# Is it practical to build a truly distributed payment system?

Ross Anderson, Khaled Baqer

Cambridge

CCS, Vienna, Oct 26 2016

# Centralised or distributed payment?

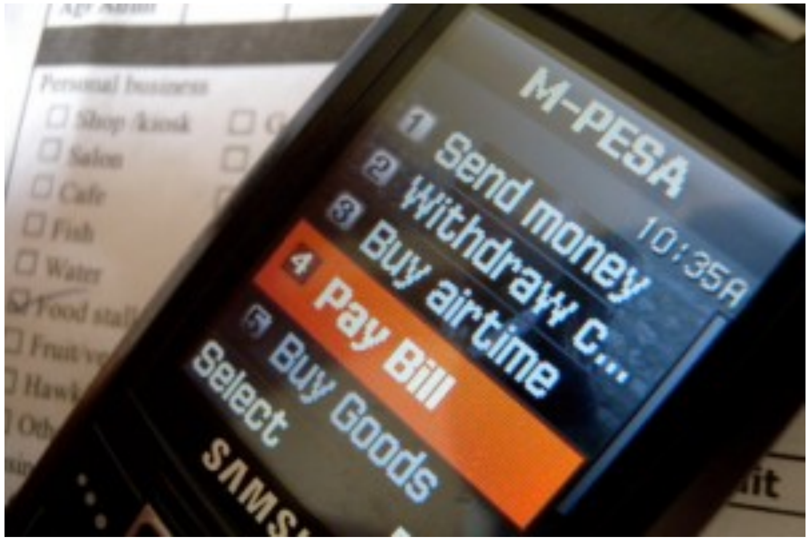
# Centralisation and tech

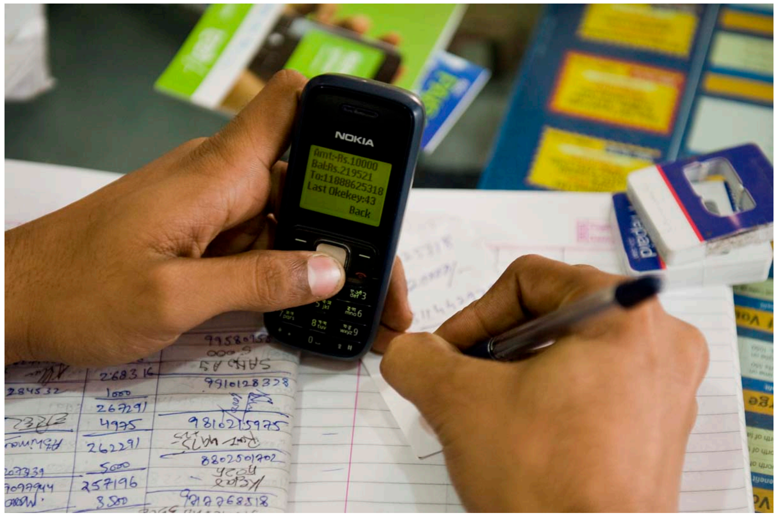
- The pendulum has swung back and forth but for most of my working life we’ve been centralising payments and putting them online
- E.g. UK ATMs moved online-only in 1993
- EMV uses shared-key crypto card <-> bank
- However some applications have always resisted the move online
- Many others use offline as a fallback
- And bitcoin: is it really distributed?

# Prepayment meters

- The STS specification we did 20+ years ago (IEEE S&P 95) is now used in 100+ countries
- Idea: copy 20-digit ciphertext from a ticket

# 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?

- 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?

# 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: top issues were network access, then costs (though this varies between countries)
- 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 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

# Background: Short Message Authentication

- Short message authentication codes: telex test keys, firing codes, CVV auth codes
- Goal: operate in offline or constrained environments
- Tradeoffs between security and usability
- We set out to design for usability
- Our starting point was minimum change to the familiar transaction flow

# Background: M-Pesa transaction

- Alice wants to pay Bob Ksh 400 ($4)
- Bob gives her his phone number
- Alice enters it, and '$4'
- She's asked for her PIN
- An encrypted SMS is sent to the phone company
- After a random delay (+- 1 minute) Bob gets a confirmation SMS

# 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

- If Bob wants $4 from Alice, he selects her name and enters the amount, “$4”, on his phone
- It shows an 8-digit authorization request, say ‘4761 0825’ which he shows or reads or shows 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 or shows to Bob
- He taps in the code
- If it’s correct, his phone displays “$4 received” at once, with a full log of the transaction

# Under the hood – first protocol

- Alice agrees to pay Bob X and each of them enters both this amount and the other party's phone number into their phones
- Bob chooses a 3-digit nonce $N_B$ and forms a 3-digit MAC C (using the shared secret key K) of B and X. He tells Alice the values

