Chip and PIN internals

Omar Choudary
University of Cambridge

work in collaboration with the members of the security group

Last updated: 14/11/2011

The issue

Q: Are smart card payments secure?

UK Payments:

"In line with NFSA's statement that "Fraud costs every person in the country £231 per year", if you were to apply our figures in the same context:

Card fraud costs every person in the country £10 per year..."

http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/

... Chip & PIN users support the fraud

- Many cases in which card users are blamed for fraudulent transactions
- Banks claim that a PIN was entered, the card was present so it must have been the customer
- Even organisms such as Ombudsman may not help
- Sometimes it can be a family member
- But there can also be other reasons ...

Mafia relay attack

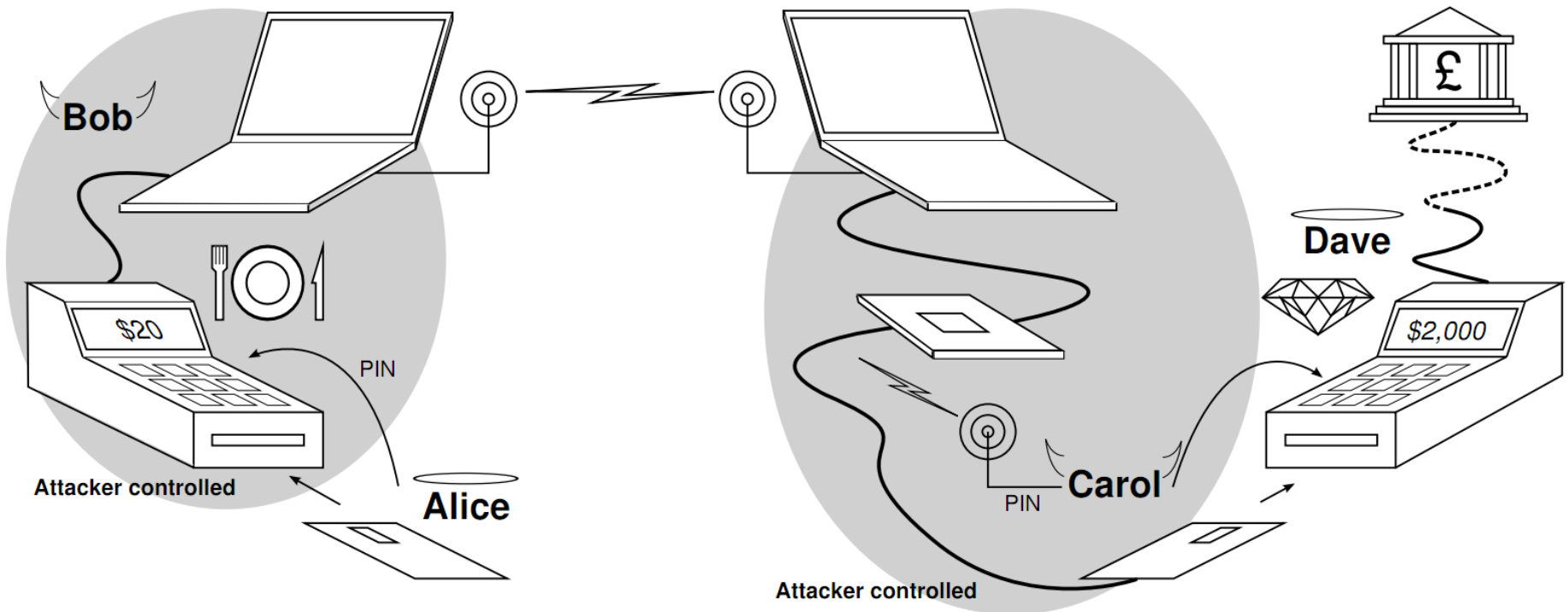


Image from *"Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks"*, Saar Drimer and Steven Murdoch

