Security and Fraud in Financial Services for Emerging Digital Economies

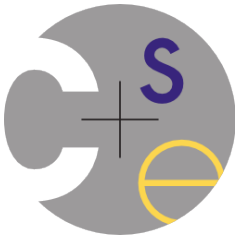
Sam Castle

University of Washington

Seattle, USA

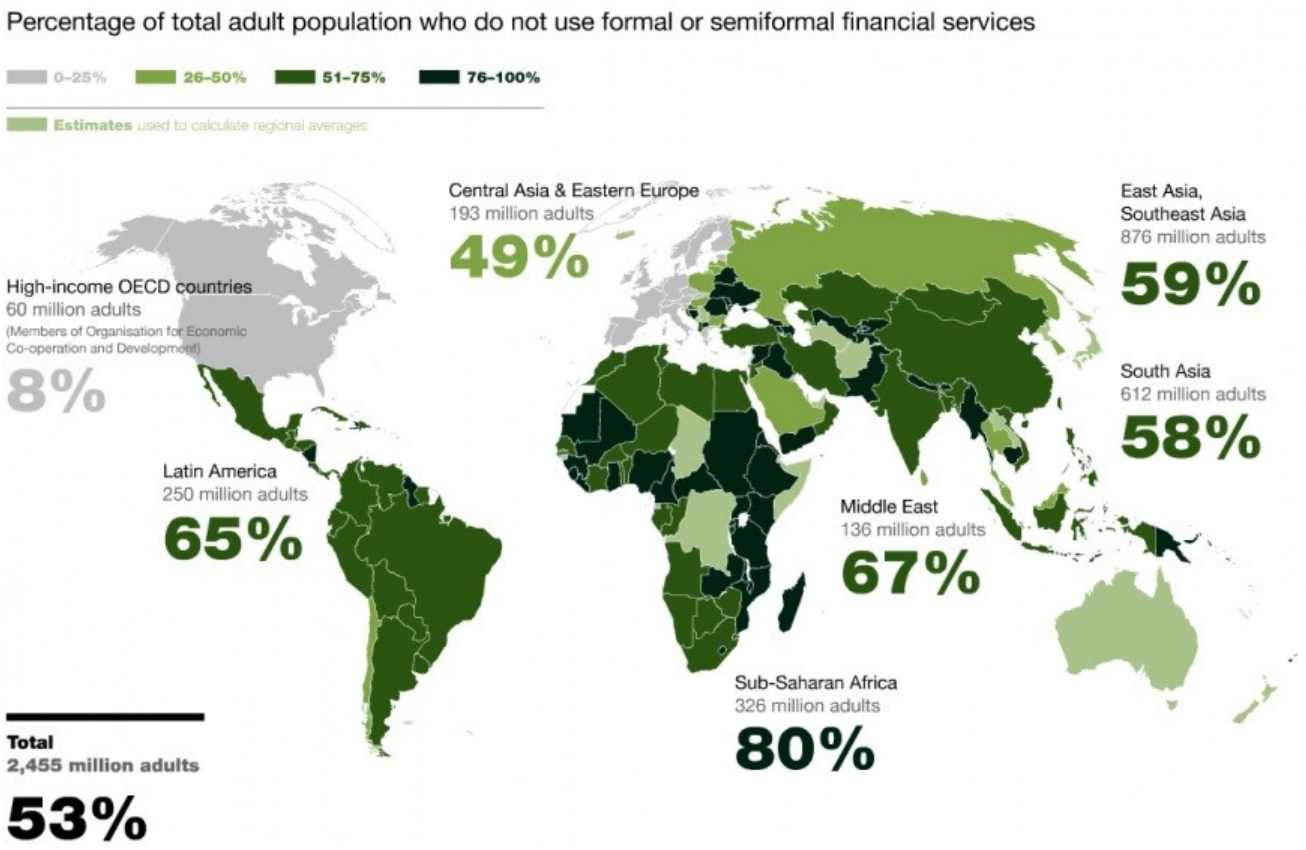
Advisors: Richard Anderson, Franzi Roesner

UNIVERSITY of WASHINGTON



DIGITAL FINANCIAL SERVICES RESEARCH GROUP

More than 2 billion people have no access to financial services.

