Can we redesign mobile payments to deal with poor networks and cut transaction fees?

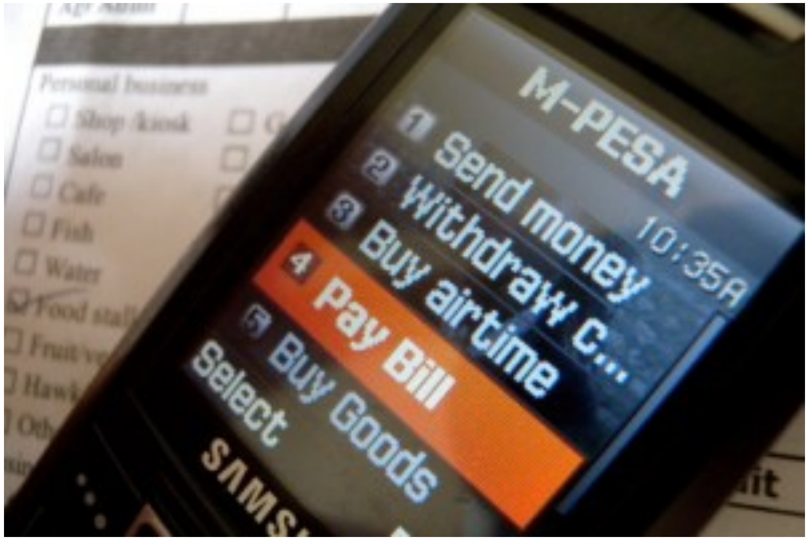
Ross Anderson and Khaled Baqer

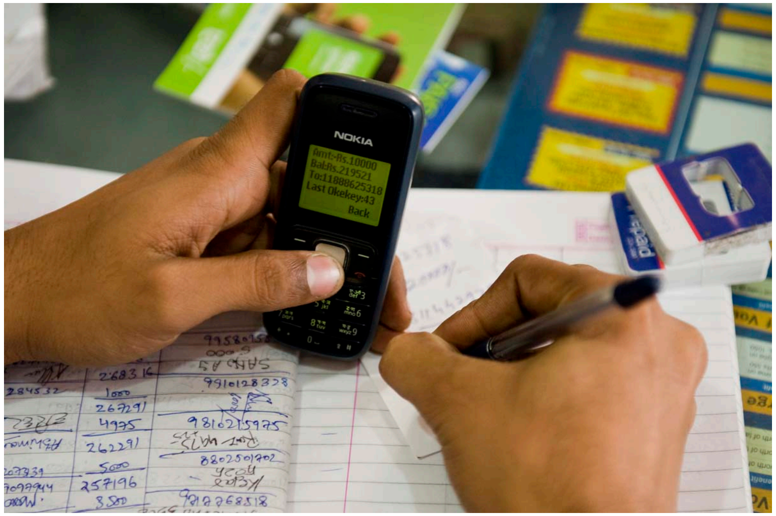
University of Cambridge

Computer Laboratory

Nairobi, August 29 2016

The mobile money revolution





Mobile money achievements

- Helped poorest communities in many ways!
- Brought banking services to hundreds of millions who didn't have them
- Built mechanisms for direct payments and remittances; store of value; personal safety; transaction history; access to credit
- Provided direct channel for government payments and services
- Connected lots of people to the online world

What are the remaining challenges?

- Is our priority to:
- Extend payments to areas with no mobile service (mountains, deserts, islands)?
- Make service still work when network service intermittent (congestion, power cuts)?
- Cut network charges / transaction fees?
- Establish standards and interoperability for international remittances?

Who we are

- Cambridge University Computer Laboratory is interested in payment security and fraud
- The Cambridge Cybercrime Centre now collects data on online scams and abuse
- During the 1990s we studied fraud on ATMs using magnetic-strip cards
- We helped develop the STS prepayment meter systems used to electrify millions of households (South Africa, Brazil … even Kenya!)