Mafia relay attack - implemented

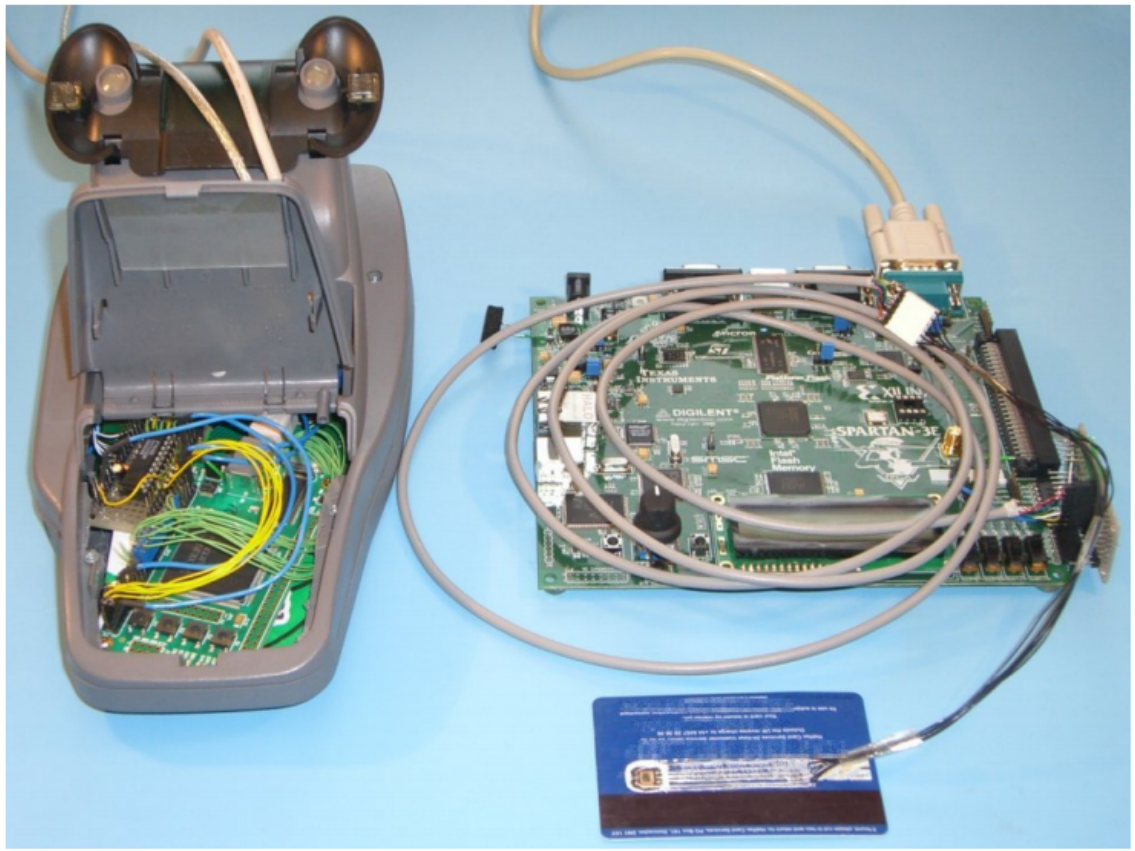
