μPay: NFC-Based Micropayment System and its Android Implementation

Mauro Conti*, Hendri Appelmelk*, Earlene Fernandes* and Bruno Crispo**

* Vrije Universiteit Amsterdam
** University of Trento
Introduction/NFC/Micropayment

Significant Related Research

μPay Micropayment System
  – Protocol Overview
  – Android Implementation

Evaluation
## Introduction

A micropayment is a financial transaction involving a very small sum of money which therefore allows relaxed security.

The money involved in a micropayment transaction should have the same properties as “real” money:

- Acceptability
- Anonymity
- Speed
- Offline
- Cost
- Non-Traceability
- Invention
- Overspending
Near Field Communication

- Proximity based Communication
  (13.56 MHz, 106-424 Kbits/s, ~4 cm)

- Short Distances

- Low cost link setup (comparatively, eg: Bluetooth)

- Standardized (ISO/IEC 18092, 21481)

Really hot right now. (read: Google Android NFC)
Near Field Communication

NFC enables:

1. Electronic Ticketing
2. Payments in Public Transport
3. Electronic Boarding Passes
4. …
Ron Rivest and Adi Shamir – PayWord (1997) *

- A chain of hash values

- Each element of the chain represents a “PayWord” which is “money”

- Items to be bought are worth one or a multiple of “PayWords”

- Each hash chain can only be spent at a single vendor

E. Blass et al. - PSP: Private and Secure Payment with RFID (2009) *

- RFID tags with info. To “create money”
- User “charges tag” from a Broker
- Readers have a bloom filter

- Money can be generated by unauthorized parties

μPay

✓ Micropayment system using NFC
✓ Implemented on Android
✓ Prevents Overspending
✓ First of its kind in this space
✓ Fraud Detection
μPay

Architecture

Broker

Parking Meter

User

Verifier

NFC Tag
Protocol Overview (1/4) - Initialization

Broker

$S_1$  $S_i$  

seeds

$P_1$  $P_i$  ...

Parking Meters

$P_K$
Protocol Overview (2/4) - Charge
Protocol Overview (3/4) – Check In

\[ E_{K^P} \left\{ \{\overline{\omega^j_i}, TS_u\}_{\text{sig}_U} \right\}, \text{Cert}_U, j, D, CP, l \]

\[ E_{K^U} \left\{ \{\overline{\omega^j_{i'}}\}_{\text{sig}_P} \right\}, l, TS_P \]

\[ h(h^{l-1}(\omega^j_L), \omega^j_L) \equiv \overline{\omega^j_i} \]

\[ (l - D) \geq 0 \]

\[ i' = i + D \]

\[ l = L - i' \]

\[ \overline{\omega^j_{i'}} = h(h^{l-1}(\omega^j_L), \omega^j_L) \]
Protocol Overview (4/4) – Check Out

\[ E_{K_P}^{\text{pub}} \left\{ \{ \overline{\omega_i^j} \}_{i \leq j}, TS_u \}_{\text{sig}_U} \right\}, \text{Cert}_U, j, l \]

\[ h(h^{l-1}(\omega^j_L), \omega^j_L) \equiv \overline{\omega_i^j} \]

\[ l = l - R \]

\[ i'' = L - l \]

\[ \overline{\omega_i^{j''}} = h(h^{l-1}(\omega^j_L), \omega^j_L) \]
Implementation Details (1/2)

✔ Android 2.2 + Nexus One + Arygon NFC Reader

✔ USB Host Mode – Kernel Mod

✔ Couple of Kernel Modules – usbserial.ko, cp210x.ko

✔ libnfc

✔ Some framework hacking
Implementation Details (2/2)

- μPay application (Java)
- JNI wrapper (Java/C++)
- Android system server (C++)
- Android native services (C++)
- LibNFC (C)

System Architecture
## Evaluation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>On-line purchases</td>
<td>On-line purchases</td>
<td>On-line purchases</td>
<td>Public transport</td>
<td>On-line purchases</td>
<td>Parking &amp; products</td>
</tr>
<tr>
<td><strong>Implemented</strong></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Able to handle deposit</strong></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Technology used</strong></td>
<td>Internet</td>
<td>Internet</td>
<td>Internet</td>
<td>RFID</td>
<td>Internet</td>
<td>NFC</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Offers anonymity</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Offers intraceability</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Fast</td>
<td>Fast</td>
<td>Slow</td>
<td>Fast</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td><strong>Avoid generation</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Off-line</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Avoid double spending</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Avoid overspending</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Pre/Post paid</strong></td>
<td>Post</td>
<td>Pre</td>
<td>Pre</td>
<td>Pre</td>
<td>Pre</td>
<td>Pre</td>
</tr>
<tr>
<td><strong>Used data structure</strong></td>
<td>HC</td>
<td>HC</td>
<td>HC</td>
<td>BF</td>
<td>MHC</td>
<td>HC</td>
</tr>
</tbody>
</table>

Parking & products:
- Yes
- No
Future/On-going Work

- Nexus S implementation
- Broker Implementation
- Formal Protocol Verification
http://www.few.vu.nl/~earlence