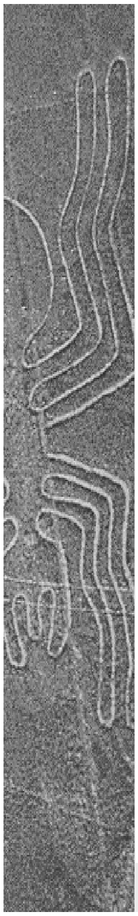
MINX: Micropayments with Secure Network Exchange

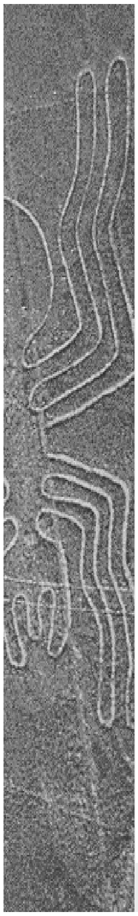
Krzysztof Szczypiorski, Aneta Zwierko, Igor Margasiński
Institute of Telecommunications, Warsaw University of Technology

International Interdisciplinary Conference on Electronic Commerce
ECOM-03



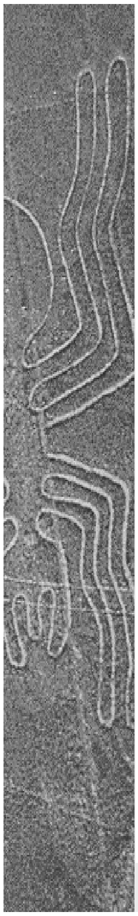
Contents

- ♦ Micropayments vs. macropayments
  - – Micropayments schemes
- ♦ MINX
  - – Electronic prepaid card vs. micropayments
  - – General overview
  - – Possible versions of scheme
  - – Application
- ♦ Conclusion
- ♦ Questions



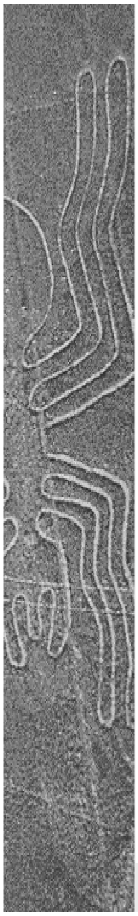
Micro- & Macro- Payments

- Macropayments
  - User makes few but large transactions
  - Widely use in e-commerce systems (shops, etc)
- Micropayments
  - User makes many small transactions
  - Buying web content, streaming services, etc.
- Micro vs Macro
  - Frequency of macropayments is quite low
    - computation connected with using strong cryptography (public key cryptosystems) and need of on-line communication between broker (bank), vendor and client is not a problem
  - In micropayments frequency of transactions is quite high
    - use of PKI is impossible – too many computation per one transactions
    - Need for an on-line communication between broker, vendor and client is problematic



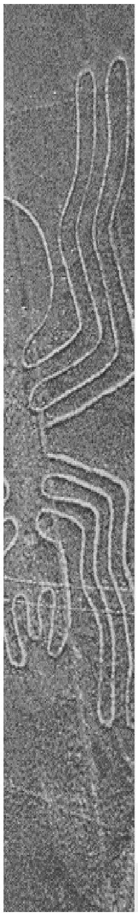
Known Micropayments Schemes

- Payword & Micromint
  R. Rivest, A. Shamir (1996)
- CAFE system (ESPIRIT project)
  T. Pedersen (1994)
- NetPay
  X. Dai, J. Grundy (2002)
- Micropyments based on Probabilistic Polling
  S. Jarecki, A. Odlyzko (1998)
- Electronic Lottery Tickets
  R. Rivest (1998)
- Internet Keyed Payment System (*i*KP)
  R. Hauser, M. Steiener, M. Waidner, IBM (1996)