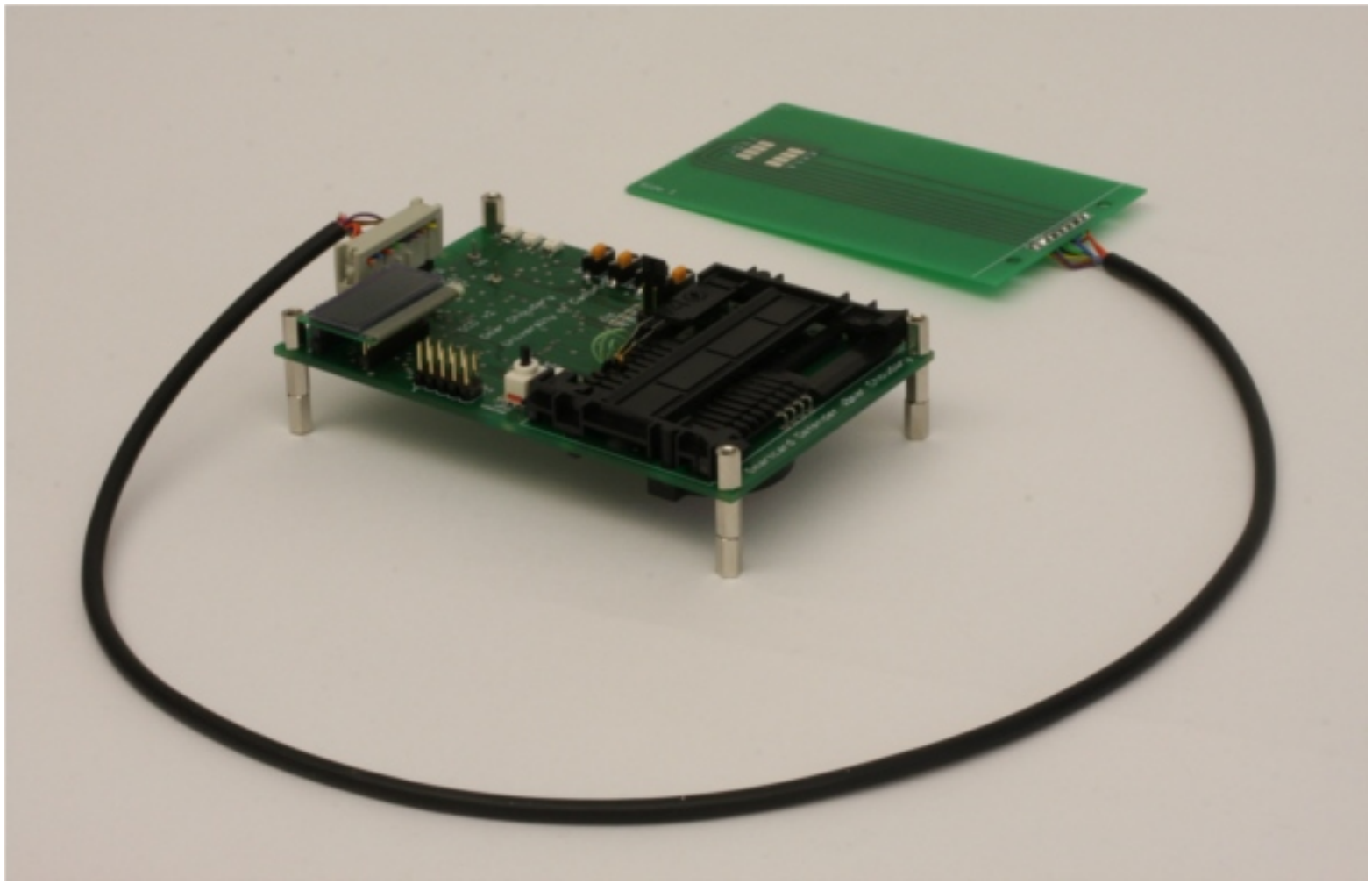