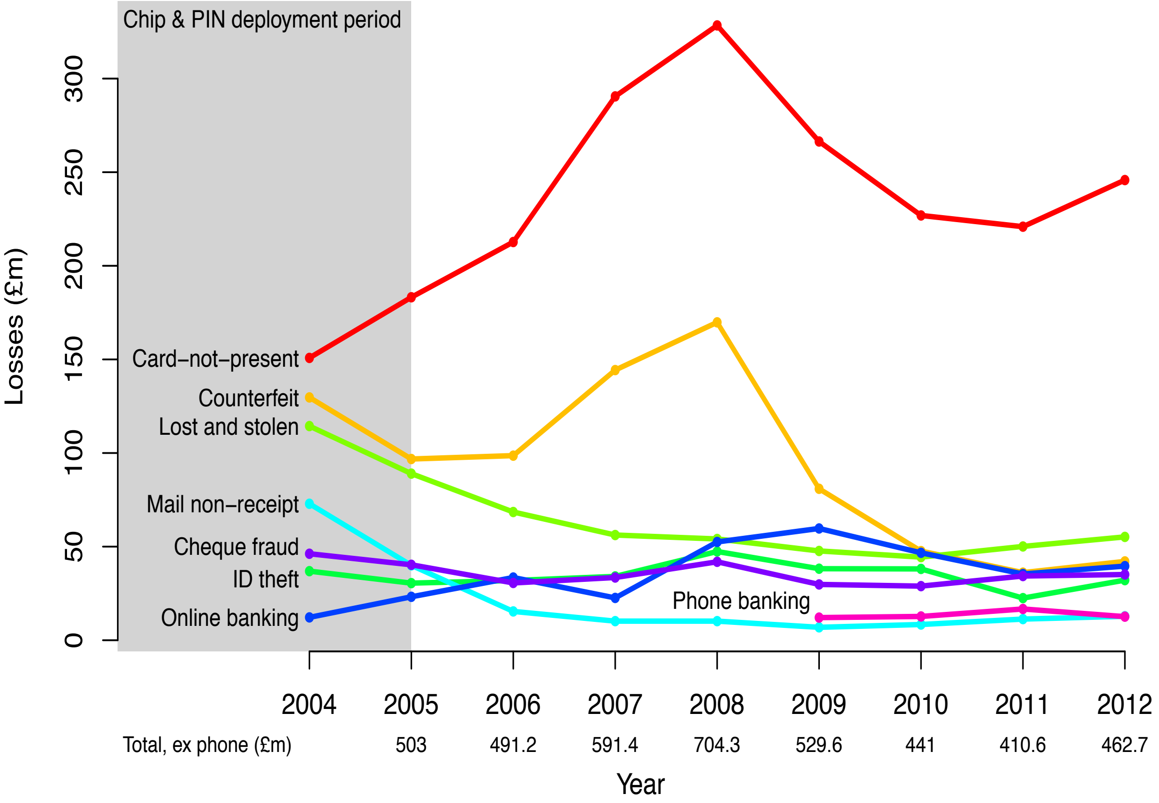
EMV ('Chip and PIN')

Chip and PIN

EMVCo

- Deployed in Europe and elsewhere since 2003–5
- 'Liability shift' – disputes are charged to the card holder if PIN was used, else to the merchant
- Changed many things, not always in the ways banks expected…

Fraud history, UK

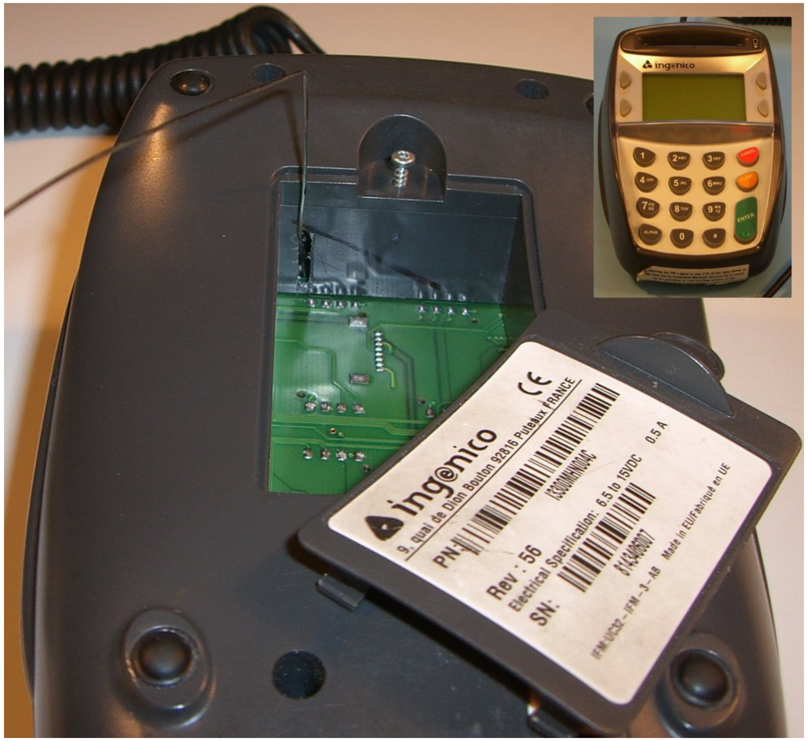


- Cardholder liable if PIN used
- Else merchant pays
- Banks hoped fraud would go down
- It went up …
- Then down, then up again

