Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond
University of Cambridge

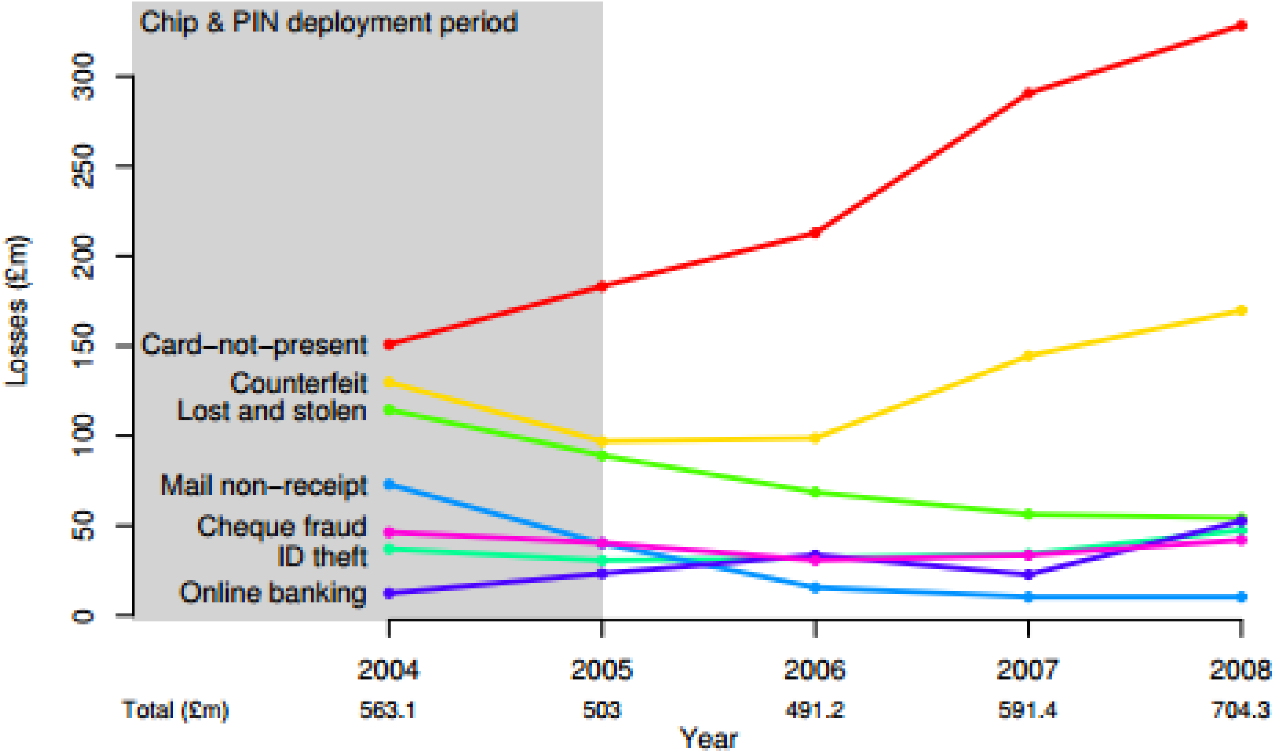
S&P 2010

Presented by: Yi Zhang
September 1 2016

EMV Card

- As of early 2008, there were **730 million** EMV cards in circulation.
- EMV Card claimed to secure transactions by “**Chip and PIN**”:
  - ✓ Allows PIN-based authentication, even for offline transactions
  - ✓ Chip to prevent card counterfeiting
  - ✓ PIN to prevent abuse of stolen card