Photo from *"Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks"*, Saar Drimer and Steven Murdoch

How to defend against mafia fraud?

- Distance bounding: measure communication delay
  see "Keep your enemies close..." by Drimer and Murdoch
- Create a kind of hop-count metric:
  see "Make noise and whisper..." by Choudary and Stajano
- Or, as a quick practical solution, we could add a trusted display...

... the Smart Card Detective (my MPhil thesis, Cambridge 2010)

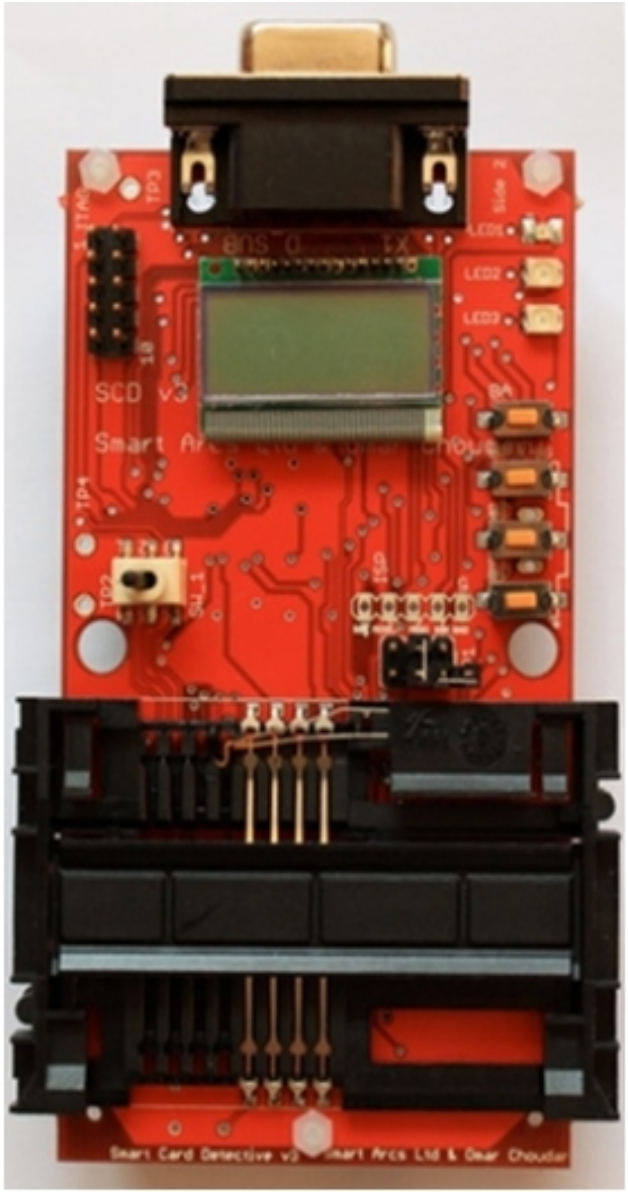


See my MPhil thesis *"The Smart Card Detective: a hand-held EMV interceptor"*, Omar Choudary

SCD Overview

- Trusted display and buttons
- smartcard and terminal interfaces
- EEPROM to log transaction data
- intercept and modify active transactions
- Currently available from Smart Architects as a general smart card research framework

