

Smart Card Secure Environments for Mobile Privacy and Security

Smart card is a best-fit product regarding the user mobility issues as it is attached to the user. The card holder may use it whenever and wherever (applicable) he wants, while at the same time the user information is decentralized on the end-user himself. The ability of the smart cards to maintain information areas under scalable security requirements makes them eligible as a media of mobile privacy and security assurance. Access to the protected information schemes is allowed depending on the privileges of the requesting party. The end user maintains the ultimate control of each transaction just by handling physically the smart card.

The current drawback of the smart card technology is the relatively high cost and the small memory and processing capabilities regarding the requirements of security enforcement and application transaction times. Being a relatively slow reacting environment with limited space it is hard to maintain user information, applications and security-oriented applications altogether under cover. Thus, some interworking with a hosting system is required in order to achieve the requirements of a successful transaction completion. After all, this is and the only way that smart cards could become operatable. Hosting system may be a computer or other device with processing capabilities that "harbors" the smart card. The interaction between the two devices as and the responsibilities of each should be carefully designed according to the application requirements in order to maintain maximum throughput of the system along with the maximum conformity between the various devices functioning under the same application's umbrella.

Various applications are applicable for mobile privacy and security, some more demanding and some less. The more demanding applications involve the sensitive user data and therefore require intense care for the maintaining of the user privacy and security. Sophisticated procedures should be applied in order to protect user information resulting to memory and processor demanding requirements. Such requirements could impose substantial drawbacks for the application of smart card technology as it is currently available depending on the requirements of the application applied. Card-Based Security Systems are typical of such cases, where the card is regarded as an active computing device, with or without active memory manager that would allow dynamic application-specific program downloading. Substantial part of the processing and data handling takes place within the card leaving only encrypted replies to leave its borders. But what about the time required for the processing and message replying? What happens with the communicational part of the transaction and the protocols involved?

The less demanding applications are less demanding from the smart card technology but may be too simple to justify such an expense. After all, smart cards are yet not so cheap to become disposable after usage. Host-Based Security Systems applied to such cases treat a card as a simple data carrier. Because of this, straight memory cards can be used cost-effectively. All protection of the data is done from the host system, while the card data may be encrypted. A common method of increasing the security is to write a key that usually contains a date and/or time along with a secret reference to a set of keys on the host. Each time the card is re-written the host can write a reference to the keys, making in this way each transmission different. This security can be even more increased by the use of smart memory cards that employ a password mechanism to protect unauthorized reading of the data.

A strong point of applying holistic security approach within the borders of a smart card is that transactions may be realized offline whenever necessary. The existence of strong authentication and non-repudiation procedures along the security schemes, cases like the Public Key Encryption technique, allows for the completion of a transaction between an end-user and a provider without the real time mediation of an authentication server. In more extend, it is then possible for various applications running in parallel on the same smart card, independently between each other, as the security methods applied would vary per case and isolate the applications as and their associated data. Even further, future smart cards may become full-fledged Internet devices. Since a smart card could become a legal proxy for an end-user, it can conduct Internet business in the physical absence of its owner. The validity of the order depends on the digital signature on the smart card and not on the presence or absence of the buyer, buyer who always maintains the ultimate control over his card with the choice to plug or unplug it online.

The security affects and the communicational parts between the smart card and the other side of a transaction. The communication between the smart card and the host system, between the host system and the operator or service provider or authenticator, between the host system and the other

side system as well as between the peer applications are all eligible to security and privacy enforcement. Given the already deployed security for the communicational parts of vertical systems like the mobile phone networks, care should be taken in order to maintain the role and the validity of each layered approach as well as to define new security standards for the parts that are directly affected by the participation of smart cards into the transaction proceedings. After all, given a fully secure system with all-in-one build mechanism within a smart card, in a well harmonized environment where buyers and merchants could transact successfully even offline, what would be the role of the operator? Is there any reason to use my mobile phone operator network when I can communicate directly with the peer user? The demolition of the star topology between a central controlling authority and the decentralized users could introduce side effects that should be investigated and justified as well.

Application and technology oriented requirements pose their specific expected characteristics of a smart card reaction to a given transaction. Tolerant and intolerant applications blur the insight of an integrated design with global conformity as and technology poses reaction-specific targets to be achieved in order to comply with the communicational environment as design so far. Still it is crucial to define the least requirements of operation of selected application-oriented groups in order to classify and categories the potential principles that would drive the design of the future secure smart card oriented systems.

It is clear that the smart cards can play substantial part of the mobile privacy and security environment. Their current memory storing capabilities justify the hosting of user information along with the protection characteristics applied to them. The advent of the processing capabilities of the smart cards could engage them into the cryptography as well, transforming them into a closed secured system. Until then, pre-computed and pre-allocated security primitives could be assigned to smart cards along with the user characteristics in order to enforce the function of specific applications such as e-banking. More applications of the smart cards are reluctant to the application in interest, leaving room for the involvement of relative technologies as smart tags and smart labels or even wireless smart cards.

REFERENCES

- [1] Smart card and security basics, CardLogix Inc.
- [2] Cryptography and network security, principles and practice, William Stallings, Prentice Hall.
- [3] An overview of smart card security, S. C. Chan.
- [4] Smart card security, Gemplus.
- [5] Java Card: Internet Computing on a Smart Card, Schlumberger Electronic transactions.
- [6] Computer Networks 3rd Ed., A. Tanenbaum, Prentice Hall.
- [7] Smarter, More Secure Smartcards, Ian Blythe, BYTE Magazine.

Giannis A. PIKRAMMENOS, Ph.D., MBA,
Senior Research Associate of National Technical University of Athens (NTUA),
Electrical Engineering & Computer Science Dept.,
Telecommunications Laboratory,
Eroon Politechniou 9,
15773 Zografou, Athens,
GREECE
Tel: (+30 1) 772 2583
Fax: (+30 1) 772 2534
E-mail: gpik@telecom.ntua.gr