Attacks on EMV in the real world

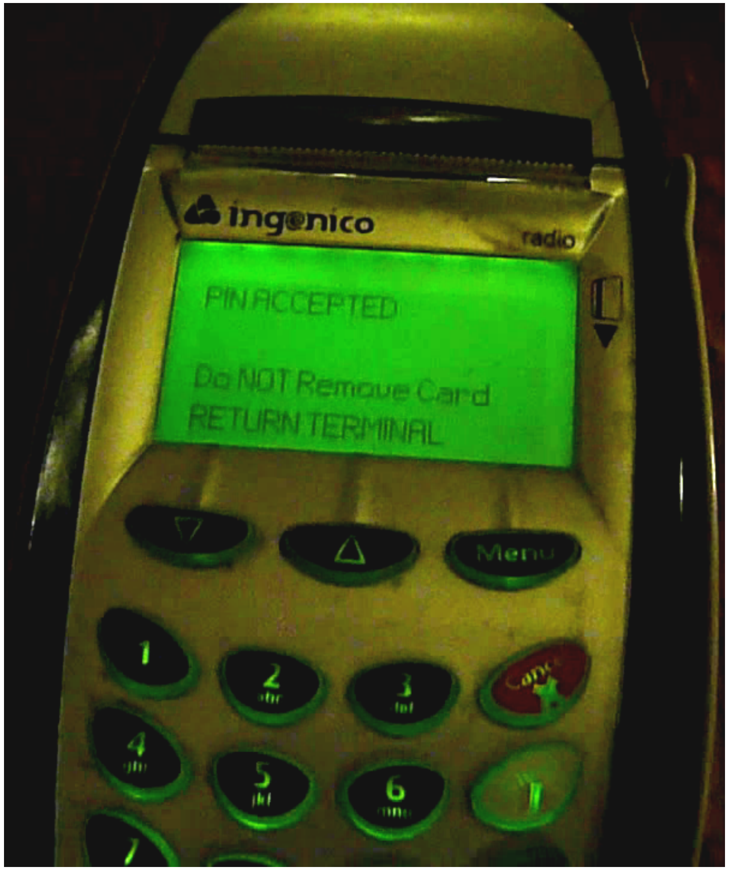
- The first thing the bad guys did was to go for mail order, phone order and Internet fraud
- Then mag-strip fallback fraud ballooned as people were now entering PINs everywhere
- PEDs tampered at Shell garages by ‘service engineers’ (PED supplier was blamed)
- Then ‘Tamil Tigers’
- After fraud at BP Girton: we investigate

TV demo: Feb 26 2008


ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
PN:
Rev : 56
Electrical Specification: 6.5 to 15VDC 0.5A
SN:
Made in EU/Fabriqué en UE
ENTER

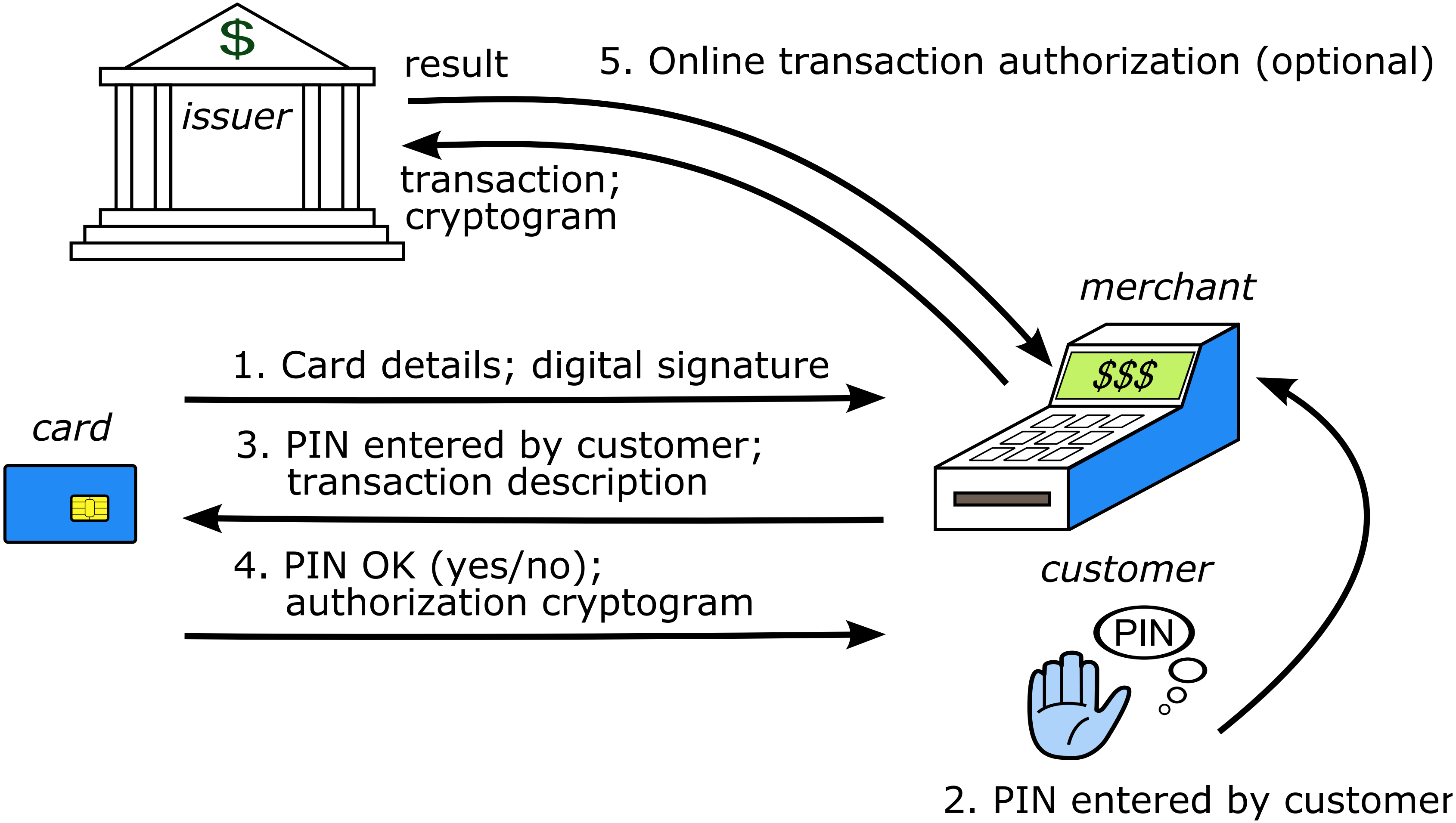
- PEDs ‘evaluated under the Common Criteria’ were trivial to tap
- Acquirers, issuers have different incentives
- Banks said (Feb 08) it wasn’t a problem…
- Khan case (July 2008)
- Trial (Oct 2011): banks offered no evidence…