$(N_B, C)$ where $C = Mac_K(B,A,X,N_B) \bmod 10^3$

# First protocol (continued)

- Alice verifies the MAC, then authorises the transaction (using her PIN) to create a nonce and the response to the challenge ($N_A$,R) where R = $Mac_K (A,N_A,C,N_B,B) \bmod 10^4$
- Bob enters $N_A$ and R into his purse, and checks it increments by X
- This verified in a straightforward way using the BAN logic (see Protocols Workshop paper)

# First protocol – bugs

- Bob now chooses a higher price X′
- Bob generates new nonces, to find a collision:

  $Mac_K(A,X, N_B,B) \equiv Mac_K(A,X', N_B',B) \equiv C \bmod 10^3$
- Bob aborts all other trial transactions
- Bob then gives ($N_B$,C) to Alice, but on his SIM uses $N_B$′ and X′.
- Thus, Alice pays X; Bob gets X ′ > X
- Fix: $R = Mac_K(A,N_A,X,N_B,B)$

# Further design constraints

- Bob could try to add money to his SIM card by faking transactions with fake customers and just guessing the response R
- Bob can also try to fake transactions with real customers A, by keeping a record of their $Mac_K$ $(A, N_A, X, N_B, B)$ replies:
  - Bob can choose A and $N_A$
  - if the real Alice has already paid n times, then Bob finds some $(N_B, R)$ fake a transaction with prob $n \cdot 10^{-3}$
- Issue: most formal tools don't track entropy!

# Evolution 2: Delay-Tolerant Needham–Schroeder

- Banks happy with universal shared secrets only for small transactions. So what about big ones?
- Answer: turn the bug in the Needham-Schroeder (NS) protocol into a feature!
- A and B can ask for Sam's help to establish KAB
- Either of them starts NS protocol with Sam when connectivity is available, and gets encrypted KAB
- Challenge: exchanging digits for the encrypted key, as 20 digits give you only 66 bits
- General mechanism for delay-tolerant networks?

# Field trial

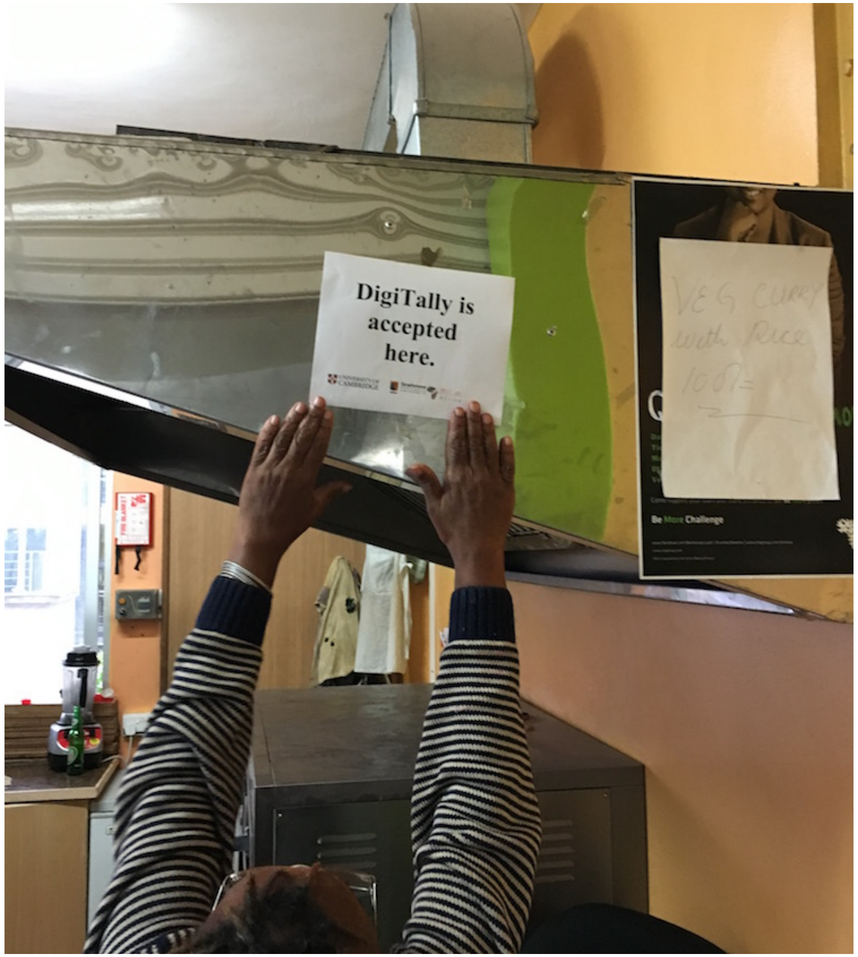
- Initial usability study with Joe Sevilla and Lorna Mutegi, Strathmore University, Nairobi
- Three outlets:
  - Bookshop (one till, quiet)
  - Coffee shop (two tills, bursty traffic)
  - Cafeteria (five tills, madly busy at mealtimes)
- We anticipated problems at the cafeteria!
- Twelve students (split male/female, arts/science, urban/rural)

