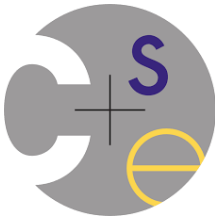
LET'S TALK MONEY

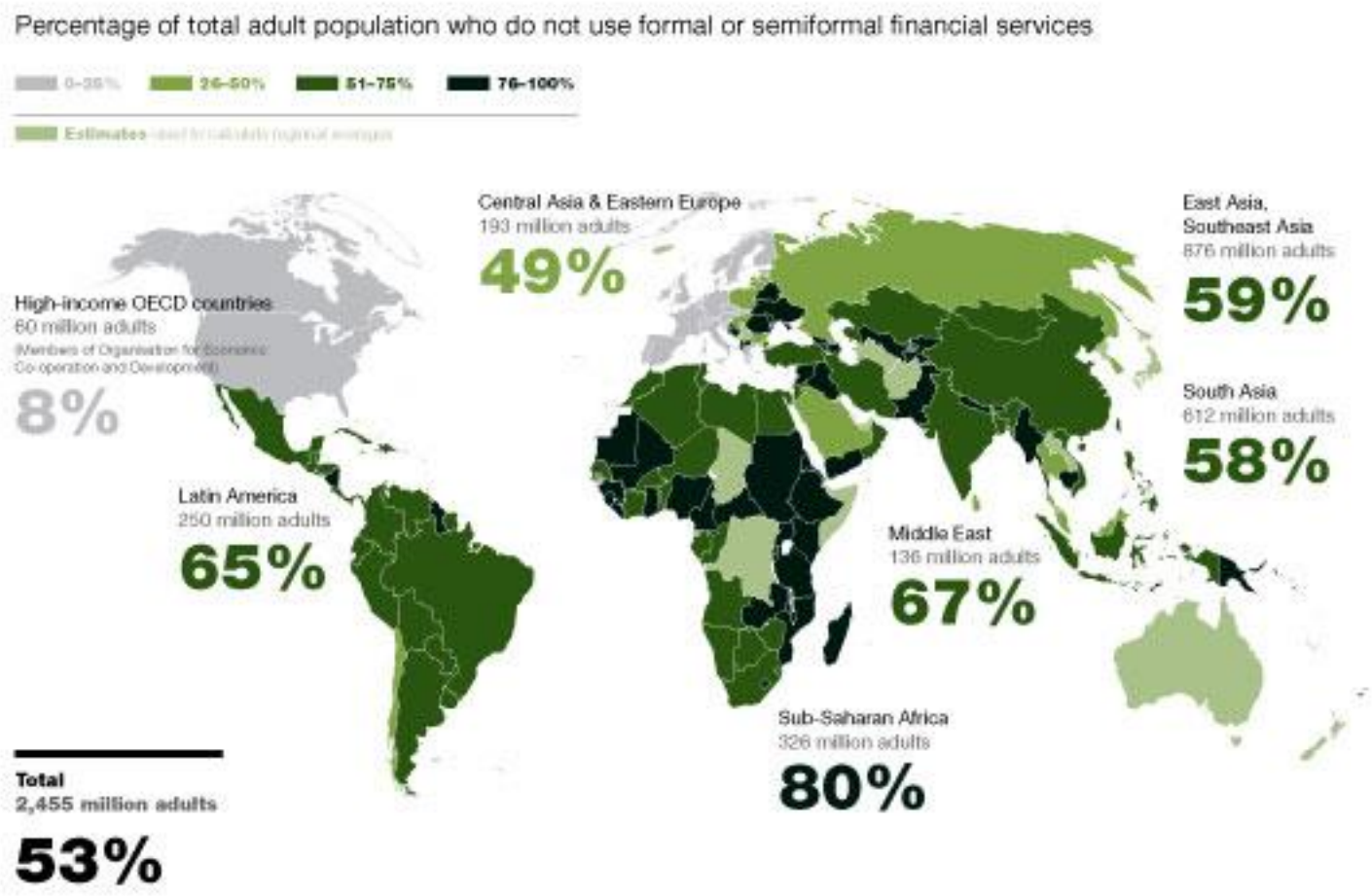
Fahad Pervaiz

Sam Castle, Galen Weld,
Franziska Roesner, Richard Anderson

UNIVERSITY of WASHINGTON



Unbanked Population



Branchless Banking

Bank/Financial Institute

Bank of America, Standard Chartered Bank

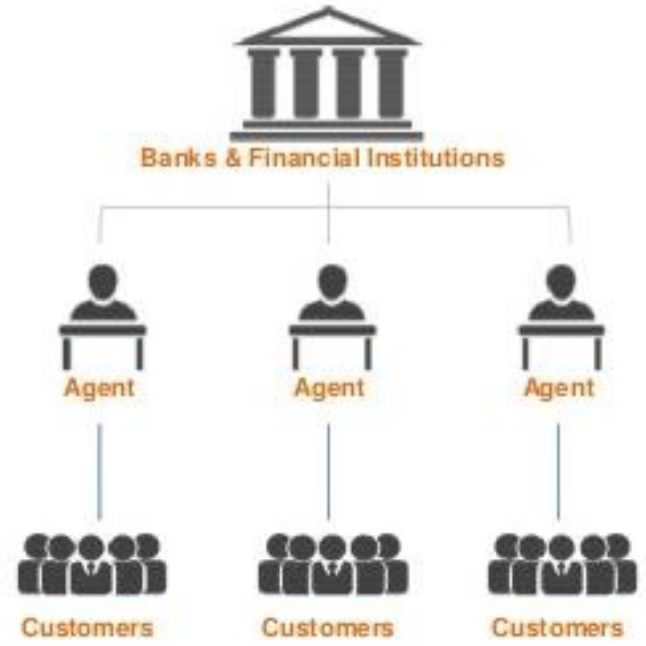
