Can Mobile Payments be 'Secure Enough'?

Roger Clarke, Xamax Consultancy, Canberra
Visiting Professor in eCommerce at Uni of Hong Kong, Cyberspace Law & Policy at U.N.S.W., Computer Science at A.N.U.

http://www.anu.edu.au/people/Roger.Clarke/ ... / EC/MPS-071025 {html, .ppt}

eCom/iCom Uni. of Hong Kong – 25 October 2007

Can Mobile Payments be 'Secure Enough'?

Agenda

1. Mobile Payment Excitement
2. Payment Mechanisms – Pre-Networks
3. Payment Mechanisms – Network Era
4. Security Analysis
5. The Acceptability of Insecurity

Octopus
Hong Kong
Since Sep 1997

- To pay, wave an Octopus card within a few cm of the reader (even if it’s in a wallet/purse)
- Audio-acknowledgement (beep)
- Display of tx amount and remaining balance
- On MTR and KCR transport, read-on-exit causes a deduction based on entry-point

RFID Tags for Road-Tolls

- Car requires a Tag
- Car drives through Tag
- Control-Point interacts with Tag
- Toll is deducted automatically
- Fixed display of fees
- Audio-acknowledgement of transaction
- Depends on blind consumer trust
Japanese Osaifu-Keitai / Mobile Wallet

- Many Japanese mobile phones contain an extra chip, which uses RFID/NFC to communicate with payment-related devices
- Services include:
  - eMoney (Edy)
  - public transport (Mobile Suica)
  - credit card?
  - vending machines (Cmode)
  - (loyalty card, id card, ...) Don’t lose it!!
- The chip is the Sony FeliCa (as in Octopus ...)
- Sony Viao PCs can interact with FeliCa

Visa MicroTag using Visa payWave Technology

- Intended to support 'instant purchase'
- Carried as a key-ring / key-chain
- Requires proximity (1-2 inches)
- Provides a visual indication when it operates
- No confirmation under a threshold [US$ 25?]
- Not standards-based?
- No independent security testing?
- No public audit and certification?

PayBox

- German scheme, with Deutsche Bank
- Type in account no, amount, a PIN e.g. in a taxi-cab
- PayBox acts as an Intermediary
- PayBox passes Payment Instructions on to the Bank for processing against the Payer’s existing Bank Account

- Links an Account with the Intermediary to:
  - an existing bank account; and/or
  - an existing credit card
  - but is now becoming a card-issuer as well
- Passes on Payment Instructions sent from:
  - web-browser
  - touch-tone to IVR
  - SMS / text-messages
- Imposes punitive terms and fees
UK Parking Payment

- Customer registers with RingGo and provides (most of) their credit card details
- Customer uses their mobile phone to call a RingGo phone-number displayed in the car-park
- Customer keys the car-park’s 4-digit code
- Customer chooses the duration of stay
- Customer keys remaining digits of credit-card
- RingGo processes a credit-card transaction, and makes data available on-line to traffic wardens
- Customer can access the transaction trail online
- [Still pre-paid, so still risk over-run!]

2. Payment Mechanisms Pre-Networks

- Cash
- Cheque
- Direct Credit
- Direct Debit
- Credit Cards at Point-of-Sale
- Credit Cards MOTO
- Charging to Telco Accounts
Direct Credit
Giro, 'TT', Salary Payments

1A. Information

1. Payment Instruction

Financial Institution

2. Value

and Information

Financial Institution

3. Information

Direct Debit
Standing Authorisation

1. Standing Authorisation (once)

Payer

Payee

6. Information

2. Payment Instruction (periodically)

Financial Institution

3. Payment Instruction

Financial Institution

5. Information

Credit-Card Details in
Card-Not-Present (MOTO) Transactions

- Changes the ‘have’ factor from ‘have the card’ to merely ‘have credit card details’
- No ‘know a secret’ factor
- Relies on:
  - secrecy of credit-card details
  - general levels of honesty
  - consumers reconciling their accounts
  - self-insurance by merchants
    (banks issue ‘charge-backs’)
**Paying Through Your Telco / Mobile Provider**

- Top-Ups
- Vending Machines
- Event Tickets
- Public Transport Tickets
- Parking Fees
- ...