  http://www.smartarchitects.co.uk/opencart/



SCD: stop relay attack

Protocol attacks

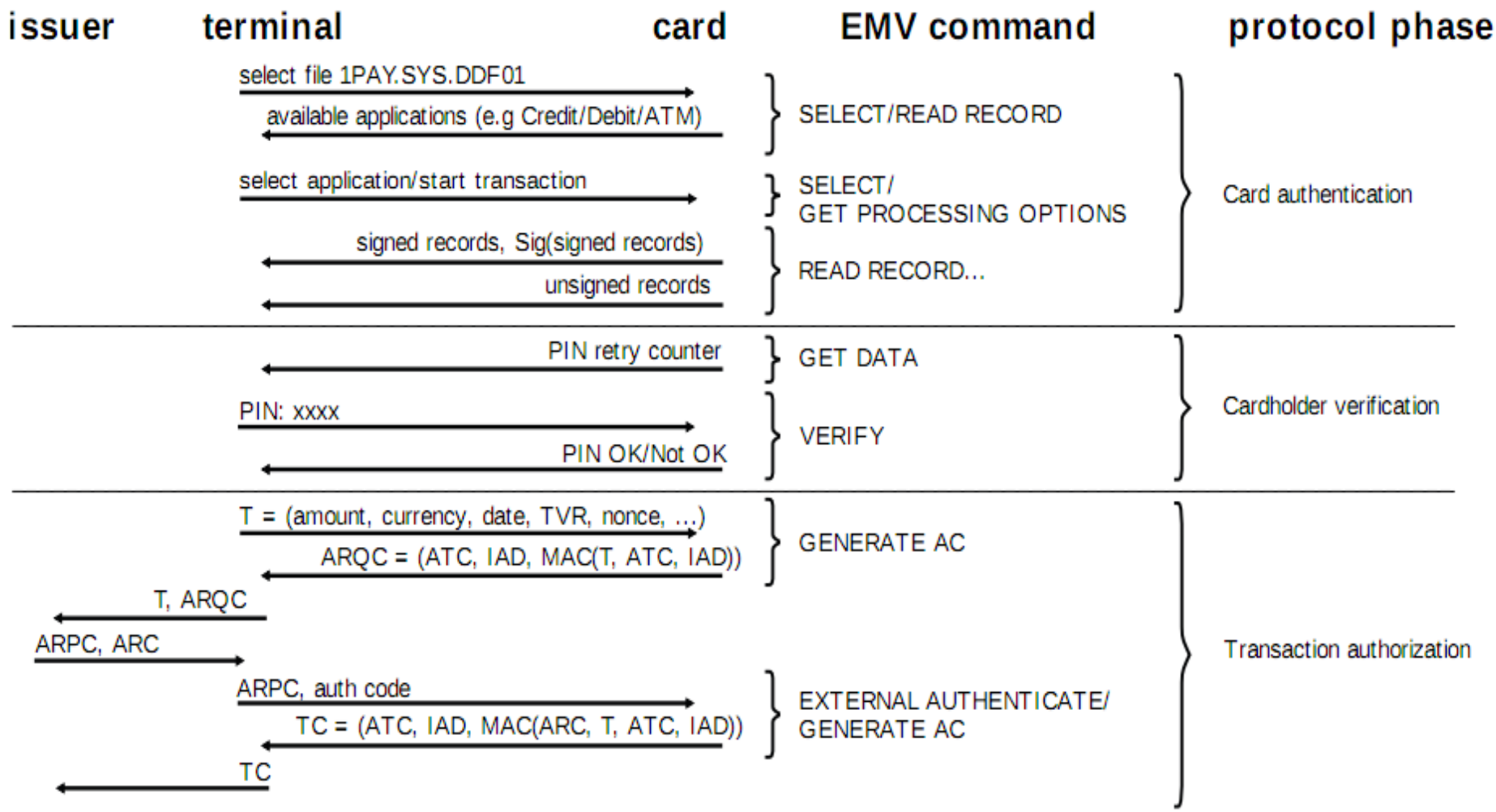
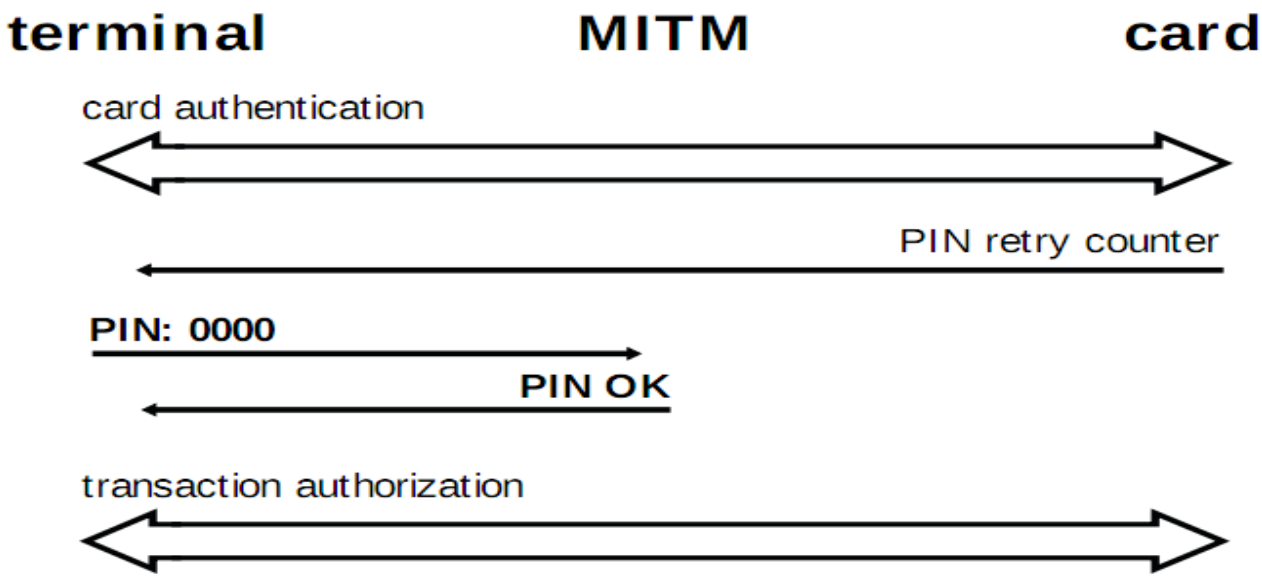


Figure 2. A complete run of a Chip and PIN protocol.

Schema from "Chip and Pin is broken" by Murdoch et al.

NO PIN needed! - Murdoch and Drimer



See *"Chip and PIN is broken"*, Steven Murdoch, Saar Drimer, Ross Anderson, Mike Bond

Banks were told since November 2009

Banks' response: hard to implement

Fraudes à la carte bancaire : pas de panique

le vendredi 22 janvier 2010 à 04:00

"The method requires heavy equipment, a computer must be connected to the terminal. It will take time for miniaturization of such equipment, " stated Jean-Marc Bornet on Thursday, director of the Group CB cards in the columns of Le Figaro.