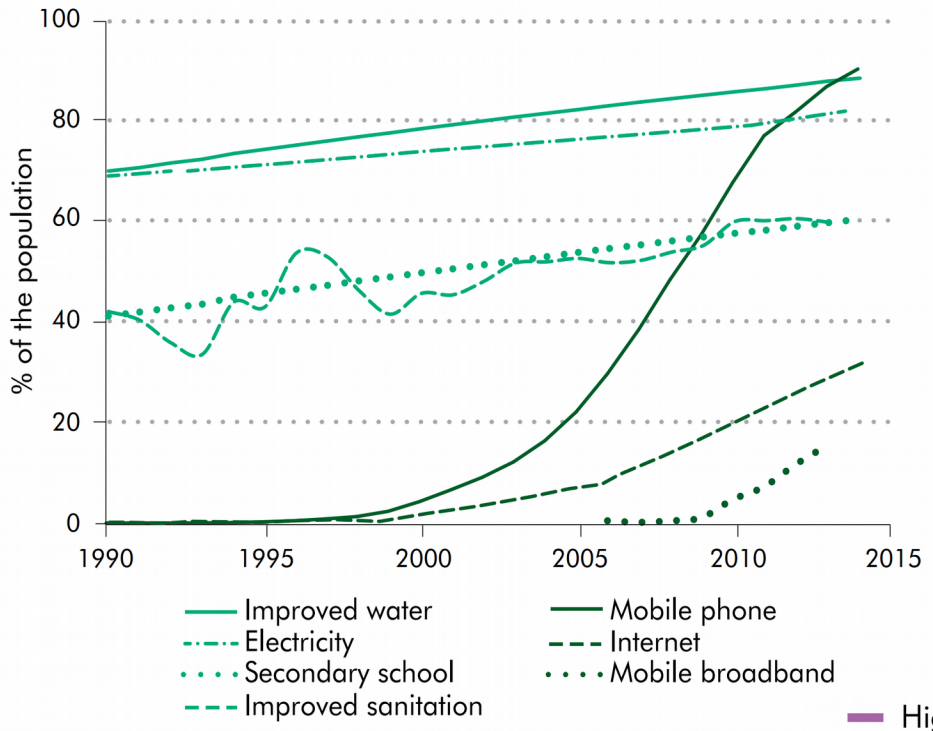


In developing countries, 8 out of 10 people now have access to a mobile phone.

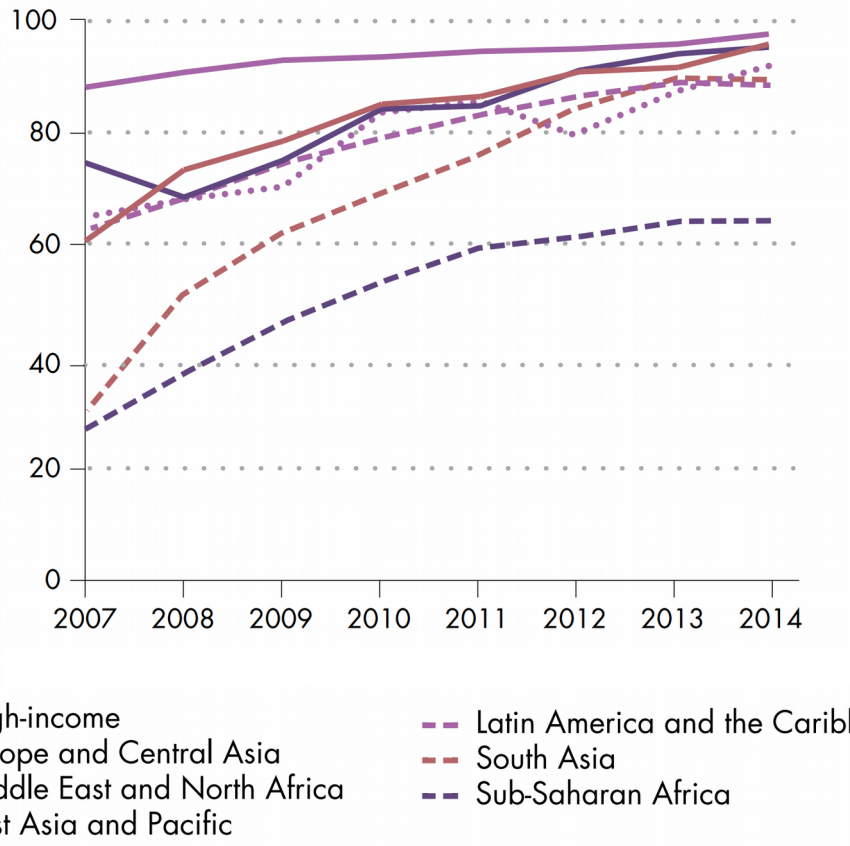
Source: McKinsey Quarterly, 2010; WDR 2016