**3. Payments in the Network Era**

- ATMs
- Internet Banking
- Credit Card Tx over the Internet
- Debit Tx over the Internet
- eCash
- ePayment Instructions
- Stored Value Cards

**ATMs**

- 2-factor:
  - have card
  - know PIN
- PIN keyed into secure PIN-pad, in a manner which makes it difficult to observe [?]
- Hash of PIN transmitted and compared
- So the ‘know’ part is protected from both physical and electronic observation
Credit Card Tx over the Internet (Very Similar to MOTO)

- The ‘have’ factor is not ‘have the card’ but merely ‘have credit card details’
- No ‘know a secret’ factor
- Relies on:
  - an encrypted channel (SSL/https)
  - secrecy of credit-card details
  - general levels of honesty
  - consumers reconciling their accounts
  - self-insurance by merchants (banks issue ‘charge-backs’)

SET (Secure Electronic Transactions) Processing for Internet Credit Cards

- Card-Holder states that he wishes to make a payment
- Merchant acknowledges
- Card-Holder provides payment amount, digital certificate
- Merchant requests an authorisation from the Payment-Processing Organisation (via a Payment Gateway / Acquirer)
- Existing EFTS networks process the authorisation
- Merchant receives authorisation
- Merchant sends capture request (to commit the transaction)
- Merchant receives confirmation the transaction is accepted
- Merchant sends Card-Holder confirmation

Internet Banking

- 2-factor (or 3-factor):
  - have card
  - know PIN
  - (have or know 2nd authenticator)
- PIN keyed into insecure key-pad, in a manner which makes it difficult to observe
- Hash of PIN transmitted and compared
- So the ‘know’ part is protected from both physical (but also electronic?) observation

Debit Transactions over the Internet

- Customer is at a merchant’s payment page
- Customer is re-directed to a specialised version of their own bank’s online-banking services
- Customer uses their own bank’s Internet Banking service to authorise the transaction including an encrypted channel (SSL/https)
- Customer is redirected to the merchant
- Canada’s scheme is called Interac Online: http://www.interaconline.com/
- This leverages on a well-trusted infrastructure, but requires careful interfacing from merchants
Other Internet Payment Schemes
1996 – 2000 ??
2007 – 20xx ?

- Electronic Value-Tokens (cash-like)
  DigiCash, NetCash
  incl. micropayment schemes
  Cybercoin, Millicent
- Electronic Payment Instructions (cheque-like)
  NetCheque, NetBill, BankNet, Netchex
- Stored-Value Cards
  Mondex

Copyright, 1995-2007

Wireless Networks

- Wide Area Networks – Satellite
  - Geosynchronous (2 second latency)
  - Low-Orbit (Iridium)
- Wide Area Networks – Cellular (to 20km per cell)
  1 – Analogue Cellular
  2 – Digital Cellular, e.g. GSM, CDMA
  3 – ‘3G’, e.g. GSM/GPRS and W-CDMA
- Wide Area Networks – ‘WiMax’, IEEE 802.16; iBurst
- Local Area Networks – ‘WiFi’, 802.11x (10-100m radius)
- Personal Area Networks – Bluetooth (1-10 m radius)
- Contactless Cards / RFID Tags / NFC (1-10cm radius)

Copyright, 1995-2007

Credit-Card Details in the MCommerce Mobile / Handheld / Wireless Era

- Inherits all weaknesses of MOTO / Internet
- Less Visible Payee, no ‘Footprint’
- Less Visible Process, perhaps invisible
- Less Visible Transaction Data?
- Notification Record / Tx Voucher?

Debit-Card Details in the MCommerce Mobile / Handheld / Wireless Era

- Less Visible Payee, no ‘Footprint’
- Less Visible Process, perhaps invisible
- Less Visible Transaction Data?
- Notification Record / Tx Voucher?
- Capture of Authenticators on mobile
- Transmission of PIN or hash w/- SSL?
4. Security Analysis

A Security Model

Vague Threats
Become Actual Threatening Events,
Impinge on Vulnerabilities,
Overcome Safeguards
& Cause Harm

Security is an (unusual) condition
in which Harm does not arise
because Threats are countered by Safeguards

MPayments – Key Categories of Harm

- Unauthorised Conduct of Transactions
- Acquisition of Identity Authenticators
  Credit-Card Details (card-number as identifier,
  plus the associated identity authenticators)
  Username (identifier) plus Password/PIN/Passphrase/Private
  Signing Key (identity authenticator)
- Interference with Legitimate Transactions
- Use of a Consumer Device as a Tool
  in a fraud perpetrated on another party

Unauthorised Transactions Aren’t Just Theory

- Design Flaw:
  - Octopus customer started to add value to their
    card at self-service add-value points located in
    MTR and KCR stations
  - Customer cancelled the transaction
  - But the bank accounts were debited
  - The flaw existed from at least 2000,
    but was not discovered until 2007!
  - HK$ 3.7 million deducted from 15,270 accounts

Second-Party Risks

- Trust Levels:
  - Banks
  - Telcos / Mobile Phone Providers
  - Intermediaries
  - Devices
- Terms of Contract
- Enforceability
- Consumer Rights
Third-Party Risks – Within the System
(Who else can get at you, where, and how?)

