) on globally applicable user's identification. For transferring statements about identity and authentication, this service must use a universally applicable protocol supporting both hierarchical verification in informal systems with generally structured delegation of verification rights and obligations, and p2p registration models in organically structured communities.

Another problem relating to identity which cannot be resolved until the identity problem is resolved, is the issue of manifestation of the man's will. In some application it is necessary to enable users to demonstrably express and maintain manifestation of their will by which the person (i.e. the user) indicates their intention to perform a certain act. This manifestation of will must be:

- unique in terms of identity and attributes
- capable of expressing the man's will
- undoubtful and auditable (i.e. verifiable by a third party)

The essential problem which we can see is a difficult unity between the human world of non-digital communication in which different mechanisms for identification and manifestation of our will are used (such as name, password, oral or written contract) and the IT world, where digital communication is applied. This digital communication then uses different means for identity verification or manifestation of will, such as electronic signature or other authentication mechanisms. Linking the world of non-digital communication with the world of digital communication is not an easy task (see Figure 1) and consequently additional, reliable means are required.

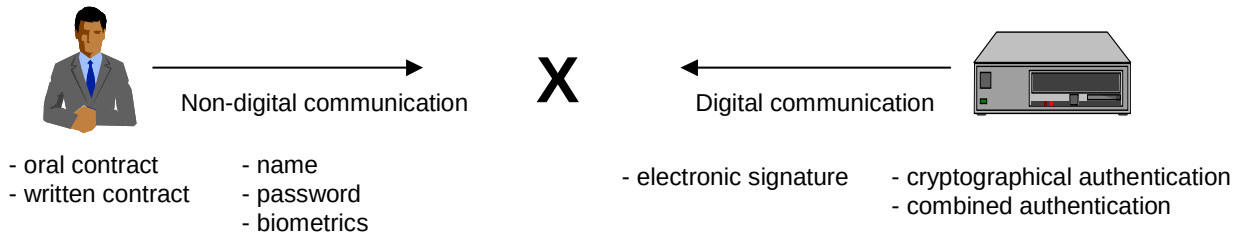

Fig. 1. World of non-digital and digital communication

2 Trusted device

2.1 Who protects whose interests

In order to gain a better understanding of the issue of mobile device security, it is necessary to look closely at the interests of the parties involved and at the persons defending these parties. Let's imagine a system which uses e.g. a mobile phone for communication and for performing payment operations with a bank. Three parties are involved in such system (a user, mobile operator and bank) which communicate to each other using multiple devices and whose task is to execute a payment in this system. These three entities, however, pursue completely different and, in principle, contradictory interests. The main part of the transaction is carried out by a mobile telephone. Whose interests does the telephone protect? The user's, operator's or the bank's interests?

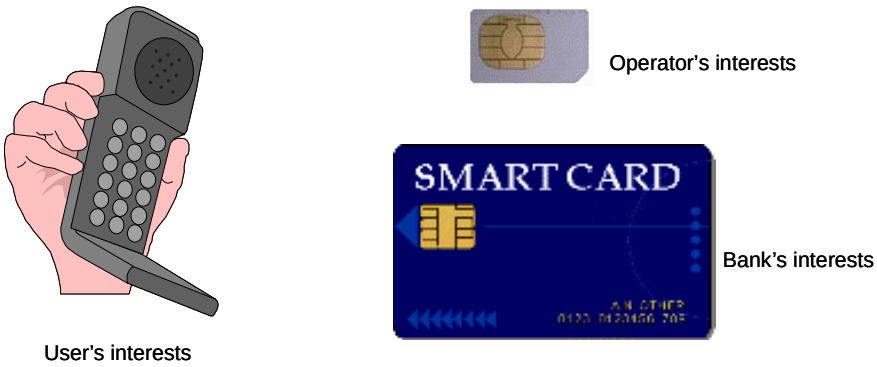

Fig. 2. Whose interests do the devices protect? Čí zájmy hájí různá zařízení

Naturally, it has to protect the interests of all the three parties involved, however in a different manner. In particular, it has to protect the user's interests because the user is its owner and if the telephone did not protect

his/her interests, the user would ditch it. At the same time, it has to protect securely both the operator's and the bank's interests. Since the telephone is owned by the user, we have to find a means enabling the telephone to provide remote protection of the interests of the non-present operator and the bank. For this purpose the telephone has to have a device which is secure for the user and which makes it possible that other parties' interests are protected in the telephone. This device is a *SIM module* in mobile telephones (SIM stands for Subscriber Identity Module) which is basically a smart card. This SIM module plays the role of „*secure hardware*" in the mobile telephone.