Telecommunication Company

Verizon, Safaricom

3rd Party Software Company

Paypal, Google Wallet

Agent Based Banking

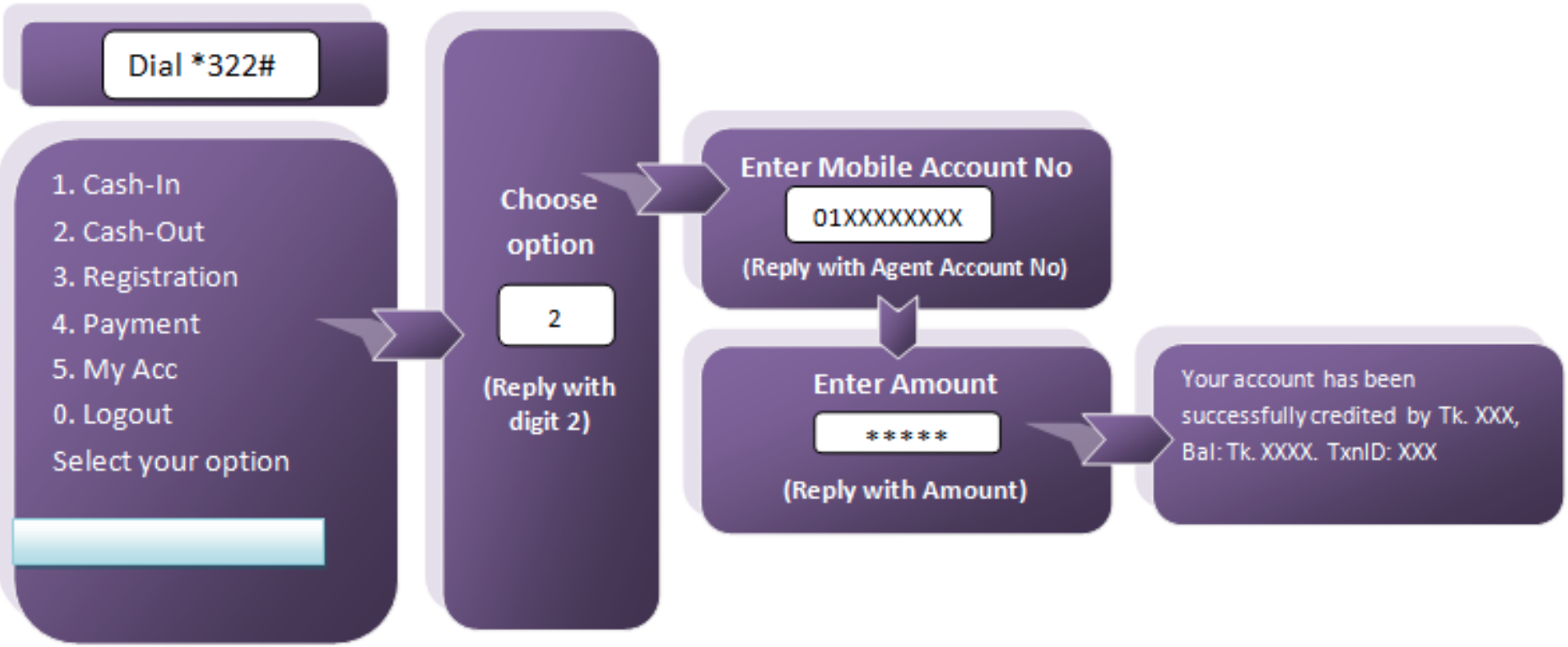


Communication Channels

Internet

SMS

USSD



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

Reaves et al. "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World." USENIX 2015.

