LET’S TALK MONEY

Fahad Pervaiz

Sam Castle, Galen Weld, Franziska Roesner, Richard Anderson
Unbanked Population

Percentage of total adult population who do not use formal or semiformal financial services

- High-income OECD countries: 8% (60 million adults)
- Latin America: 65% (250 million adults)
- Middle East: 67% (136 million adults)
- Sub-Saharan Africa: 80% (326 million adults)
- Central Asia & Eastern Europe: 49% (193 million adults)
- East Asia, Southeast Asia: 59% (876 million adults)
- South Asia: 58% (612 million adults)

Total: 53% (2,455 million adults)
Branchless Banking

Bank/Financial Institute
Bank of America, Standard Chartered Bank

Telecommunication Company
Verizon, Safaricom

3rd Party Software Company
Paypal, Google Wallet
Agent Based Banking
Communication Channels

- USSD
- SMS
- Internet

Dial *322#

1. Cash-In
2. Cash-Out
3. Registration
4. Payment
5. My Acc
0. Logout
Select your option

Choose option

Enter Mobile Account No
01XXXXXXXX
(Reply with Agent Account No)

Enter Amount
*****
(Reply with Amount)

Your account has been successfully credited by Tk. XXX, Bal: Tk. XXXX. TxnID: XXX
Physical Security to Digital Security
Prior Work

Vulnerabilities in seven branchless banking applications

- Improper certificate verification
- Non-standard and weak cryptography
- Information leakage
- Data Exposure
- Weak password recovery

Building Threat Model

Confidentiality
- External Apps
- External Libraries
- SMS Intercept

Integrity
- Server Attack
- Man-in-the-Middle
- Authentication Attack
- SMS Spoof
- Agent-driven Fraud
- Fake Accounts

Availability
- Data Loss
- Denial-of-Service (DoS)
- Theft of Services
- Device Theft
Methodology

• **General Analysis**
  • Decompiled android apps
  • Ran automated scripts to find indicators

• **In-Depth Analysis**
  • Examine service’s website
  • Search for promotional flyers

• **Developer Interviews**
  • No of Developers: 7
  • Average Interview duration: 45 min
  • Questions: Experience, Org Structure, Training and Security Processes
General App Analysis

- Approx 400 active services; majority are from GSMA mobile money development tracker database lists

- Selected Services: 197 Android apps

- Indicators: version, permission, external libraries, URLs
Stealing Data from Android Debug Log

- Another app can get permission to access logs
- Issue fixed in Android v4.1
Over-Privilege Applications

- Over-privilege apps leaves room for vulnerability
External Tracking Libraries

- Malicious or buggy 3rd party libraries can introduce new data leaks and vulnerabilities
Insecure Connections

- Insecure connections are vulnerable to man-in-the-middle attacks
In-Depth App Analysis

- Selected set have 71 services that includes Android app as well as USSD supported apps
In-Depth App Analysis

36 apps can return account info, balance and transactions via SMS
20 services can be accessed without user's SIM card
12 services do not require user to present a government issued ID
Fake Accounts

Fake Account Attack
Authentication Attack

<table>
<thead>
<tr>
<th>Number of Services</th>
<th>ID Required</th>
<th>SIM Linked to Account</th>
<th>SMS Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>30</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>No</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Yes</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
In-Depth App Analysis

Password Reset

- 16 Apps reset the password via security questions based on personal information that is common knowledge in rural area
- 4 Apps reset the password to ‘1234’
Developer Interviews

• To better understand the sources of vulnerabilities, we interviewed developers from developing world.
• Contacted 249 unique email address
• Location: Nigeria, Kenya, Uganda, Zimbabwe, Colombia
• Organizations: Bank (3), Telco (2), Software (2)
• Majority of organizations were large
• One small company with only 50 K – 100 K downloads
Developer Interviews

- Most developer had college degrees and more than 5 year industry experience
- Except for one, all companies provided technical training to their developers
- All organizations had a separate security review team and code review processes
- External libraries use was allowed but either developers were skeptical or there is organizational review needed
- All developers except for one listed stack overflow among top two resources to use for help
Developer Interviews

Incomplete Threat Model

- Protecting organization from theft is considered more important than protecting customers

“There are two security risks and both are human. One is an ex-employee, and second is the customer....I take part in API discussions and system architecture for a new system...With my experience and training, I would say if I left the company today, there are 900 security breaches, and I would be able to breach one of them.”
Developer Interviews

Partner Requirements and Regulations

• Certain insecurities are dictated by the partner specifications and/or government regulations

“We did one crazy one [implementation] in West Africa where they didn't use any [encryption]. There again we are just at the mercy of the partner...We made them sign documents seven ways to Sunday because we were absolutely worried about [security]. What you’ll find in these markets is that you have an IT person, and you are forced to work to their level of expertise.”
Conclusion

• Designed a Threat Model
• General Analysis
  • Mandating updated Android versions
  • Whitelist of secure 3rd party libraries
  • Advocate end-to-end secured communication
• In-Depth Analysis
  • Use of Govt. ID to avoid fake accounts
  • Better requirements are needed for password reset
  • Privacy issues with SMS communication
• Developer Interviews
  • Vulnerabilities due to specifications managed by different stakeholders
  • Complete threat model is needed to eliminate lack of understanding
  • Providing resources for best security practices to replace unreliable online forums
Thank You

Fahad Pervaiz
fahadp@cs.washington.edu