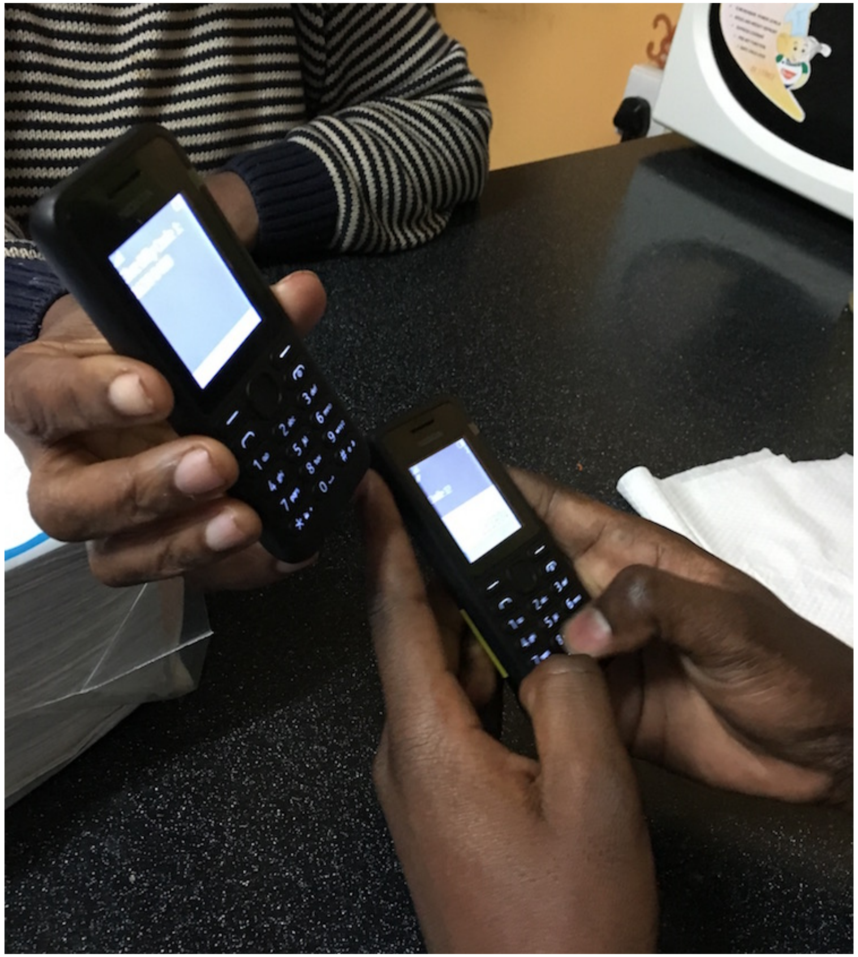
# The students

# The bookshop


# The coffee shop

# The coffee shop



# The cafeteria


# What we found

- It worked fine in the bookshop, as expected
- The coffee shop staff didn’t like it as they were making coffee and also taking money
- The cafeteria staff, to our surprise, strongly preferred it to M-Pesa!

# What we found

- It worked fine in the bookshop, as expected
- The coffee shop staff didn't like it as they were making coffee and also taking money
- The cafeteria staff, to our surprise, strongly preferred it to M-Pesa!
- They did not have to wait about a minute for the confirmation SMS to come through
- Full usability study paper in preparation…

# Pre-market research

- We talked to
  - the incumbent
  - the other phone company
  - the President’s office
  - and one bank that has been trying to establish its own mobile money system using overlay SIMs
- We then did market research in one of the richest towns (Thika) and one of the poorest (Busia)

# Busia, near Lake Victoria

# Busia county office


# What we found

- The rich county thought it an interesting tech, but of most use for controlling money
- The poor county thought it was awesome and could transform their lives
- The phone network is awful there, so phone payments are really hard
- However the incumbent phone company wants to maximise profits from its SIM space
- That means gambling apps, not offline payments

# The project so far

- The Gates Foundation paid us to develop a tech to extend mobile payments offline
- We've done that, and it works – both in the lab and the field
- Deployment in Kenya looks hard for now
- We've been talking to phone and payment companies elsewhere, and to bodies like the World Food Programme

# Why tools like this matter

- Perhaps something other than payment will be the killer app
- Pay-as-you-go solar energy is growing fast
- Delay-tolerant networks will be pervasive!
- Also, we're now getting tamper-resistant devices and enclaves everywhere
- Lightweight shared-key crypto can be used for optimistic bootstrapping, rate control / DoS prevention