Building Threat Model

Confidentiality	Integrity	Availability
• External Apps	• Server Attack	• Data Loss
• External Libraries	• Man-in-the-Middle	• Denial-of-Service (DoS)
• SMS Intercept	• Authentication Attack	• Theft of Services
	• SMS Spoof	• Device Theft
	• Agent-driven Fraud	
	• Fake Accounts	

Methodology

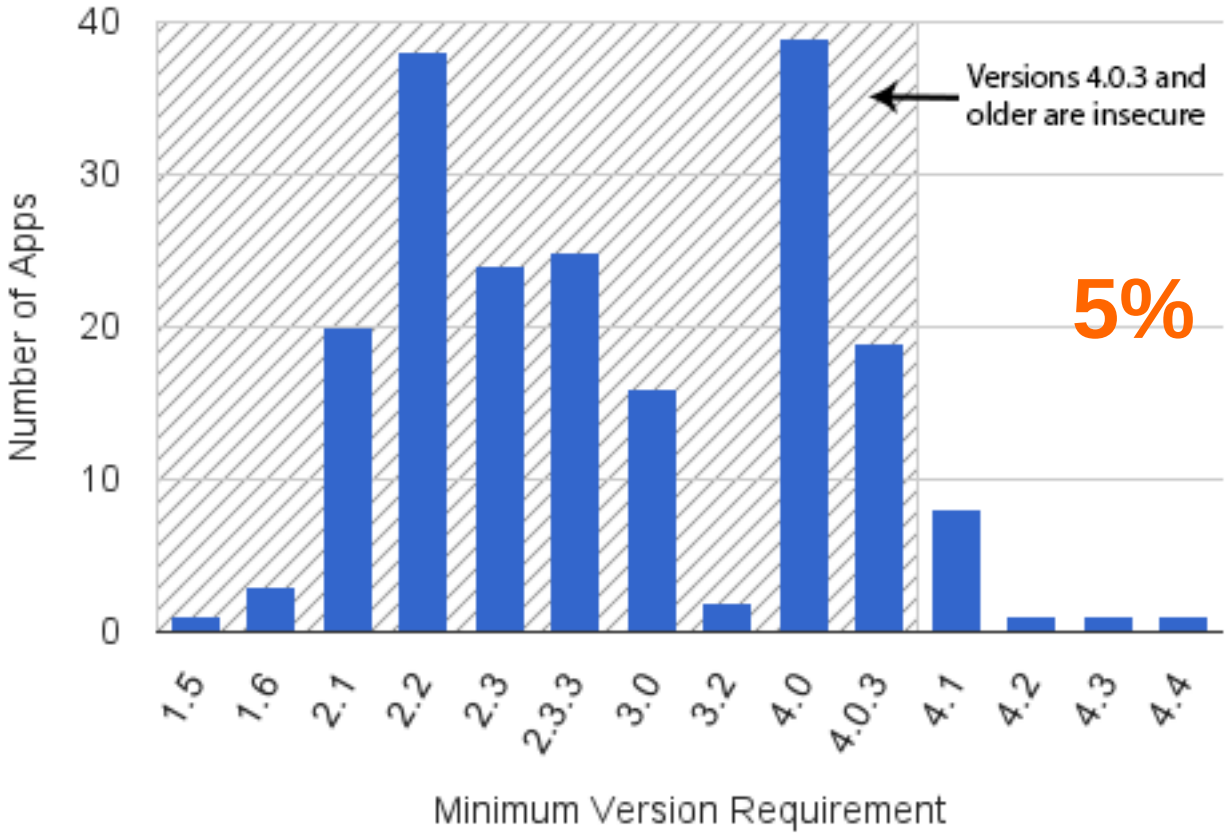
- **General Analysis**
  - Decompiled android apps
  - Ran automated scripts to find indicators
- **In-Depth Analysis**
  - Examine service's website
  - Search for promotional flyers
- **Developer Interviews**
  - No of Developers: 7
  - Average Interview duration: 45 min
  - Questions: Experience, 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