Effect on Fraud



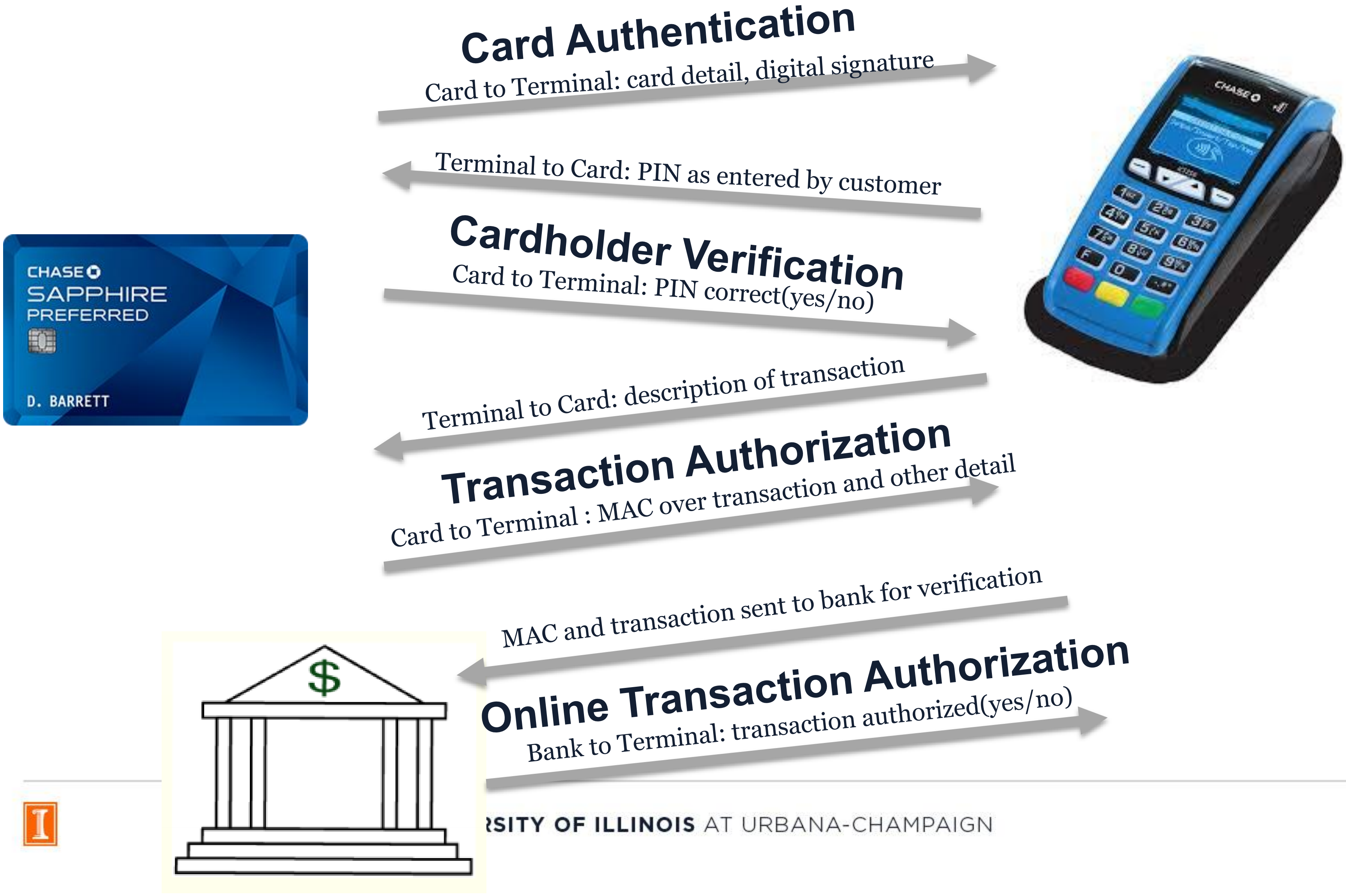
Banks claim EMV is infallible, so victims could not get their money back.