Digital technologies are spreading rapidly in developing countries

Technology use



Individuals with mobile phone access

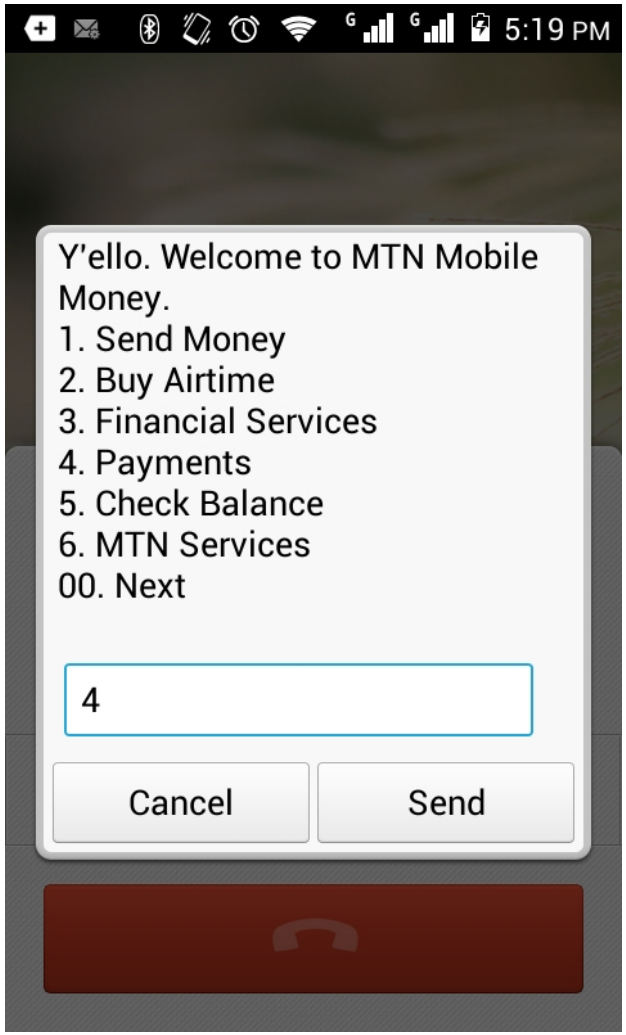


Source: 2016 World Development Report


HONDA

What are digital financial services?

