Pp. 173 - 176 in Viktor Seige et al.: The Trends and Challenges of Modern Financial Services – Proceedings of the Information Security Summit; May 29-30, 2002, Prague; Tate International; ISBN 80-902858-5-6

CamWebSIM and friends

Steps towards Personal Security Assistants

Kai Rannenberg
Microsoft Research Cambridge, UK; *www.research.microsoft.com/~kair*
T-Mobile-Stiftungsprofessur für M-Commerce, Johann Wolfgang Goethe-Universität
Frankfurt; Germany; *www.m-lehrstuhl.de*

This contribution gives a short motivation for personal security assistants and then describes CamWebSIM, a small quasi-HTTP server based on a GSM SIM card together with some application examples.

Multilateral Security and Personal Security Assistants

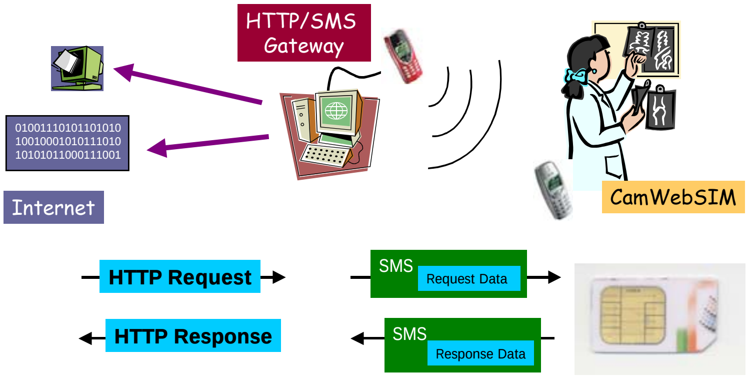
Security today is not only about protecting one “good” party against one “bad” party, but about helping parties with different interests to balance their security (Multilateral Security [Rannenberg 2000]). Most fair security and protection measures require that at least some information is held and processed by the users themselves, e.g. access codes, cryptographic keys (for digital signatures or privacy), or digital money. Storing the information with service providers does not match its personal (private) character, so some personal security devices (Personal Security Assistant, PSA) are needed.

PSAs could be based on different platforms, e.g. PDAs, mobile phones, smart cards or combinations of these. While in theory they could be perfectly secure and interoperate with any security and communications infrastructure, all practical implementations depend heavily on their environment both regarding operability and security. Moreover technology at this time does not seem to be mature enough for a feature-rich AND secure PSA. So there is also some sense in exploring available technologies for their security properties and for appropriate combinations that can open additional secure channels. Some of the MSR Cambridge projects go into this direction. An example is CamWebSIM, a small HTTP server on a GSM SIM card based on Microsoft Windows for Smart Cards.

CamWebSIM

CamWebSIM makes use of the capabilities of chip cards and of the fact that the GSM mobile phone network has already established a widespread security infrastructure with a smart card based SIM (Subscriber Identity Module) fitted into any GSM mobile phone. A further development of the WebSIM, CamWebSIM is a small quasi-HTTP server on a GSM SIM based on Microsoft Windows for Smart Cards. By making the SIM accessible over HTTP, the phone and the SIM become a personal security server in the Internet that is based on the GSM trust model.

CamWebSIM processes HTTP requests and enables applications like authorizing a transaction or an access request. The Internet connectivity of CamWebSIM is achieved by a proxy host with both an Internet and a GSM connection (see Figure 1). This proxy host receives HTTP requests coming from the Internet and forwards them to the SIM via the GSM SMS (Short Message Service).