Electronic Prepaid Card

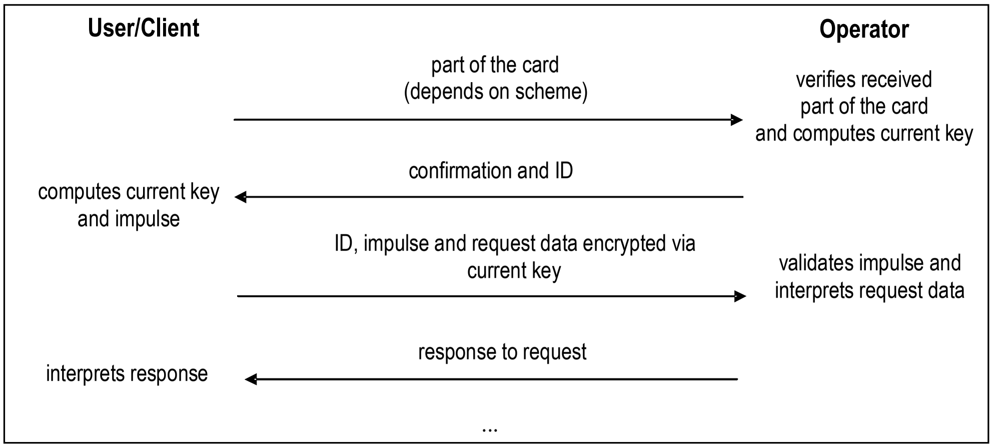
- Prepaid card is kind of micropayments scheme
- Idea based on real-life prepaid cards
- Main properties
  - User buy a prepaid card from operator
  - User trust operator that card is valid and will be able to use it
  - Card can be used only partially
  - User can utilize card in any moment
  - User is not required to provide operator with any data apart of data concerning the card
  - No TTP (Trusted Third Party) required



MINX – General Overview (1)

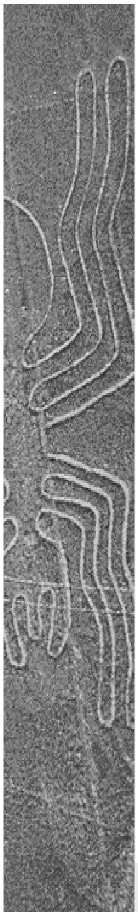
- Main advantages
  - Functionality of electronic prepaid card
  - Ability to perform cryptographic key distribution with micropayment process
- Cryptographic primitives
  - One-way has function
  - Pseudorandom bit generator
- Basic definitions
  - Key
  - Impulse
  - ID
- Card is built of the following:
  - secret seed – x
  - card’s value
  - number of impulses – z
  - function for generating impulses or secret parameters of CSPRBG

MINX – General Overview (2)



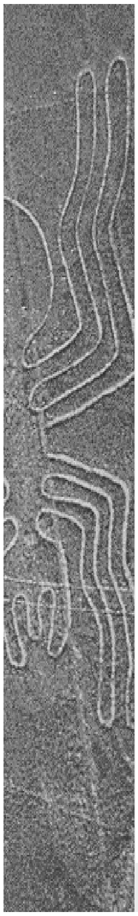
MINX – Hash Function Version

- Secret key and impulse are generated using one-way hash function from seed x: h(x)
- The advantages of this scheme include:
  - confidentiality of communication between a user and an operator
  - possibility of using services with different values/prices with one card
  - no need for TTP to compute impulses prior to card usage. A user does not have to request an authorization of a card
- The disadvantages include:
  - computation of impulses and keys, their validation is slower then in classical micropayments schemes
  - an operator has to be trusted same as in the real world



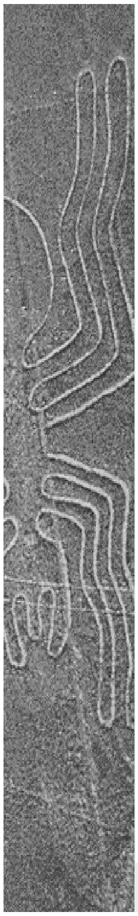
MINX – CSPRBG Version

- Instead of the hash function, a client uses cryptographically secure pseudorandom number generator (CSPRBG)
  - generation and a verification of a key and an impulse take almost the same amount of time
- The advantages include:
  - the same number of operations to generate key/impulse every time and to verify them
  - the same as in the previous scheme
- The disadvantages are:
  - generating proper parameters of CSPRBG is quite complex
  - computation CSPRBG values is not very fast, and poses almost the same problems as public-key cryptosystems