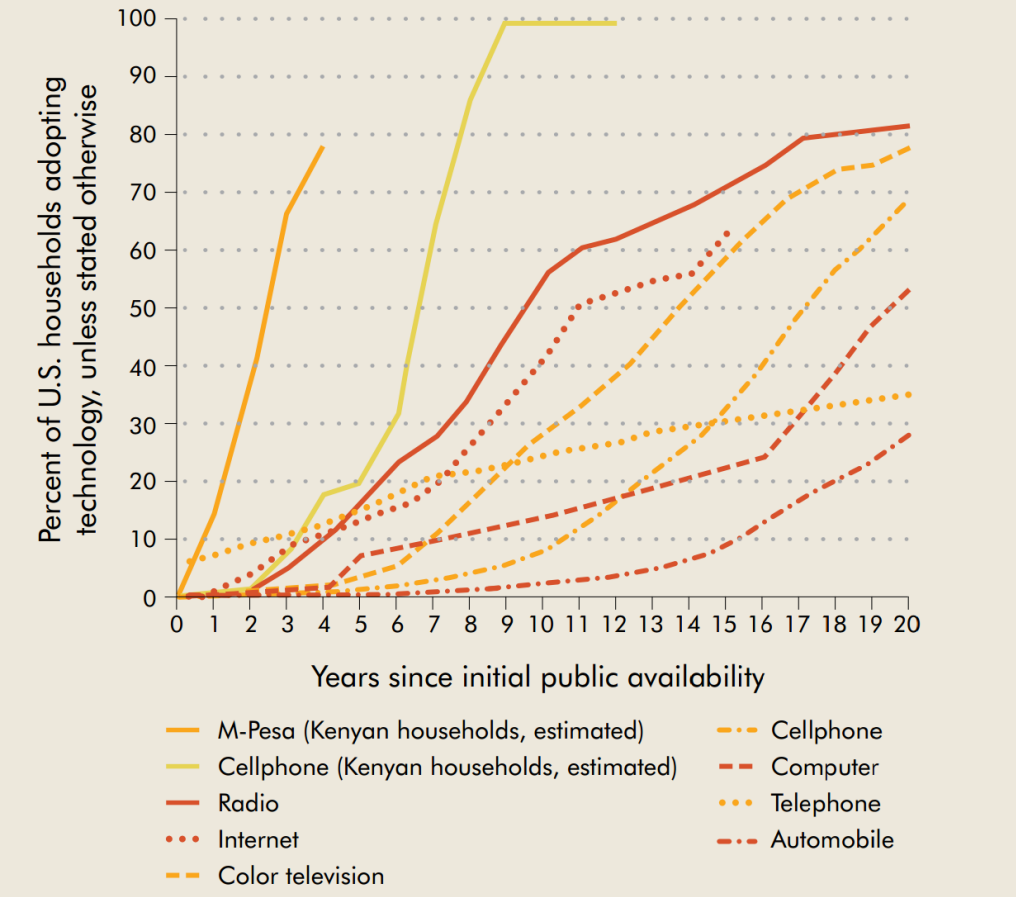
- Savings
- Peer-to-peer transactions
- Payments
- Loans
- Remittances
- G2P Salary payments
- Utilities payments

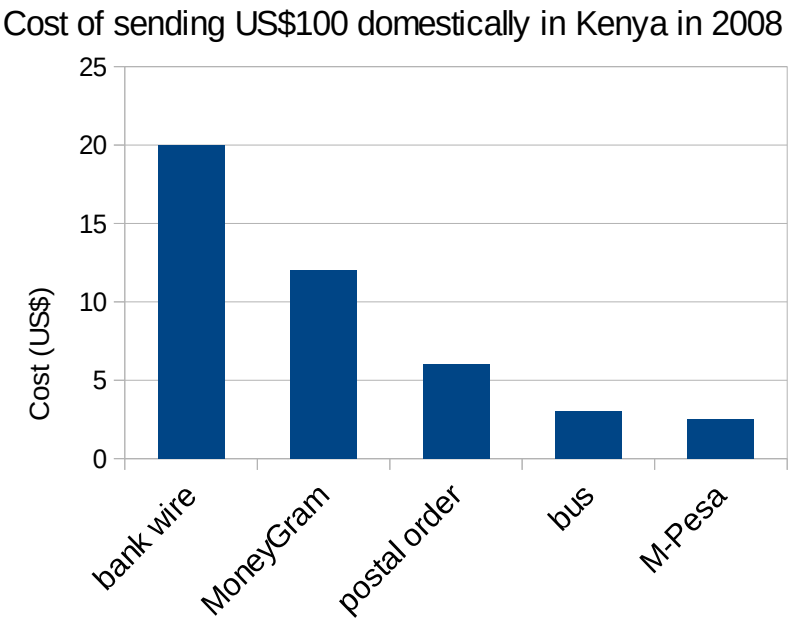


Why are they useful?

- Efficiency of payments
- Safe savings
- Small business funding
- Planning for fees and financial shocks

Kenya's M-Pesa payment system reached 80 % of households within 4 years





Source: WDR 2015

What are digital financial services?