3 „Secure hardware" mechanism

The concept of tamper resistant hardware is tightly coupled with the concept of reference monitor. The reference monitor was defined in [4] and was standardized in [5]. The reference monitor concept was found to be an essential element of any system that would provide multilevel secure computing facilities and controls. Reference monitor is also a heart of the most of cryptographic modules using secret-key cryptography. A usual implementation of reference monitor is a reference validation mechanism, so we will define the reference monitor in this implementation (see [5]). Reference validation mechanism as "an implementation of the reference monitor concept that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user." Three design requirements that must be met by a reference validation mechanism are:

- The reference validation mechanism must be tamper proof.
- The reference validation mechanism must always be invoked.
- The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured.

The implementation of this concept in described system is done by using the secure microcontroller as a computing subsystem. The used microcontroller should always have such physical and logical properties that it complies to the three above conditions. The conditions are met in following ways:

- The reference validation mechanism is tamper proof because of physical properties of the used microcontroller, which is designed as secure hardware that is resistant against physical, electrical, electro-magnetic, and chemical tampering.
- The reference validation mechanism is invoked because of communication protocol that is the only way to communicate with the microcontroller.
- The reference validation mechanism is small enough to be subject to analysis and tests, because of simplicity and standardization of the communication protocol that is used.

For the long time the tamper resistance of security computers (e.g. smartcards and security processors) was accepted without discussion. It was known, those large companies, like Intel or IBM, can successfully reverse-engineer complex chips, but everybody thought that this kind of attack is far beyond abilities of general attackers. The problem of evaluating the level of tamper resistance offered by a given product has been neglected by the security research community. It was discovered in the past that attacks on tamper resistance are possible also by small companies and even by individuals (see [9]). The tamper resistance of smartcards and security processors has to be now closely examined product by product to discover possible vulnerabilities.

4 What is and is not a trusted device

A trusted device is a device which protects interests of a particular entity (typically its owner, however there are exceptions) and provides an interface between the digital and non-digital worlds. Generally speaking, a trusted device must meet three basic requirements:

- keep the data stored in it secret
- do only what its owner wants to do
- not do what other entities, apart from its owner, want to do

These three requirements are rather tough and it is not easy to comply with all of them. In addition, there are other requirements imposed on the trusted device. From the user's point of view, it must be certified in a certain way, that means that its owner must trust in the device construction fulfilling the afore-mentioned requirements. It has to communicate with its holder in a simple, unambiguous, convenient and secure manner. It has to be

protected against harmful impact of third parties, such as protection against malicious codes (e.g. viruses) and unathorized modification protection. It also has to recognize, i.e. authenticate, its user.

The following devices have been and are used as trusted devices:

- *PC*. Personal computer was in the ancient times of IT technology really understood as a trusted computing device which protects its user's interests against other, remote computers connected for instance through a computer network. Unfortunately, this principle vanished with an explosive growth of malicious software and at present we are not able to say unambiguously which software is malicious and which is not. Attempts to get back to previous stages when PC was a trusted device still exist (e.g. using TPM – Trusted Platform Module), however they have not led to generally applicable results yet.
- *Smart card*. Smart card seemed to be an ideal mean to implement a trusted device. It is cheap, easily portable, secure and able to perform cryptographic operations. Unfortunately, it has one drawback which can be critical in some applications – it cannot directly communicate with its holder.
- *PDA (Personal Digital Assistant)*. PDA was considered to be an ideal trusted device for some time. From this point of view it suffered from its functions being improved. Nowadays its capabilities have come close to PC capabilities with all its shortcomings, that means it has insufficient resistance to malicious software.
- *Mobile telephone or smartphone*. Mobile telephone was considered an ideal trusted device for some time (like PDA). The improving functions of mobile phones, however, diminished trust in its software.
- *Single-purpose authentication device*. Single-purpose authentication device (sometimes called authentication tokens) have existed for a relatively long time, its roll-out was prevented by its high cost in the beginnign or the lack of standardization. We can say, however, that this device most resemble the ideal authentication device.

5 Conclusion

At the conclusion of our contribution we can establish two facts which we have been trying to demonstrate. The first fact is that human (non-digital) world and electronic (digital) world are divided and their connection for the purposes of identification and manifestation of will is difficult. Their interconnection usually requires introduction of additional devices which sometimes makes the connection more complicated. The other fact is that there is no universal device for identity verification. Every solution developed up to now performs well only under restricted conditions which are, moreover, changing in the course of time.

This work was supported by the Research Project No. MSM 0021630528 – Security-Oriented Research in Information Technology.

References

[1] Hanáček, P., Staudek, J.: Správa identity, In: Sborník konference DATAKON 2005, Brno, CZ, MUNI, 2005, s. 123-146, ISBN 80-210-3813-6

[2] Security Requirements for Cryptographic Modules, FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, January 11, 1994

[3] Hanáček, P.: Historie a perspektivy elektronické identifikace, In: Sborník konference SmartWorld, Zlín, 2005, s. 1-4

[4] Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I, ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).

[5] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STDm December 1985, US Department of Defense, December 26, l985