« Nous pouvons remercier Ross Anderson. Grâce à lui, nous allons pouvoir déjouer la faille avant que les fraudeurs ne la découvrent », indiquait jeudi la Banque de France. Ce professeur de sécurité informatique anglais a réussi à contourner le code secret des cartes de paiement à puce, pourtant réputées bien plus sûres que les cartes magnétiques. Depuis lors, les banques européennes se mobilisent pour contrecarrer ce risque de fraude, et se montrent rassurantes.

« Le procédé requiert un matériel lourd, un ordinateur, qui doit être branché sur le terminal de paiement. Il faudra du temps pour miniaturiser un tel équipement », indiquait jeudi Jean-Marc Bornet, administrateur du Groupement des **cartes bancaires** CB, dans les colonnes du *Figaro*. En outre, le leurre ne trompe pas les serveurs lorsque les transactions font l'objet d'

Our response: not so hard... use SCD

See Canal+ reportage:
http://www.cl.cam.ac.uk/~osc22/media/frenchtv_scd.avi

... then decided to publish the SCD source files in our blog:
http://www.lightbluetouchpaper.org/

UKCA: take-down research request

I am writing as Chair of The UK Cards Association to draw your attention to our concerns regarding a research paper published earlier this year by a University of Cambridge student, details of which were published prominently on the University's Light Blue Touchpaper web site on 19 October. It is our belief that this web publication oversteps the boundaries of what constitutes responsible disclosure.

Our key concern, therefore, is that this type of research was ever considered suitable for publication by the University. It gives us cause to worry that future research, which may potentially be more damaging, may also be published in this level of detail.

Concern has also been expressed to us by the police that the student was allowed to falsify a transaction in a shop in Cambridge without first warning the merchant.

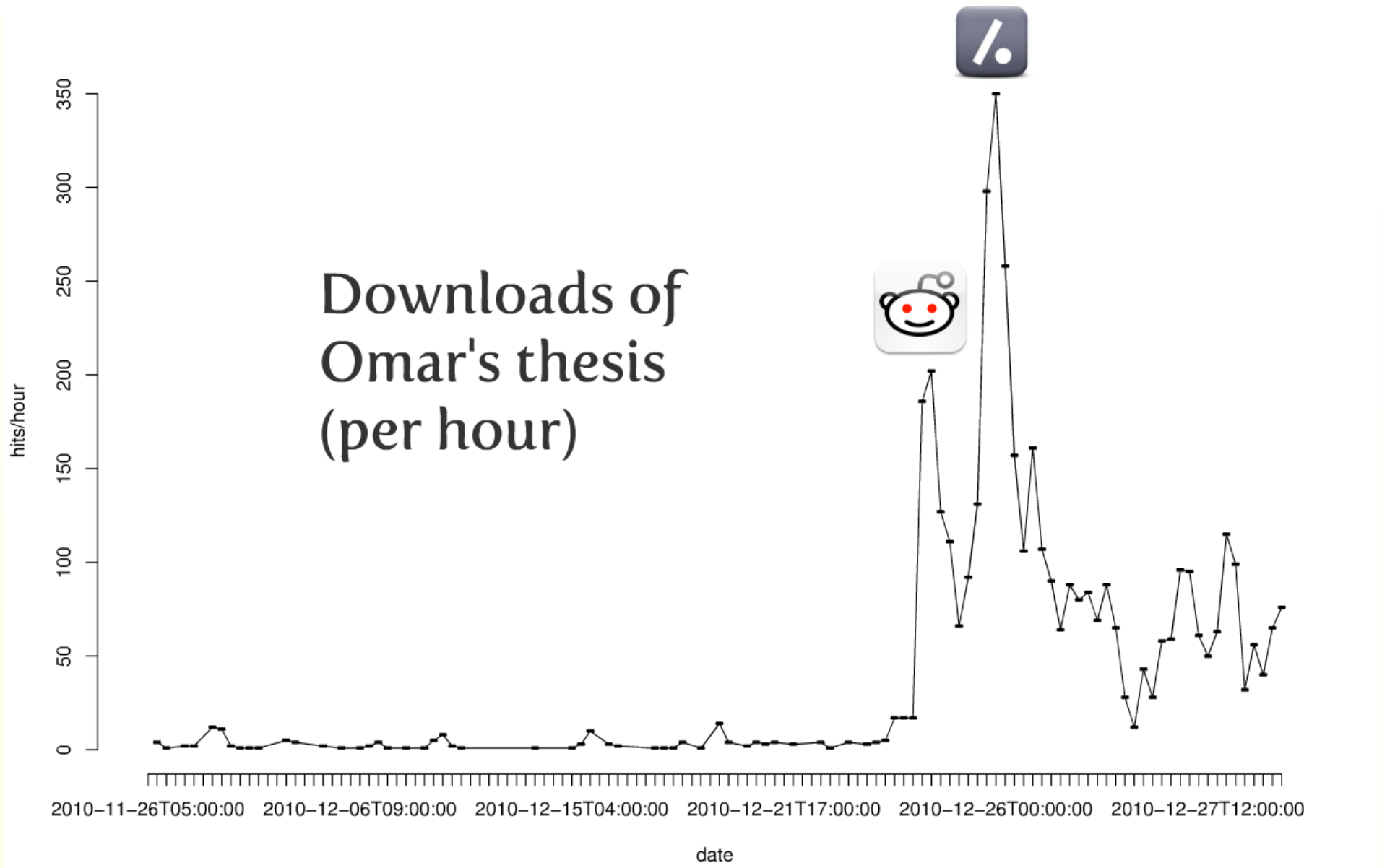
Consequently, we would ask that this research be removed from public access immediately and would hope that you are able to give us comfort about your policy towards future disclosures.