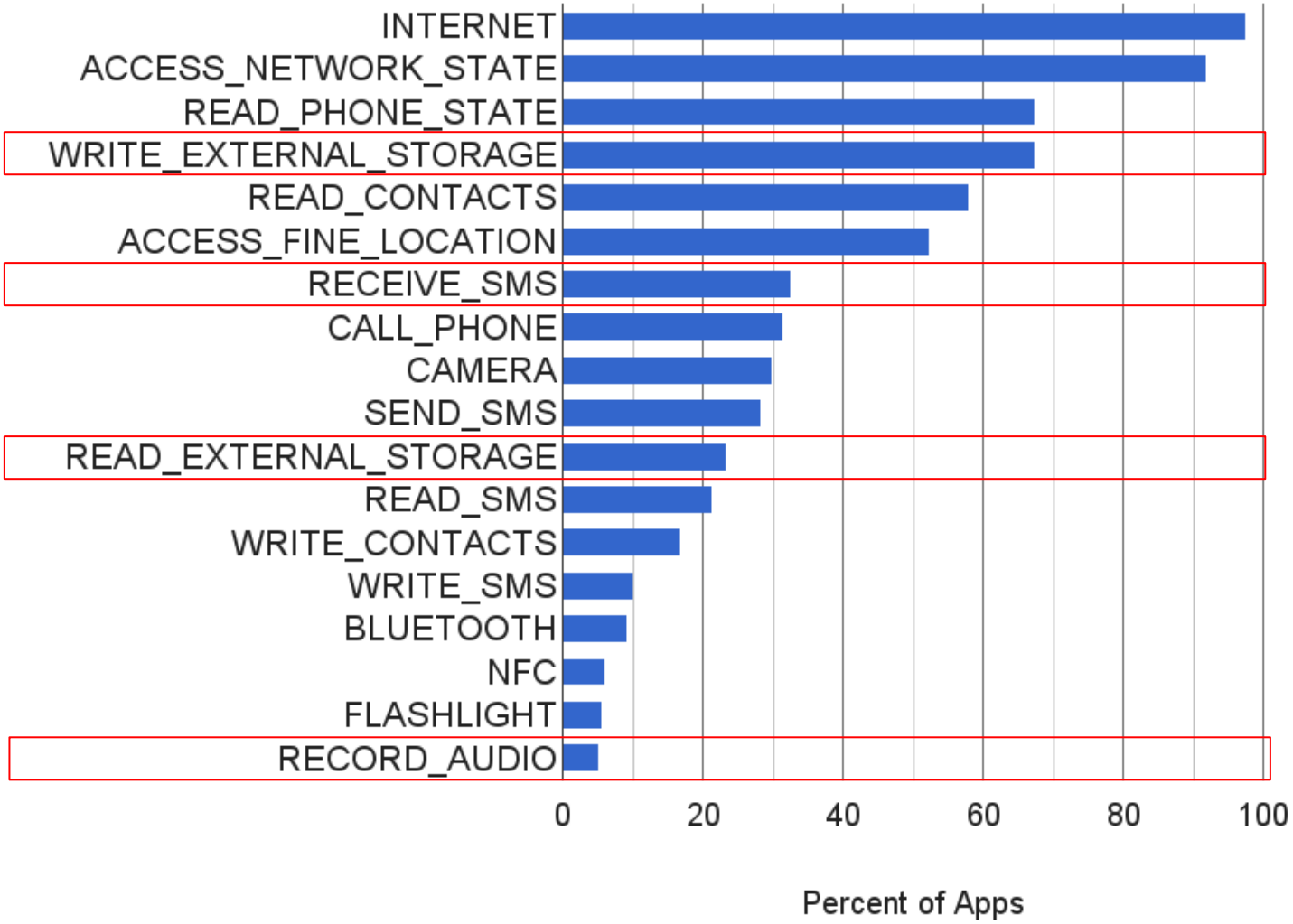
Stealing Data from Android Debug Log

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



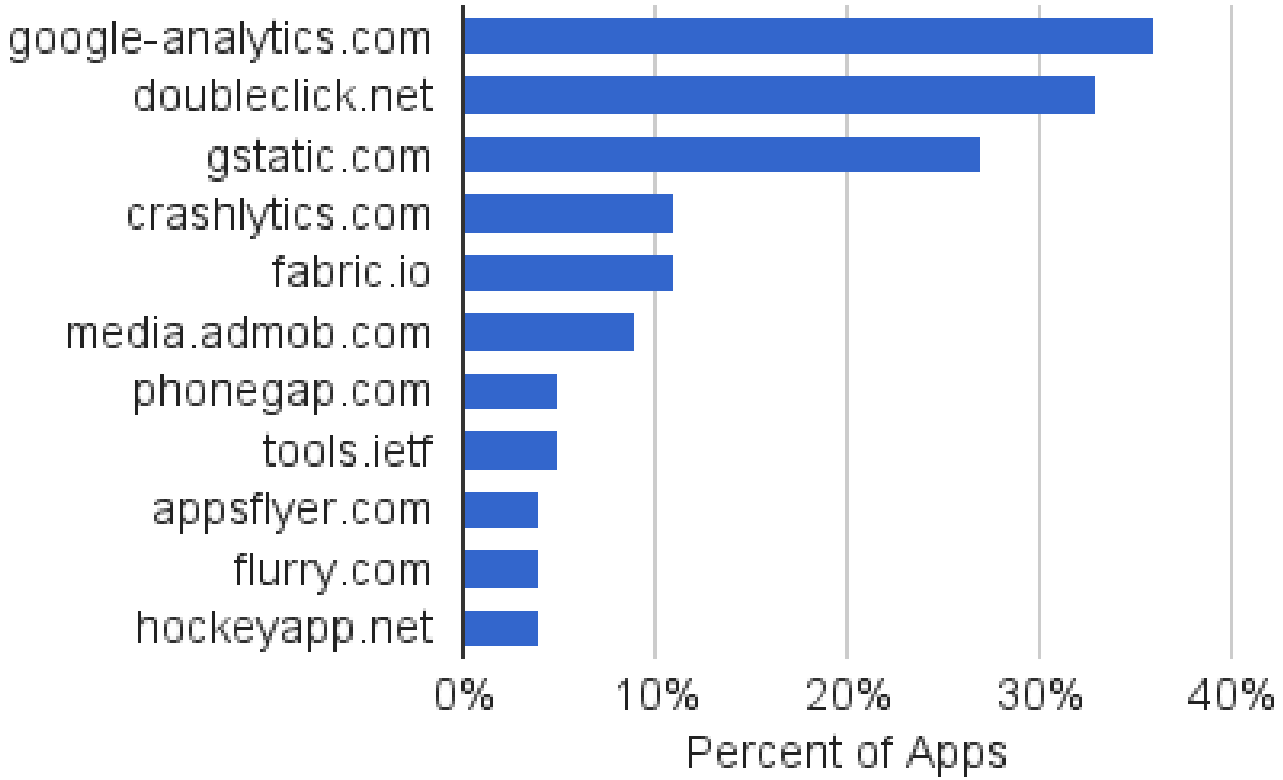