The ‘No-PIN’ attack



- Victims told us: crooks seem to be able to use a stolen card without knowing the PIN
- How? We found: insert a device between card & terminal
- Card thinks: signature; terminal thinks: pin
- TV: Feb 11 2010

A normal EMV transaction



issuer

result

5. Online transaction authorization (optional)

transaction;
cryptogram

merchant

1. Card details; digital signature

card

3. PIN entered by customer;
transaction description

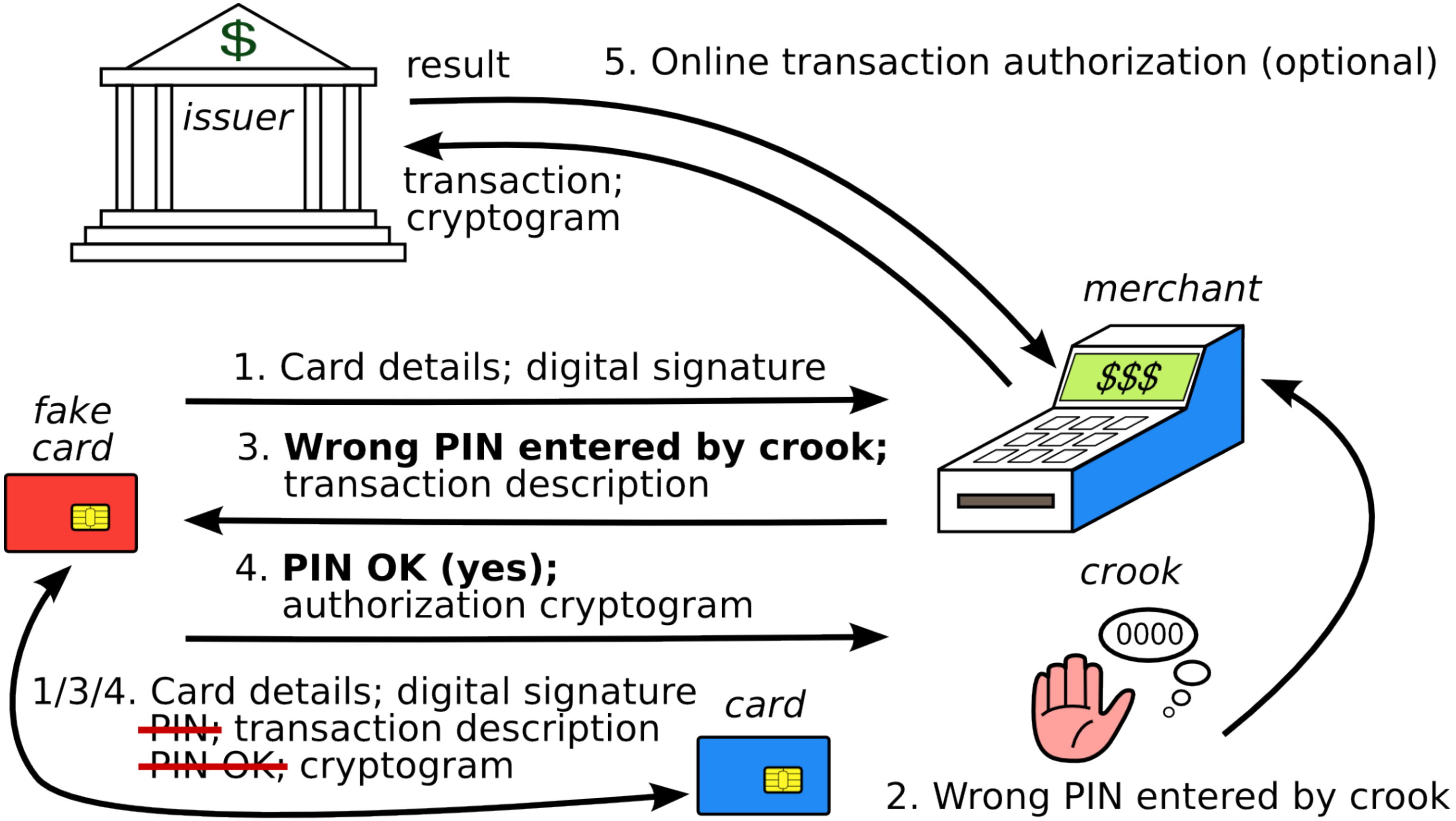
4. PIN OK (yes/no);
authorization cryptogram