They were wrong

- In the paper, the authors demonstrate a protocol flaw which allows criminals to use stolen EMV cards ***without*** knowing the PIN.
- A man-in-the middle attack is possible to trick the terminal and the card.
- Live demonstration:

https://www.youtube.com/watch?v=1pMuV2o4Lrw

A simplified EMV transaction



Card Authentication

Card to Terminal: card detail, digital signature

Terminal to Card: PIN as entered by customer

Cardholder Verification

Card to Terminal: PIN correct(yes/no)

Terminal to Card: description of transaction

Transaction Authorization

Card to Terminal : MAC over transaction and other detail

MAC and transaction sent to bank for verification

Online Transaction Authorization

Bank to Terminal: transaction authorized(yes/no)

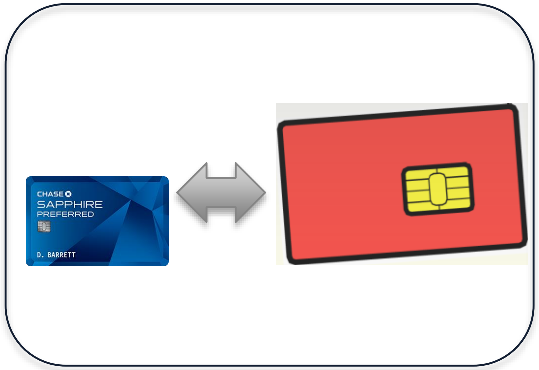
What went wrong?

- In *Cardholder Verification* phase, the PIN is verified offline.
  - The card returns 0x9000 if PIN matches, otherwise returns 0x63cX, where X is the number of further PIN verification attempts.
  - The card response is NOT directly authenticated.
- In *Transaction Authorization* phase, the authenticated information could NOT provide an unambiguous encoding of the events which happened in the protocol run.
  - The TVR generated by the terminal in the transaction description is only set if PIN verification has been attempted and *failed.*
  - The IAD generated by the card contains information about whether PIN verification was attempted but could be parsed by the terminal.
  - The bank does not know the cardholder verification method chosen, thus could not use IAD to prevent the attack.

How does the attack works?

Card Authentication

Card to Terminal: card detail, digital signature



Terminal to MitM: wrong PIN entered by criminal

Cardholder Verificatio

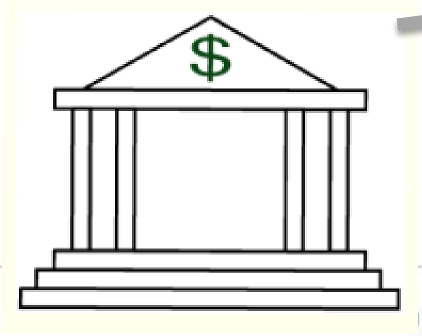
MitM to Terminal: PIN

Card: No (not required)
Terminal: No
(was entered)

Terminal to Card: descrip

Transaction Autho

Card to Terminal : MAC over transaction and other



MAC and transaction sent to bank for verification

Online Transaction Authorization

Bank to Terminal: transaction authorized(yes/no)

Possible Fix

- Terminal parses IAD
  - IAD is only intended for the issuer and has several different format.
- The card request CVMR to be included in the transaction description from the terminal
  - Whether this works depends on the bank system.
  - Actual implementation doesn't meet the specification.

Discussion

- What are the key contributions of the paper?
- Criticisms / limitations of the paper ?
- What is the root cause of the problem?
- How could we identify the flaw in the protocol design?

Certification of Symbolic Transaction

- Erich chen, Shuo chen, Shaz Qadeer, Rui Wang

  Microsoft Research
- Security and Privacy (Oakland) 2015
- Website:

  https://www.microsoft.com/en-us/research/project/certification-of-symbolic-transaction/

Problem

- Security flaws is prevalent in multiparty online service.
  - The Cloud Security Alliance cites these logic flaws in online services as “Insecure Interfaces and APIs”, the No.4 cloud computing threat.
- Why so many logic flaws?
  - There is no global data storage.
  - Security is a global property. Local checks at each party sometimes is NOT sufficient to imply the global property.

CST Approach

- Tries to verify protocol-independent safety property joint defined over all parties.
- Idea:
  - Collect the trace along the protocol run.
  - Synthesize a program from the collected trace.
    - Discard the trace performed at untrusted party or not tamper-proof.
  - Verify the program against safety property.