Internet

SMS

USSD

Bank/Financial Institute

Bank of America, Standard Chartered Bank

Telecommunication Company

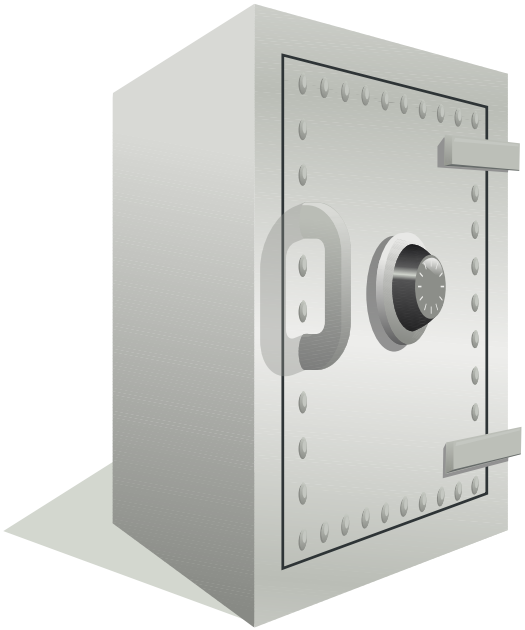
Verizon, Safaricom

3rd Party Software Company

Paypal, Google Wallet

Source: WorldRemit, Uganda

Security & Privacy in DFS



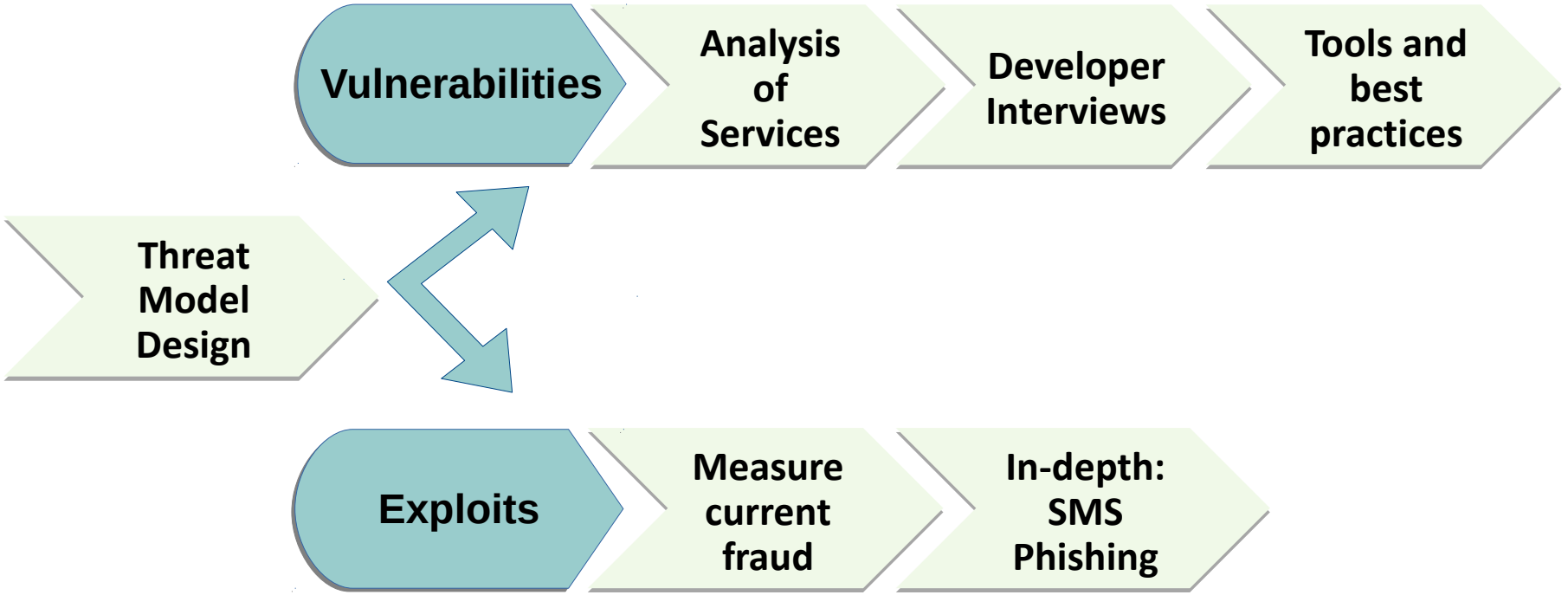
Trust

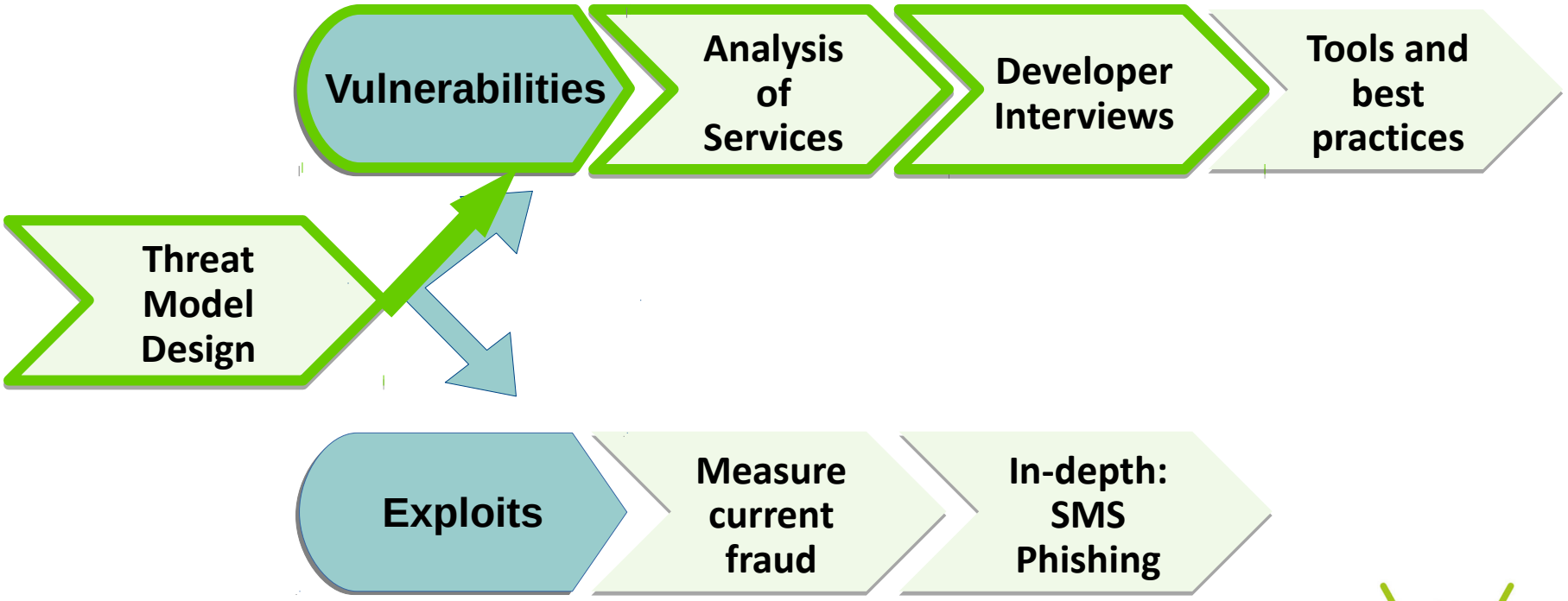
Consistency

Growth

Prior work from Reaves et al.: “The majority of these apps fail to provide the protections needed by financial services…threatening to erode trust in branchless banking and hinder efforts for global financial inclusion.”

Security Landscaping in DFS





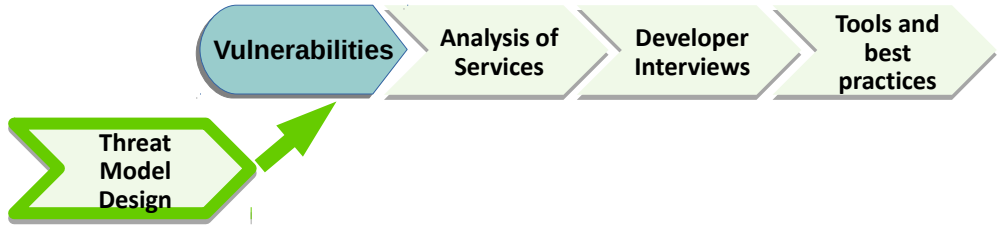
PART 1: MOBILE APP SECURITY

App Security Overview

Goal: Understand vulnerabilities in mobile money deployments

1. **Design of Threat Model Particular to Mobile Money**
2. **General Security Analysis**
   - 197 decompiled Android apps
   - Automated detection of permission requests, version requirements, external libraries, and HTTPS URL usage
3. **In-depth Analysis**
   - 71 apps, including Android and USSD-based
   - Manual assessment of relevant properties, including KYC requirements, password reset procedures, SMS usage
4. **Developer Interviews**
   - No of Developers: 7
   - Average Interview duration: 45 min
   - Questions: Experience, Org Structure, Training and Security Processes

