Contents

- Questions
- Conclusion
  - Application
  - Possible versions of scheme
  - General overview
  - Electronic prepaid card vs. micropayments
- MINX
  - Micropayments schemes
  - Micropayments vs. macro-payments

ECOM-03
International Interdisciplinary Conference on Electronic Commerce

Institute of Telecommunications, Warsaw University of Technology

Krzysztof Szczygloński, Aneta Ziwińska, Igor Margashinski

Secure Network Exchange
MINX: Micropayments with
Known Micropayments Schemes

- Internet Keyed Payment System (IKP)
- Electronic Lottery Tickets
- Micropayments based on Probabilistic Polling
- NetPay
- CAFE system (ESPIRIT project)
- Payword & Micromint
- R. Rivest (1996)
- T. Pedersen (1994)

Is problematic
- Need for an on-line communication between broker, vendor and client
- Use of PKI is impossible – too many computation per one transaction
- In micropayments, frequency of transactions is quite high
  (bank, vendor and client is not a problem)
- Frequency of micropayments is quite low

Micro vs Macro
- Buying web content, streaming services, etc.
- User makes many small transactions
- Micropayments
- Weekly use in e-commerce systems (shops, etc.)
- User makes few but large transactions
- Micropayments
MINX - General Overview (1)

- Function for generating impulses or secret parameters of CSFRE
- Number of impulses - \( z \)
- Card's value - \( x \)
- Secret seed - \( s \)

Card is built on the following:

- ID
- Impulse
- Key

Main definitions:
- Pseudorandom bit generator
- One-way hash function
- Cryptographic primitives

Cryptographic primitives:
- Ability to perform cryptographic key distribution with micropayment
- Functionality of electronic prepaid card

Main advantages:
- No TTIP (trusted Third Party) required
- No data concerning the card
- User is not required to provide operator with any data apart of
- User can utilize card in any moment
- Card can be used only partially
- User must operator that card is valid and will be able to use it
- User buy a prepaid card from operator

Electronic Prepaid Card

- Idea based on real-life prepaid cards
- Prepaid card is kind of micropayments scheme
- An operator has to be trusted same as in the real world.
- Then in classical Biometric schemes combination of Biometric and keys, their validation is slower.
- The disadvantages include:
  - The user does not have to request an authentication of a card.
  - No need for TP to compute the impulses prior to card usage.
  - Possibility of using services with different values/pieces with one card.
  - Confidentiality of communication between user and an operator.
- The advantages of this scheme include:
  - Hash function from seed x h(x).
  - Secret key and impulse are generated using one-way function.

MINX – Hash Function Version

MINX – General Overview (2)
admitted context (for example, duration or data volume) is utilized to provide transaction security according to SSL/TLS Masterkey (is extracted from a pre-paid card and Layer/Transport Layer Security (in this case, the initial session key)) Possible security protocols: SSL/TLS (Secure Sockets Use with other security protocols

including security of the context during the paying process confidentiality for client's requests or operator's responses - Keys placed on pre-paid cards are utilized to provide Application layer (where microparameters are provided)

 Independent cryptographic system

MIX - Application [Image 79x424 to 128x764]

almost the same problems as public-key cryptographys - computation CSPRBCG values is not very fast and poses

− generating proper parameters of CSPRBC is quite complex

The disadvantages are:

− the same as in the previous scheme

− every time and to verify them

− the same number of operations to generate Key/Impulse

The advantages include:

− almost the same amount of time

− generation and a verification of a key and an Impulse take

− generator (CSPRBCG)

− cryptographically secure pseudorandom number

Instead of the hash function, a client uses

MIX - CSPRBCG Version
**Conclusions**

- The absence of TTP
- One card
- Possibility of using services with different values/prices with

**Other main advantages of the proposed schemes:**
- Simple client software/hardware
- Reduced costs of key management system implementation
- The usage of keys placed in pre-paid cards
- User privacy
- Payment for access to resources without compromising distribution

Both original schemes presented in this article (the first