customer

PIN

2. PIN entered by customer

A ‘No-PIN’ transaction


issuer
$
result
5. Online transaction authorization (optional)
transaction;
cryptogram
merchant
$$$
1. Card details; digital signature
fake
card
3. **Wrong PIN entered by crook;**
transaction description
4. **PIN OK (yes);**
authorization cryptogram
crook
0000
1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram
card
2. Wrong PIN entered by crook

EMV and Random Numbers

- In EMV, the terminal sends a random number N to the card along with the date d and the amount X
- The card computes an authentication request cryptogram (ARQC) on N, d, X
- What happens if I can predict N for d?
- Answer: if I have access to your card I can precompute an ARQC for amount X, date d

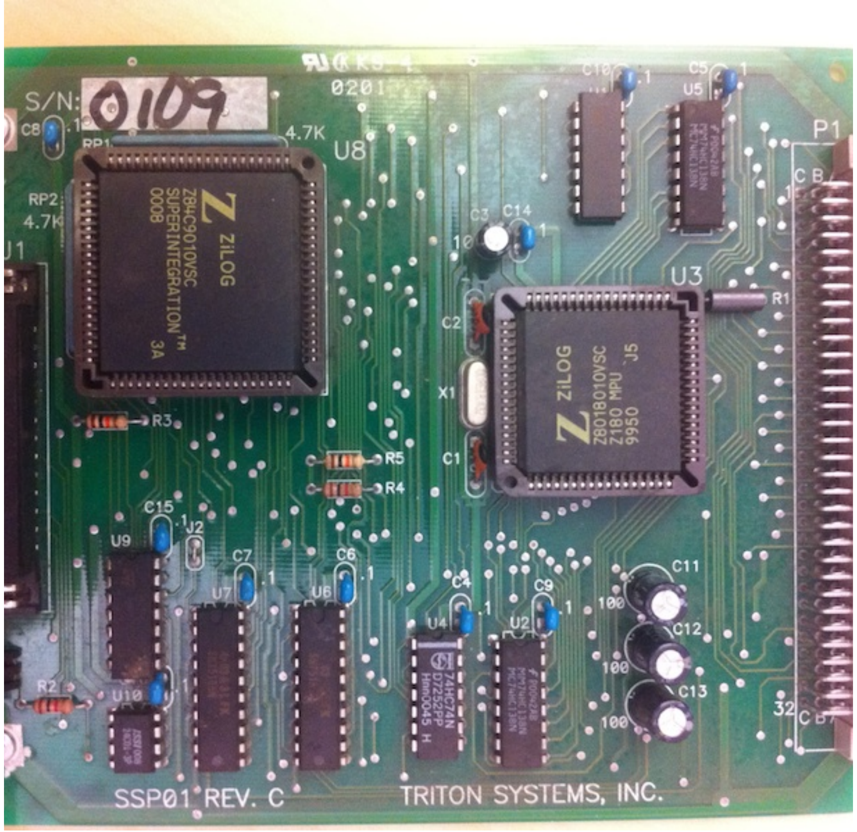
ATMs and Random Numbers (2)