Over-Privilege Applications

- Over-privilege apps leaves room for vulnerability



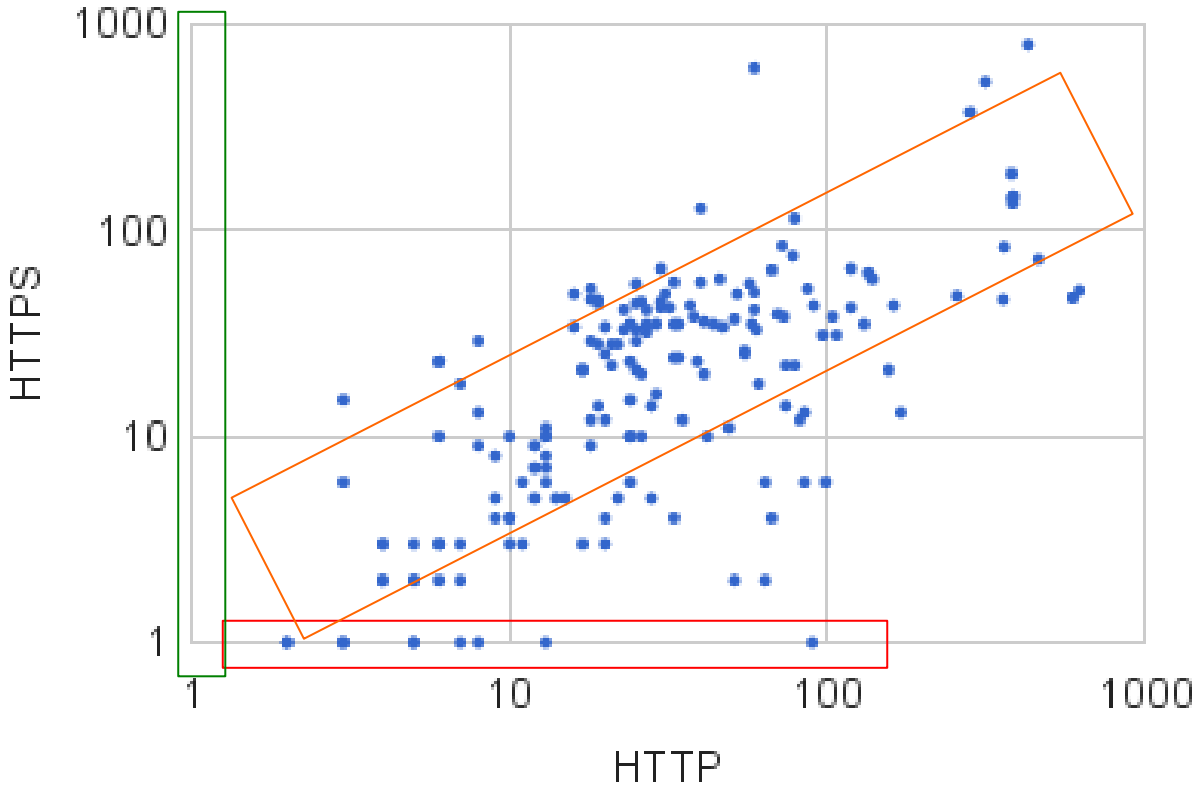
External Tracking Libraries

- 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

