Chip & PIN – beating the cheating?

Vashek Matyas, Dan Cvrcek, Jan Krhovjak
Masaryk University in Brno

Card transaction authentication

- Chip&PIN v. signature
  - We believe it increases the cost of card counterfeiting
  - We weren't sure whether it eliminates an opportunistic thief
    - Thief (or small loosely cooperating group of) pick-pocketing cards and forging signatures or observing PINs
- The main question/objective:
  - Is it easier for an opportunistic thief to abuse Chip&PIN or signature cards?
  - We need experimental practical results…

Anatomy of the experiment

- Two phases
- First (trial) phase
  - Has taken place in pseudo-realistic conditions at a university bookstore (Masaryk U. in 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
- Second phase
  - Will be realised in standard conditions
    - Most likely a jewellery in the Brno city-centre
    - Conditions set according to our experience from the first (trial) phase **and to third-party (your) feedback**!

Settings for the first phase

- Space needed
  - The shop/shopping center => Mareček’s bookstore
  - Room A for people to go shopping
  - Room B for people after shopping
- Over 40 people involved
  - Customers: 32
  - Observers-attackers: 4
  - Bystanders (innocent crowd): 3
  - Supervision: 3
  - Shop owner (assistant): 1
  - Another shop owner (experience with cards): 1

Normal behaviour?

- The customers not aware of the goal of the experiment => cover story – friendliness (& time)
- Each participant firstly filled a form for the cover story:
  - Questions target time needed for the two types of card authorisation, ...
  - … user comfort, and experience
- The merchants given the same cover story
  - level of awareness during signature verification is critical
- Signature forging explained to the “customers” after the first round (PINs)
- We promised participants more forms to fill after the experiment, but the truth was uncovered instead

Questionnaire evaluation

- A side-effect of the cover story – 32 filled forms…
- 25 out of 32 subjects use magnetic strip cards
- ½ of subjects have ever tried chip cards
- Overall satisfaction (1 – best, 5 – worst)
  - Magnetic cards/signature – 3.4
  - Smart cards/PIN – 2.5
- Max time for transaction (options 10, 20…50 sec)
  - 21 s
- Overall card transaction success rate
  - 89 % no problems, 7.5 % nuisance,
    2 % major problems, < 2 % failure

Round I – PINs

- Two PINpads used =>
  - Two groups of customers (17/15)
  - PINpad1 provides massive security/privacy shielding
- The shopping (one customer at a time)
  1. Customer enters the bookstore (filled with few other "customers" – observers and crowd).
  2. Customer leaves the bookstore
  3. Observers report their results
  4. Supervisor records time (accordingly to the cover story)
  5. Back to step 1
- Question of a cheating merchant
  - In reality easy => e.g. CCTV focused on till/PINpad
  - Not considered in the experiment

Round II – signatures

- Two groups
  - 15 customers given an empty strip to be signed
  - 17 customers given a signature to forge
    - Practicing signatures for 20-30 minutes in room B
- Execution – merchant used to accepting cards
  - Room B – customer gets a card with own/ to-be-forged signature
  - Merchant checks signatures – identifies forgeries
  - Merchant knows some customers cheat, but doesn't know how many

Remark: Customers and supervisors agree that the signature check was being (too) thorough – not the case in real-life shopping (jewellery syndrome? ☺)

Results of Round I (PINpad1)

- Observers succeed in 6 from 17 PINs (35.3%)
  - Shared knowledge
  - No verification of the PIN as entered by the customer ☹
  - They needed one guess in 5 from the 6 PINs (83.3%)
    - 3 PINs seen by 2 observers
    - 2 PINs seen by 1 observer
    - 1 built from shared knowledge / combining observations
- In 39 tips of 4-digit PINs (i.e. 156 digits)
  - 75 digits guessed correctly (48%)

Results of Round I (PINpad2)

- Observers succeed in 12 from 15 PINs (80%)
  - Shared knowledge
  - No verification of the PIN as entered by the customer ☹
  - Just one guess needed in 10 out of 12 PINs (83.3%)
    - 2 PINs seen by 4 observers
    - 1 by 3 observers
    - 4 by 2 observers
    - 3 by 1 observer
    - 2 built from shared knowledge
- From 46 tips of 4-digit PINs (i.e. 184 digits)
  - 129 digits guessed correctly (70.1%)

Results of Round II – signing

- Merchant detects 12 of 17 forging customers
  - 5 forging customers passed (29.4%)
- From the 12 detected customers
  - 8 detected immediately after the 1st signature (25%)
  - 4 detected after the second signature (12.5%)
- From the 20 (15+5) “successful” customers
  - 16 passed immediately after first signing (50%)
  - 4 passed after second signing (12.5%)
- 8 customers (25%) asked to sign twice
  - We verified the signatures very carefully!!!
  - One customer gave up the second signature ☺

Interesting observations

- Privacy shielding is really useful, however
  - Majority of PINpads not equipped by shielding
  - We used two extremes no and heavy shielding
  - Some customers may have motoric difficulties
- Observers succeed in the last digit guess in 28 from 32 trials (87.5%)
- Average time of transactions
  - Round I (PINs): 25.5 s
  - Round II (signatures): 38.5 s
- The signature forgers were newbies, as well as the shoulder-surfers

Conclusions (so far…)

- Introduction of Chip&PIN doesn't improve customer protection against opportunistic thieves
  - Factor in problematic repudiation of false transactions!
  - Why replacing a weak biometric with a weaker secret?
    - Open field for useful applied R&D!
  - Temporary remedy(?)
    - Both PIN and signature
    - Different PINs for low- and high-level transactions?
- PINpad privacy/security shielding recommended
  - Yet the heavy version still no better than signatures
  - The shop till clearly isn't the right place to enter PINs (as used today)

Questions & Discussion - Towards the next phase

- We shall
  - Automatically check the correctness of keyed-in PINs
  - Or better do real transactions – BUT… ☹
    - Would anyone know a suitable sponsor? ☺
- Is the cover story right
  - and should it be same for customers and merchants?
- How to achieve "realistic" security for signature verification and shouldersurfing detection?
- How to set same/similar conditions for training signature forgers and PIN observers?