UKCA: our response

Second, you seem to think that we might censor a student's thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values. Thus even though the decision to put the thesis online was Omar's, we have no choice but to back him. That would hold even if we did not agree with the material! Accordingly I have authorised the thesis to be issued as a Computer Laboratory Technical Report. This will make it easier for people to find and to cite, and will ensure that its presence on our web site is permanent.

You complain that our work may undermine public confidence in the payments system. What will support public confidence in the payments system is evidence that the banks are frank and honest in admitting its weaknesses when they are exposed, and diligent in effecting the necessary remedies. Your letter shows that, instead, your member banks do their lamentable best to deprecate the work of those outside their cosy club, and indeed to censor it.

Result of press incident



Plot produced by Steven Murdoch

1 year later: ITV Tonight February 2011

http://www.cl.cam.ac.uk/~osc22/video/itv_tonight_no_pin.avi

- Tests with 10 Chip and PIN cards from different banks
- All cards are still vulnerable to the NO PIN attack

More implementation-related problems

- Card cloning and skimming
- Online banking (in)security
  "Optimised to fail: card readers for online banking" by Drimer et al.
- Most PINs are chosen from known dates
  (study in progress by Joseph Bonneau)
- Protection against some attacks (e.g. separate ATM slots for magnetic/card entries) might enable others (e.g. relay)
- NFC is arriving ... watch out for malware, relay attacks, etc.

System-wide problems

- Complex specification => hard to get it right
  - many optional parts, some banks do it right, others don't
- Back-end system update costs money and perhaps fix leads to other problems
- We've found incorrect card setups:
  - Barclays card performing 128 byte DDA signature where DDA is not available
- Certification process relies on external labs and is closed: "*Implementation reviews will be conducted for financial applications, to ensure a high level of assurance. This testing will include code reviews and penetration testing.*"
  - documentation lacks details of EMV implementation tests

Q: Are payment smart cards secure?

Answer: it depends

- EMVCo evaluation checks against many physical and brute force protocol attacks
  - but only for general applications
  - doesn't certify bank's back end system
- Specification is designed to be flexible
  - but is too complex
- The protocol, on paper, doesn't have important holes
  - but as always, the devil is on the implementation
- Authorities don't appear to align incentives well enough

Questions

Presenter:
Omar Choudary
omar.choudary@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~osc22/

Smart Card Detective:
http://www.smartcarddetective.com

Light Blue Touchpaper Blog:
http://www.lightbluetouchpaper.org/