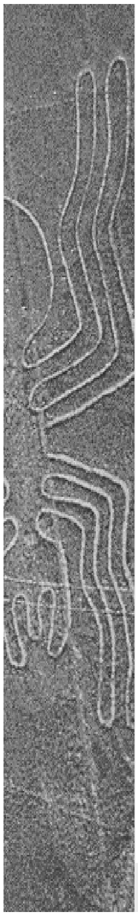
MINX - Application

- Independent cryptosystem
  - Application layer (where micropayments are provided)
  - Keys placed on pre-paid cards are utilized to provide confidentiality for clients' requests or operators' responses including security of the content during the paying process
- Use with other security protocol
  - Possible security protocols: SSL/TLS (Secure Sockets Layer/Transport Layer Security)
  - In this case (i.e. SSL/TLS), the adequate session key (SSL/TLS MasterKey) is extracted from a pre-paid card and is utilized to provide transaction security according to admitted context (for example duration or data volume)



Conclusions

- Both original schemes presented in this article (the first one based on one-way hash functions, the second one based on cryptographically secure pseudorandom bit generators) are integrated with cryptographic key distribution
- Payment for access to resources without compromising users' privacy
- The usage of keys placed in pre-paid cards
  - reduces costs of key management system implementation
  - simplifies clients' software/hardware
- Other main advantages of the proposed schemes:
  - a possibility of using services with different values/prices with one card
  - the absence of TTP



References

1. Boly, J-P., Bosselaers, A., Cramer, R., Michelsen, R., Mjřlsnes, S., Muller, F., Pedersen, T., Pfitzmann, B., de Rooij, P., Schoenmakers, B., Schunter, M., Halle, L., Waidner, M.: The ESPRIT Project CAFE. ESORICS 94, Springer-Verlag LNCS Vol. 875 (1994) 217-230
2. Dai, X., Grundy, J.: Architecture of a Micro-payment System for Thinclient Web Applications. Proceedings of the 2002 International Conference on Internet Computing (2002)
3. Dai, X., Grundy, J., Lo, B.: Comparing and contrasting micro-payment models for E-commerce systems. International Conferences of Info-tech and Info-net (ICII) (2001)
4. Dierks T., Allen C.: The TLS - Protocol Version 1.0. IETF RFC 2246 (1999)
5. Ellis, C.: Evaluation of Micropayment Schemes. Tech Report HPL-97-14 (1997)
6. Hauser, R., Steiner, M., Waidner, M.: Micro-Payments based on iKP. Research Report 2791 (# 89269), IBM Research (1996)
7. Jakobsson, M., Hubaux, J-P., Buttyan, L.: A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks. Financial Cryptography'03 (2003)
8. Jarecki, S., Odłyżko, A.: An Efficient Micropayment System Based on Probabilistic Polling. Financial Cryptography '97, Springer-Verlag LNCS Vol. 1318 (1998) 173-191
9. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Inc. (1997)
10. Micali, S., Rivest, R.: Micropayments Revisited. CT-RSA 2002, Springer-Verlag LNCS Vol. 2271 (2002) 149-163
11. Pedersen, T.: Electronic Payments of Small Amounts. Technical Report IDAMI PB-495 (1995)
12. Rivest, R.: Electronic Lottery Tickets as Micropayments. Financial Cryptography '97, Springer-Verlag LNCS Vol. 1318 (1998) 307-314
13. Rivest, R., Shamir, A.: PayWord and MicroMint: Two simple micropayment schemes. Proceedings of 1996 International Workshop on Security Protocols, Springer-Verlag LNCS Vol. 1189 (1997) 69-87