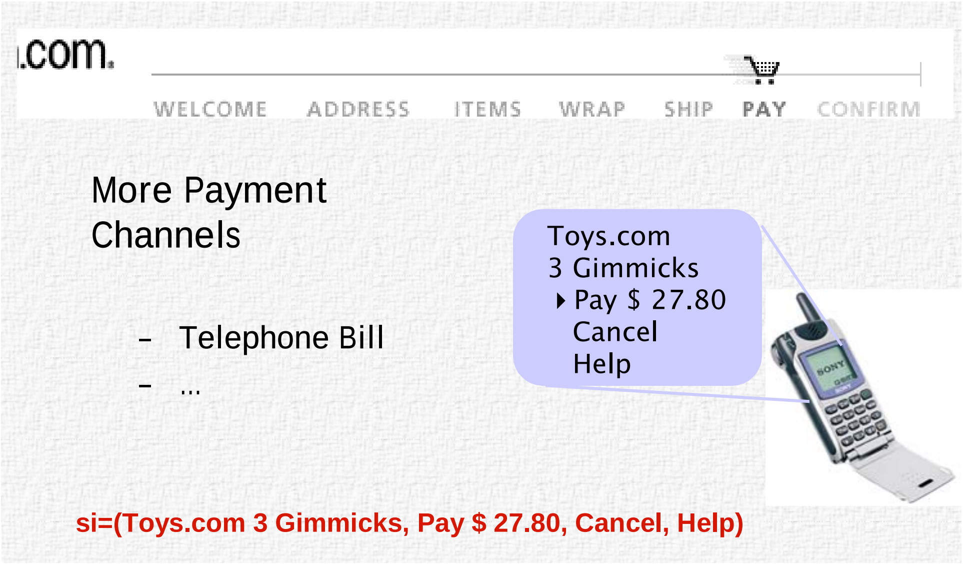


http://www.camwebsim.telco.com/+14253334711/si=(select,opt1,opt2)

Figure 1: CamWebSIM Setup

CamWebSIM Applications

One application example is paying for Internet services via one’s GSM telephone account (see Figures 2 and 3). This can even enable cash-like payments if the account is a prepaid one and not bound to a person. While past attempts to establish electronic cash systems did not reach the critical mass on the customer or merchant side, this approach would avoid the costs for an extra rollout to consumers, as mobile phone vouchers are bought and sold anywhere anyway.



More Payment Channels

- Telephone Bill
- ...

Toys.com
3 Gimmicks
▸ Pay $ 27.80
Cancel
Help

si=(Toys.com 3 Gimmicks, Pay $ 27.80, Cancel, Help)

Figure 2: Payment Authorization

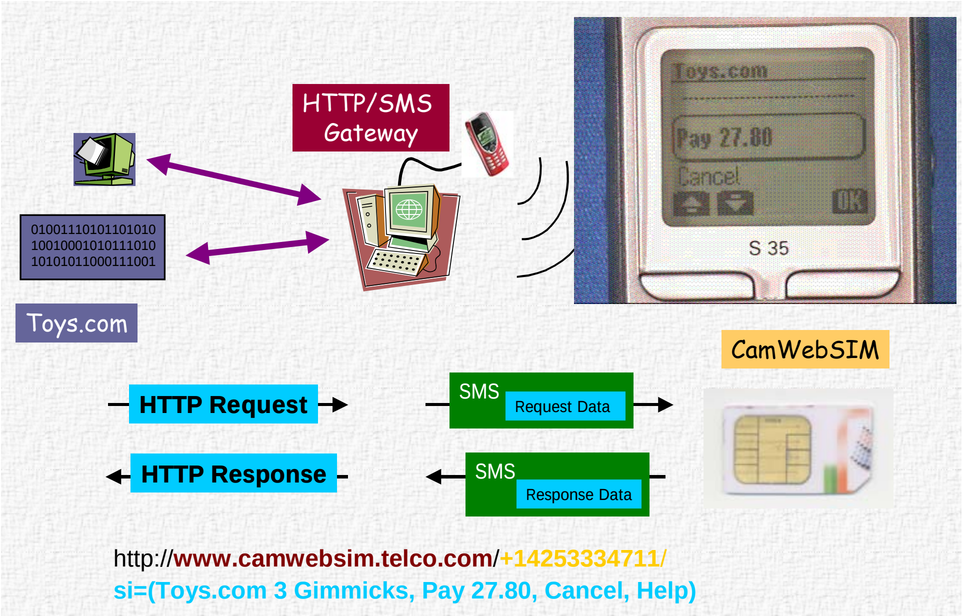


Figure 3: Payment Authorization Setup

The crypto capabilities of Microsoft Windows for Smart Card also allow for trust relationships beyond the GSM trust model, e.g. by signing a payment order with a key that is trusted by other parties than the GSM network operator. Current work is also on using the additional secure channels for securing more mobile applications in e.g. a privacy friendly way.

Wireless Trust for Mobile Business

One important application area these days is secure mobile access to enterprise information systems by a proper combination of PDAs, phones and chip cards, e.g. SIMs. Therefore in the project WiTness (Wireless Trust for Mobile Business) we are exploring the requirements of this field together with SAP and leading players in the mobile communication business, e.g. RadioMobil (T-Mobile partner in the Czech Republic). One reason for this approach is, that early adopters of PSA technology will probably come from the business-to-employee-environment and thus can provide some real-world experience of advanced technology. In parallel this work is being reflected against the requirements of private consumers.

References

[CamWebSIM]: www.research.microsoft.com/security

[Rannenberg 2000]: Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3; Earlier version in: Cd/papers/202ra.pdf on CD-Proceedings of the 23rd National Information System Security Conference, October 16-19, 2000, Baltimore, Maryland

[Windows for SmartCard]: www.microsoft.com/smartcard

[WiTness]: www.wireless-trust.org/index.html