DigiTally: Piloting Offline Payments for Phones

Khaled Baqer
Cambridge

Collaborators: Ross Anderson, Jeunese Adrienne Payne, Lorna Mutegi, and Joseph Sevilla

SOUPS, Santa Clara, 13 July 2017
The mobile money revolution
Mobile money achievements

• 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
• 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: issues were network access and 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 (feature phones)?
Busia (near Lake Victoria)
Busia county offices (near Lake Victoria)
DigiTally overview

• DigiTally is a prototype system we’ve built to do research on offline mobile payments
• Address financial inclusion challenges in developing countries
• It works by copying short authentication codes from one phone to another
• It can also be implemented in 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 design

• Work in existing environments
• Do not require/introduce unfamiliar hardware
• Minimize assumption about constrained devices
• Focus on feature phones
• Mimic existing mobile payment systems
• Work seamlessly alongside any existing SIM card
DigiTally payment (I)

• Bob enters the amount, “Ksh 450” on his phone
• It shows an 8-digit authorization request, say “8972 0307” which he reads to Alice
• She taps “Ksh 450” and “8972 0307” 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 (II)

- Alice’s phone displays an 8-digit authorization response, say “7021 0003”, which she reads to Bob
- He taps in the code
- If it’s correct, his phone displays “Ksh 450 received” with a log of the transaction (Alice gets a similar log)
Preliminary study (I)

• Collaborate with Strathmore University (Nairobi, Kenya)
• 19 participants at Strathmore University
• Duration: 5 days
• Loaded balance for student phones with Ksh 2000 (about $19.50)
• Three outlets: Coffee shop (one till, quiet), Bookshop (two tills, bursty traffic), Cafeteria (five tills, madly busy at mealtimes)
The coffee shop
Preliminary study (II)

• Data collected:
  • Error rates (code-entry errors, and wrong PIN input)
  • Number of transactions
  • Number of attempts to unlock the SIM
  • Total amounts for all transactions (spent and received)
  • Transaction duration times
# Results (students)

<table>
<thead>
<tr>
<th>$Code_1$ errors</th>
<th>$Code_2$ errors</th>
<th>Total code errors</th>
<th>Average time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8 (26.7%)</td>
<td>8 (26.7%)</td>
<td>30.9</td>
</tr>
<tr>
<td>9 (32.1%)</td>
<td>0</td>
<td>9 (32.1%)</td>
<td>24.4</td>
</tr>
<tr>
<td>2 (11.1%)</td>
<td>8 (44.4%)</td>
<td>10 (55.6%)</td>
<td>28.1</td>
</tr>
<tr>
<td>9 (40.9%)</td>
<td>1 (4.6%)</td>
<td>10 (45.5%)</td>
<td>44.9</td>
</tr>
<tr>
<td>1 (3.5%)</td>
<td>0</td>
<td>1 (3.5%)</td>
<td>24.2</td>
</tr>
<tr>
<td>0</td>
<td>1 (3.9%)</td>
<td>1 (3.9%)</td>
<td>54.3</td>
</tr>
<tr>
<td>1 (3.9%)</td>
<td>0</td>
<td>1 (3.9%)</td>
<td>50.9</td>
</tr>
<tr>
<td>5 (17.9%)</td>
<td>0</td>
<td>5 (17.9%)</td>
<td>32.4</td>
</tr>
<tr>
<td>0</td>
<td>4 (40.0%)</td>
<td>4 (40.0%)</td>
<td>28.8</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>37.1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>42.1</td>
</tr>
<tr>
<td>5 (22.7%)</td>
<td>0</td>
<td>5 (22.7%)</td>
<td>38.9</td>
</tr>
</tbody>
</table>

SOUPS, Santa Clara, 13 July 2017
## Results (merchants)

<table>
<thead>
<tr>
<th>$Code_1$ errors</th>
<th>$Code_2$ errors</th>
<th>Total code errors</th>
<th>Average time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4 (6.8%)</td>
<td>4 (6.8%)</td>
<td>40</td>
</tr>
<tr>
<td>0</td>
<td>6 (9.8%)</td>
<td>6 (9.8%)</td>
<td>43.9</td>
</tr>
<tr>
<td>0</td>
<td>4 (6.8%)</td>
<td>4 (6.8%)</td>
<td>69.8</td>
</tr>
</tbody>
</table>

SOUPS, Santa Clara, 13 July 2017
Results (System Usability Scale)

• All participants: the average SUS score for DigiTally was 78.8 (‘Good’; ‘B+’ grade)
• Eight participants gave the equivalent of an ‘A+’ grade
• Merchant participants: the average SUS score was 71.4 (‘Good’; ‘C+’ grade)
• Student participants: the average SUS score was 83.1 (‘Excellent’; ‘A’ grade)
Final remarks

• Our goal was to investigate usability problems for offline payments, and user requirements for development projects

• DigiTally participants' experience was generally positive (perceived security, speed, deterministic, no network req.)

• Research direction: rethink (reintroduce) resilience in critical systems, learn from delay-tolerant networks (DTNs), etc.

• Focus on the ‘bottom billion’ and the effects of unreliable networks and constrained tech on security and usability
Q & A

Khaled Baqer

firstname.lastname@cl.cam.ac.uk

https://www.cl.cam.ac.uk/~kabhb2/