- Log of disputed transactions at Majorca:

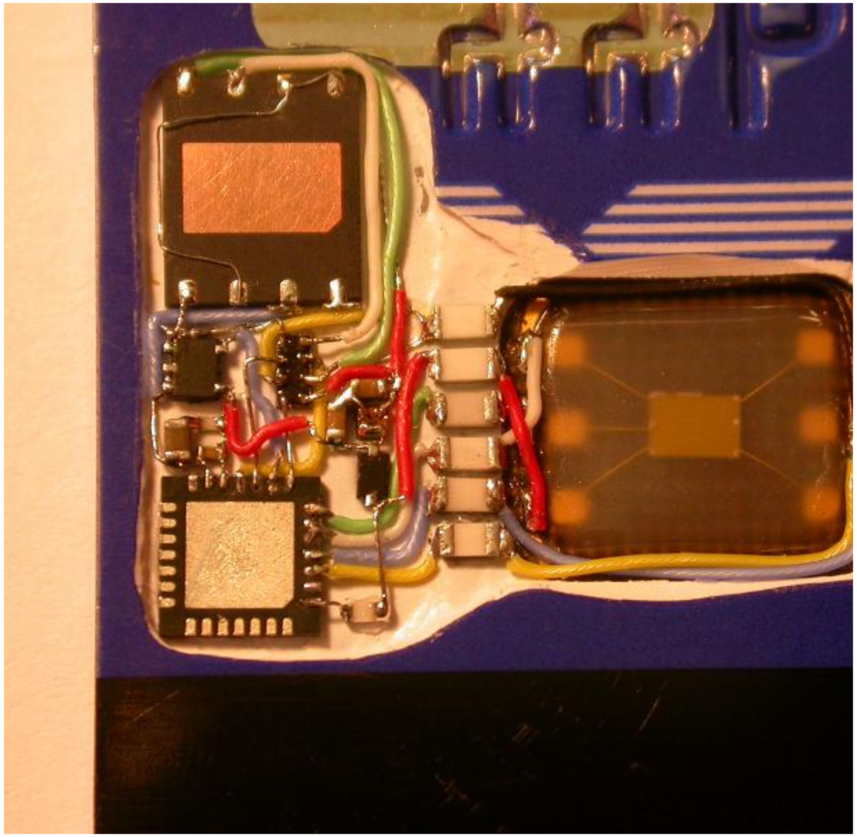
```
2011-06-28          10:37:24          F1246E04
2011-06-28          10:37:59          F1241354
2011-06-28          10:38:34          F1244328
2011-06-28          10:39:08          F1247348
```

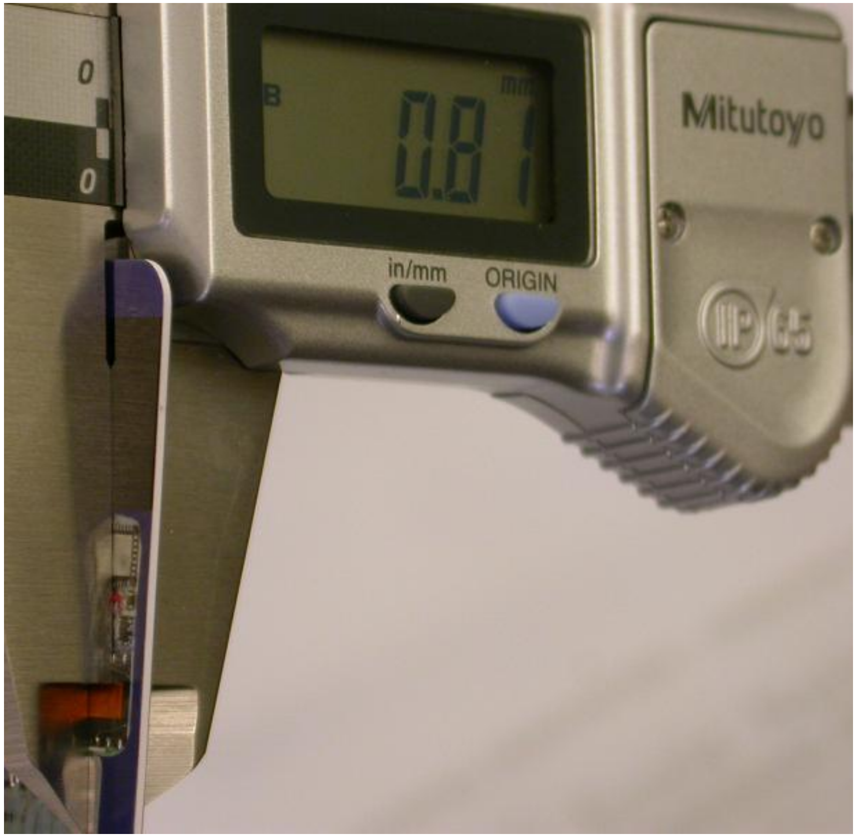
- N is a 17 bit constant followed by a 15 bit counter cycling every 3 minutes
- We test, & find half of ATMs use counters!

