Security of Electronic Transactions (Theory and Practice)

Jan Krhovják, Marek Kumpošt, Vašek Matyáš

Faculty of Informatics
Masaryk University, Brno

Outline

- Chip&PIN or signature cards – experiment
  - Anatomy of the experiment
  - Results of the Phase I & II
  - Summary of both phases
- EMV standard
  - Transaction processing
  - Selected security mechanisms
  - Other security implications

Anatomy of the Experiment

- The main question/objective
  - Is it easier for an opportunistic thief to abuse Chip&PIN or signature cards?
  - We wanted to see/have experimental practical results
- First (warm-up) phase (over 40 people involved)
  - Has taken place in pseudo-realistic conditions at a university bookstore (Masaryk U., Brno)
    - Age of the customers from 18 to 26 – “hired” students
    - Time to practice a signature limited to about 30 minutes
    - Time to practice “shoulder-surfing” about 2 hours
  - Not genuine payment cards (no verification of the PIN)
- Second phase (over 35 people involved)
  - Was realised in standard conditions
    - In one of the largest supermarket in Brno
    - Conditions set according to our experience from first phase
  - Genuine payment cards (real verification of the PIN)

Results of the Phase I

- PINpad 1 (security/privacy shielding)
  - Observers succeed in 6 from 17 PINs (35.3%)
    - They needed one guess in 5 from the 6 PINs (83.3%)
  - In 39 tips of 4-digit PINs (i.e., 156 digits)
    - 75 digits guessed correctly (48%)
- PINpad 2 (no shielding)
  - Observers succeed in 12 from 15 PINs (80%)
    - Just one guess needed in 10 out of 12 PINs (83.3%)
  - In 46 tips of 4-digit PINs (i.e., 184 digits)
    - 129 digits guessed correctly (70.1%)
- Signatures (15+17 customers)
  - Merchant detects 12 of 17 forging customers
    - 5 forging customers passed (29.4%)
  - 8 from 32 customers asked to sign twice
    - After second signing: 4 detected & 4 passed
  - We verified the signatures very carefully!!!

Results of the Phase II

- PINpads with & without security/privacy shielding
  - 13 obs. from shielded pad, 7 from unshielded pad
  - Observers succeed in 4 from 20 PINs (20%)
    - 3 PINs from shielded pads, one from unshielded pad
  - In 26 tips of 4-digit PINs (91 digits announced)
    - 38 digits guessed correctly (42%)
  - One (from three) observers group was more assertive and able to closely follow the targets => best results
    - Correct digits by groups: 25%, 27%, **68% (!)**
    - Third group: four correct PINs in 3 or less attempts
- Signatures (20 customers, stop after 17 succ. attempts)
  - 10–30 minutes for practicing a given signature
  - No problem reported from both the customers / till assistants
    - No one was asked to sign again or to show an ID
  - Some signatures were checked very poorly or not at all

Summary of Both Phases

- The signature forgers were newbies, as well as the shoulder-surfers
  - Correctly observed PIN digits (60% or 42%)
  - Significant difference between fake signatures detection (70% or 0%) – space for improvement
- Privacy shielding is really useful, however
  - Majority of PINpads not equipped by shielding
  - Light (=non-effective) privacy shielding in shops
  - Some customers may have motoric difficulties
- Temporary remedy (?)
  - Both PIN and signature
  - Different PINs for low- and high-level transactions?

EMV (Europay, MasterCard, and Visa) Standard

- EMV 4.1 specification (4 books with ~800 pages)
  - Interoperability & security of payment systems
    - Smartcards, payment terminals, banking HSMs
  - Introduction of Chip&PIN technology
    - Magnetic-stripe cards can be easily copied (skimming)

- Transaction processing (online or offline)
  - Authentication of on-card data
    - Offline detection of fake (altered/duplicated) cards
    - Static/dynamic data authentication
  - Authentication of cardholders/users
    - Based on handwritten signatures or PINs
    - Priority list of card-supported verification methods
  - Automatic risk analysis
  - Online transaction authorization

Selected Security Mechanisms

- Static data authentication (SDA)
  - On-card RSA signed static data
    - Send to the terminal for offline verification
    - No on-card asymmetric crypto => cheaper smartcards
  - SDA still allows skimming
- Dynamic data authentication (DDA)
  - Additional RSA key pair securely stored on card
    - On-card signing of random challenge from terminal
      => more expensive smartcards
  - DDA defeats skimming
- User authentication & card verification methods (CVM)
  - CVM list included in signed data only optionally
  - Adversary can modify this list of methods
    - PIN => handwritten signatures

Other Security Implications

- Problem of the EMV specification
  - Payment terminals protect interests of merchants
  - Payment cards protect interests of banks
  - Interests of customers are typically overlooked
- Malicious merchant can always cheat the customer
  - Copying the cards
  - Collecting of authorization data
  - Relay the EMV protocol
- Electronic advocate
  - Enters to the EMV protocol
  - Protects only interests of the customer
    - Portable electronic device between smartcard & terminal
    - Can display the details of each transaction & accept/reject

Conclusions

- Introduction of Chip&PIN does not improve customer protection against opportunistic thieves
  - Factor in problematic repudiation of false transactions
- Good PINpad privacy/security shielding recommended
  - The shop till clearly isn't the right place to enter PINs
- Verification based on signatures
  - Absolutely insufficient in a standard shop
  - Better, e.g., in jewellery
- Shoulder-surfing is an underestimated issue
  - Also in other (less "hostile") environments, e.g., office

- Security of EMV systems still dependent on particular implementation
- The system still protects mostly merchants and banks