# Lessons learned

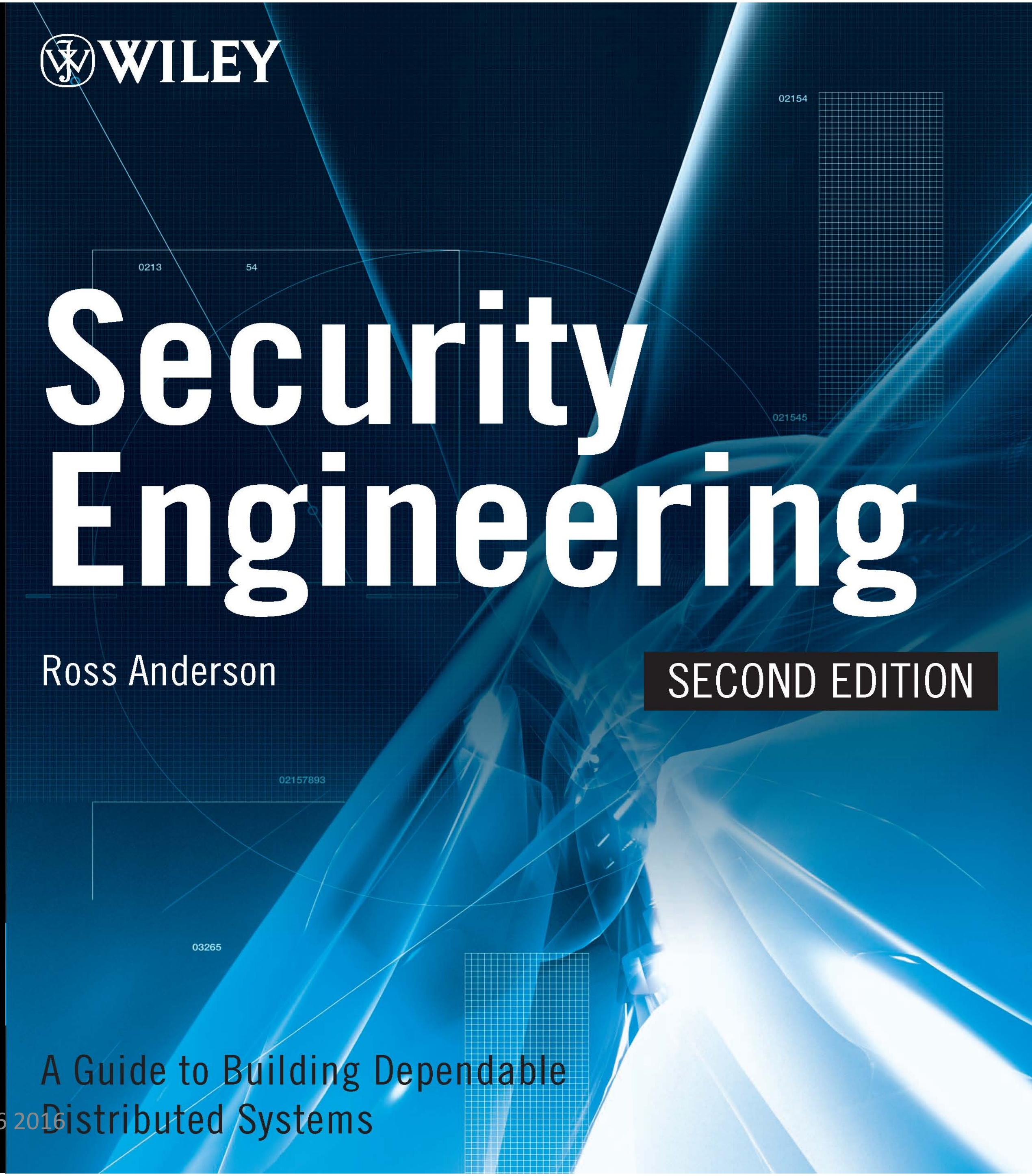
- Build it and try it out!
- (My thesis adviser Roger Needham used to say ‘good research comes from real problems’)
- Start with the people, not the tech
- Look at needs, design for usability
- Ceremonies – protocols with human participants – are worth systematic study
- Short message authentication protocols are a surprisingly common example
- Ask: can I do more with less?

# Deeper lessons learned

- Economic incentives determine not just security, but deployability too
- Institutions matter, and regulation
- Often disruptive technology is about defeating regulation so as to replace tired institutions
- Ask: “what’s the source of market power?”
- Here, it’s not just network effects; a short resource the ability to turn cash into electrons
- The incumbent saw off a bitcoin challenger!
- Finally – think through the ethics

# 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 my 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