ATMs and Random Numbers (3)



ATMs and Random Numbers (4)





The preplay attack

- Collect ARQCs from a target card
- Use them in a wicked terminal at a collusive merchant, which fixes up nonces to match
- We won an interesting test case in 2015…
- Sailor spent €33 on a drink in a Spanish bar. He got hit with ten transactions for €3300, an hour apart, from one terminal, through three different acquirers, with ATC collisions
- So: how can we apply all this to mobile?

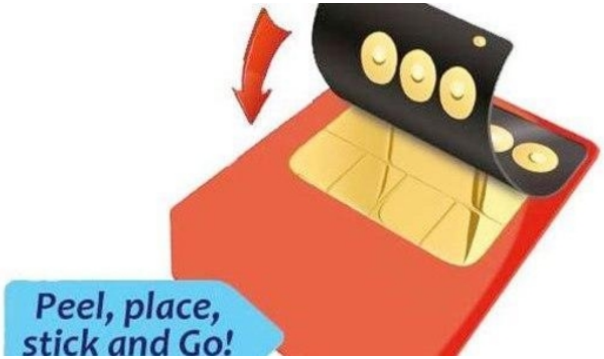
The DigiTally project

- The Gates Foundation asked for ideas to increase merchant use of mobile money
- We talked to operators and users in several countries: issues were network access, costs
- So: how can you do a payment between two phones when there's no GSM signal?
- It's easy with two smartphones, but what about basic handsets?

DigiTally

- DigiTally is a prototype purse system we've built to do research on offline mobile payments
- It works by copying short authentication codes from one phone to another
- Our prototype is implemented in overlay SIMs for use in simple phones
- It can also be implemented in your SIM toolkit or as a smartphone app

Overlay SIMs



- Tamper-resistant SIM
- Sticks on top of the regular SIM
- Bypasses the mobile network operator
- Independent secure device, like SE in NFC
- Can be used to compute authorization codes, just as in EMV

DigiTally payment, step 1

- Alice wants to pay Bob $4 for a taxi ride
- The first step is for each of them to give the other their phone number which they each enter into their DigiTally menus
- This is just like in current systems, where Alice and Bob use the phone system to verify and store each other's phone numbers

DigiTally payment, step 2

- Bob then enters the amount, “$4” on his phone
- It shows an 8-digit authorization request, say ‘4761 0825’ which he reads to Alice
- She taps “$4” and “4761 0825” on her phone
- If they agree on the two phone numbers and the amount, then Alice’s phone proceeds to the next stage

DigiTally payment, step 3

- Alice enters her PIN (just like in a normal phone payment)
- Her phone displays “$4 paid” and an 8-digit authorization response, say “6409 3527”, which she reads to Bob
- He taps in the code
- If it’s correct, his phone displays “$4 received” with a full log of the transaction

Usability lessons learned

- Prepayment meters widely introduced 20 years ago (South Africa, Brazil, Kenya …)
- People have no difficulty copying 20 digits

Operations

- As now, village agent recruits customers, merchants, and installs overlay SIMs in their phones
- And customers pay money to load their purse
- And the payment service operator maintains a system of shadow purse accounts
- All that changes is that whenever a customer or merchant goes into an area with working network service, the overlay SIM uploads transaction history

Security case

- Implementation in tamper-resistant overlay SIMs or other secure products acceptable to the banks
- Cryptography can use AES or 3DES to generate authentication codes
- The payment protocol was formally verified and sent to the Security Protocols Workshop this spring for peer review
- Here is the basic version…

Under the hood

- When Alice agrees to pay Bob X, each of them enters both this amount and the other party's phone number into their phones
- Bob chooses a 4-digit nonce N_B and forms a 4-digit MAC C (using the shared secret key K) of B and X
- He tells Alice the 8 digits

$$(N_B, C) \text{ where } C = MAC_K\{B,A,X,N_B\}$$

Under the Hood II

- Alice types in the digits, verifies the MAC, then authorises the transaction (using her PIN)
- It decrements the value counter by X, creates a 4-digit nonce and computes a 4-digit response which she reads or shows to Bob:

$$(N_A, R) \text{ where } R = MAC_K\{A, N_A, X, N_B, B\}$$

- Bob enters the 8 digits (N_A, R) into his phone, and checks that it increments by X

