Questions on complex dynamic security

Zoltán Kincses

Security is the art of conscious risk taking. The meaning of this definition is that it has to be invested more in a system's security than the cost of evading this security. It is obvious that there is no 100security, even if the security of the system is increased up to a non-usable level of the system. In case a secure and easy to operate system is needed, the possibility of auditing is an essential feature, in order to detect the invader during or leastwise after the attack. The right tool for solving this problem is the sure identification.

Sure identification means identifying the individuals and not only the terminals or passwords. This can be ensured through **biometry**.

The secure (authenticated) communication between extremities must be alive during the whole life-cycle of the transmitted information. This can be resolved by **cryptology**. We have different algorithms proved mathematically that security depends on the key- handling. This key must be secure stored, portable, easy to use, and not detected by any recently known way from the stored format.

Due to different platforms the main problem is the platform dependency. The spreading of the Java programming language makes possible to prepare applications based on the idea of "write once, run anywhere!"

The requirements can be resolved through a tool, called **smart card**. Based on ISO 7816 standard it is possible to use modern smart cards that are able to generate 1024 bit length RSA keys, store biometrics data for sure identification, etc. Their security is well-organized against both software and hardware attacks. Due to Java Card specification it is possible to create **platform independent** applications.

In the paper I intend to show some problems and results in comparison of the ideas described above by creating the *complex dynamic security of a smart card based system*.

There are several components that have some contact points to other components, but the integrity of security of the whole system must be ensured during the mixing operation. On the other hand complex security must handle flexibly every arising changes.

When analyzing different security systems it can be seen the lack of a general framework description in planning - developing - applying processes. Such a framework description should take also into consideration some exceptions, like identification of people with different deficiencies. Embedding exceptions handling should not decrease the security of the system.

As well the proved functioning a complex security system must have also a representation for better illustration. Beside the above mentioned this will also be presented in the full paper.