- Points-of-Payment Physical:
  - Observation
  - Coercion
- Points-of-Payment Electronic:
  - Rogue Devices
  - Rogue Transactions
  - Keystroke Loggers
  - Private Key Reapers
- Network Electronic
  - Interception
  - Decryption
  - Man-in-the-Middle Attacks
- Points-of-Processing
  - Rogue Employee
  - Rogue Company
  - Error

Consumer Device Vulnerabilities

- The Environment
  - Physical Surroundings
  - Organisational Context
  - Social Engineering
- The Device
  - Hardware, Systems Software
  - Applications
  - Server-Driven Apps
    (ActiveX, Java, AJAX)
  - The Device's Functions:
    Known, Unknown, Hidden
  - Software Installation
  - Software Activation
- Communications
  - Transaction Partners
  - Data Transmission
- Intrusions
  - Malware Vectors
  - Malware Payloads
  - Hacking, incl.
    Backdoors, Botnets

Consumer Device Threats

- Physical Intrusion
- Social Engineering
  - Confidence Tricks
  - Phishing
- Masquerade
- Abuse of Privilege
  - Hardware
  - Software
  - Data
- Electronic Intrusion
  - Interception
  - Cracking / ‘Hacking’
    - Bugs
    - Trojans
    - Backdoors
    - Masquerade
- Infiltration by Software with a Payload

Infiltration by Software with a Payload

Software (the ‘Vector’)
- Pre-Installed
- User-Installed
- Virus
- Worm
- ...

Payload
- Trojan:
  - Documented or
    Undocumented
- Bot / Zombie
- Spyware:
  - Software Monitor
  - Adware
  - Keystroke Logger
  - ...
Key Elements of a Secure Approach

- Two-Sided **Device Authentication**, i.e.  
  - by Payee’s Chip of Payer’s Chip  
  - by Payer’s Chip of Payee’s Chip
- **Notification to Payer** of:  
  - Fact of Payment (e.g. Audio-Ack)  
  - Amount of Payment  
  - At least one **Authenticator**  
  - Protection of the **Authenticator(s)**  
  - A **Voucher** (Physical and/or Electronic)  
  - Regular **Account Reconciliation** by Payers

Can Mobile Payments be ‘Secure Enough’?

**Things We Need To Know**

- What does the public want?  
- What’s the price of convenience?  
- What security-levels will the public accept?  
- How will we know where the threshold of acceptability is?  
- If we exceed it, will we harm adoption?  
- How long do people remember stuff-ups?

Contactless / RFID / NFC Technologies

- No Notification At All  
  - Surreptitious Payment Extraction
- Real-Time Notification Provided (no record)  
  - Octopus, Drive-Through eTags for Road-Tolls
- Receipt Provided (or at least Offered)  
  - UK RingGo Parking Payment Scheme
- Act of Consent Required  
  - e.g. Tap the Pad in Response to Display of Fare
- Provision of Partial (Non-Secret) Details  
  - UK RingGo Parking Payment Scheme
- Provision of a Secret Authenticator  
  - PIN for Telstra/NAB/Visa payWave above US$ 25?

Some Factors to Consider

- **Apparent Risk**  
  - Apparent Size of Payment  
  - Monetary Value in Wallet/Purse  
  - Monetary Value in Account / Cr Limit  
  - Identifiers  
  - Authenticators
- **Frequency of Payment**  
- **Context of Payment**  
- **Fit to Life-Style:**  
  - Quick, Simple, Intuitive, ‘In’/Style/Fashion  
  - Confidence in ‘the System’, ‘the Parties’
**Possible Public Reactions**

- Sullen Acceptance
- Habituation
- Scepticism
- Opposition / Non-Adoption / Rejection

**Consumer Rights as an Enabler of MPayments**

- Architecture (e.g. Device Authentication)
- Audit and Certification
- Education and Awareness
- Liability Assignment
- Complaint Handling
- Recourse

But NZ Banks have just reduced Consumer Rights, and Aust Banks are lobbying for it!!

---

**Can Mobile Payments be ‘Secure Enough’?**

**Conclusion**

Mobile Payments can be
- Faster
- More Convenient
- Less of an Obstacle

**For the Thief Too**