DigiTally benefits

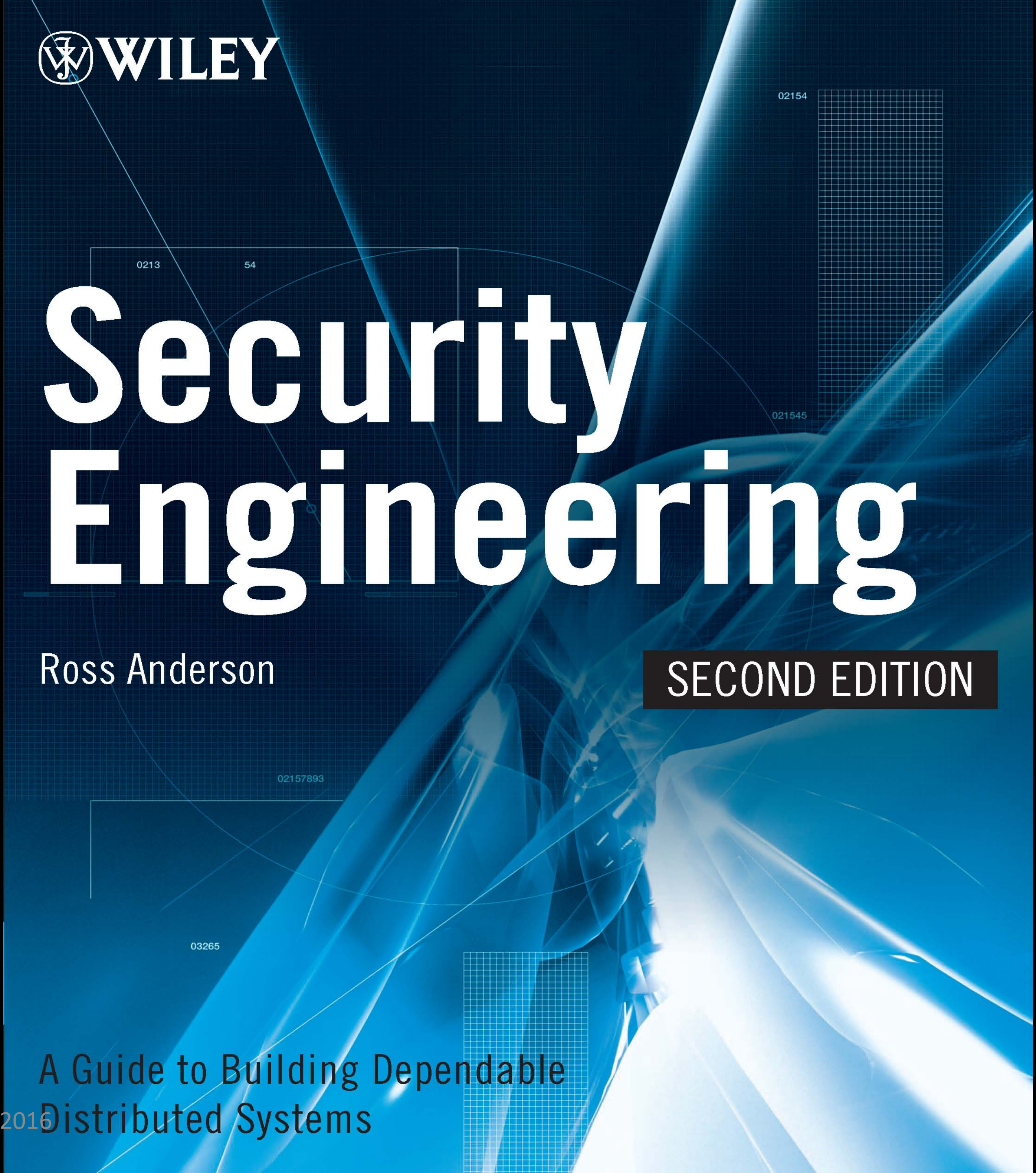
- Serve customers in villages with no network
- Serve customers when the network is congested or down
- Cut network costs for repeated transactions between the same customer and merchant
- Works for customers who don’t have smartphones (as well as those who do!)
- And perhaps in many other applications…

Next steps

- We have built a prototype offline payment system using an overlay SIM toolkit
- We'll do initial usability study here next week
- Next: incorporate lessons learned in larger-scale field trial
- Goal: free open-source software for all to use!
- What other applications might benefit from offline value transfer?

More

- More on DigiTally at the project web page http://www.cl.cam.ac.uk/~kabhb2/DigiTally/
- More on the security group at http://www.cl.cam.ac.uk/research/security/
- More on bank fraud in our blog http://www.lightbluetouchpaper.org
- And get the book on security engineering from http://www.cl.cam.ac.uk/~rja14/book



WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems

Nairobi, August 29 2016