11

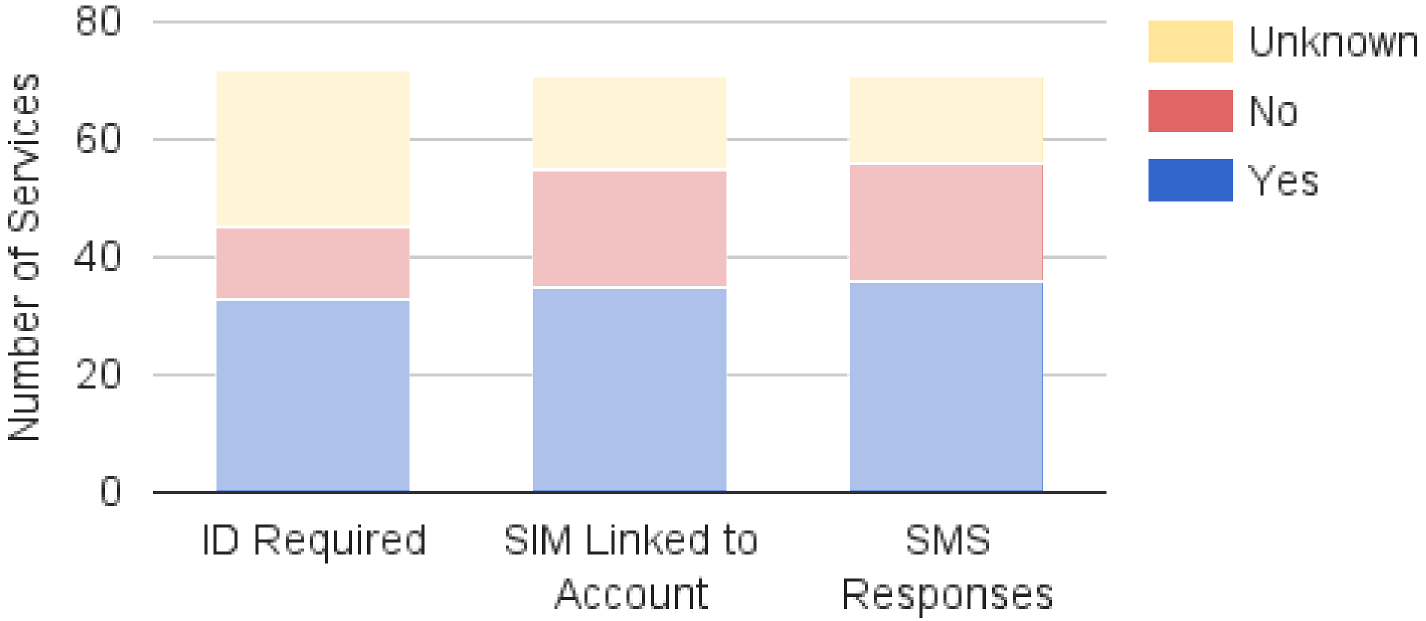
43

17

In-Depth App Analysis

[illegible]

[illegible] Authentication Attack



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