Threat Modeling



Confidentiality
protection of customer information

External Apps
External Libraries

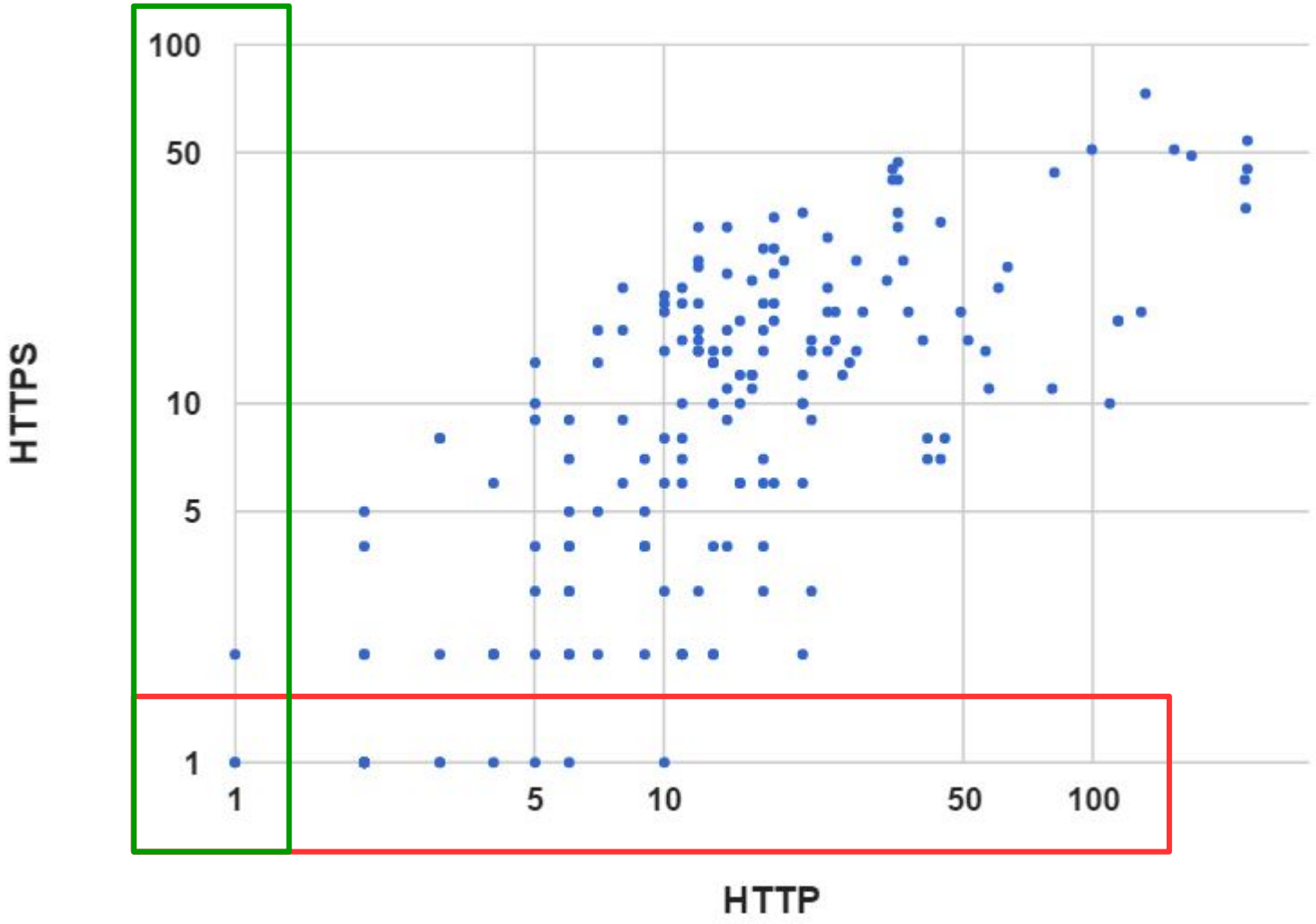
Integrity
incorruptibility of data

MITM
SMS Spoofing
Agent-driven Fraud

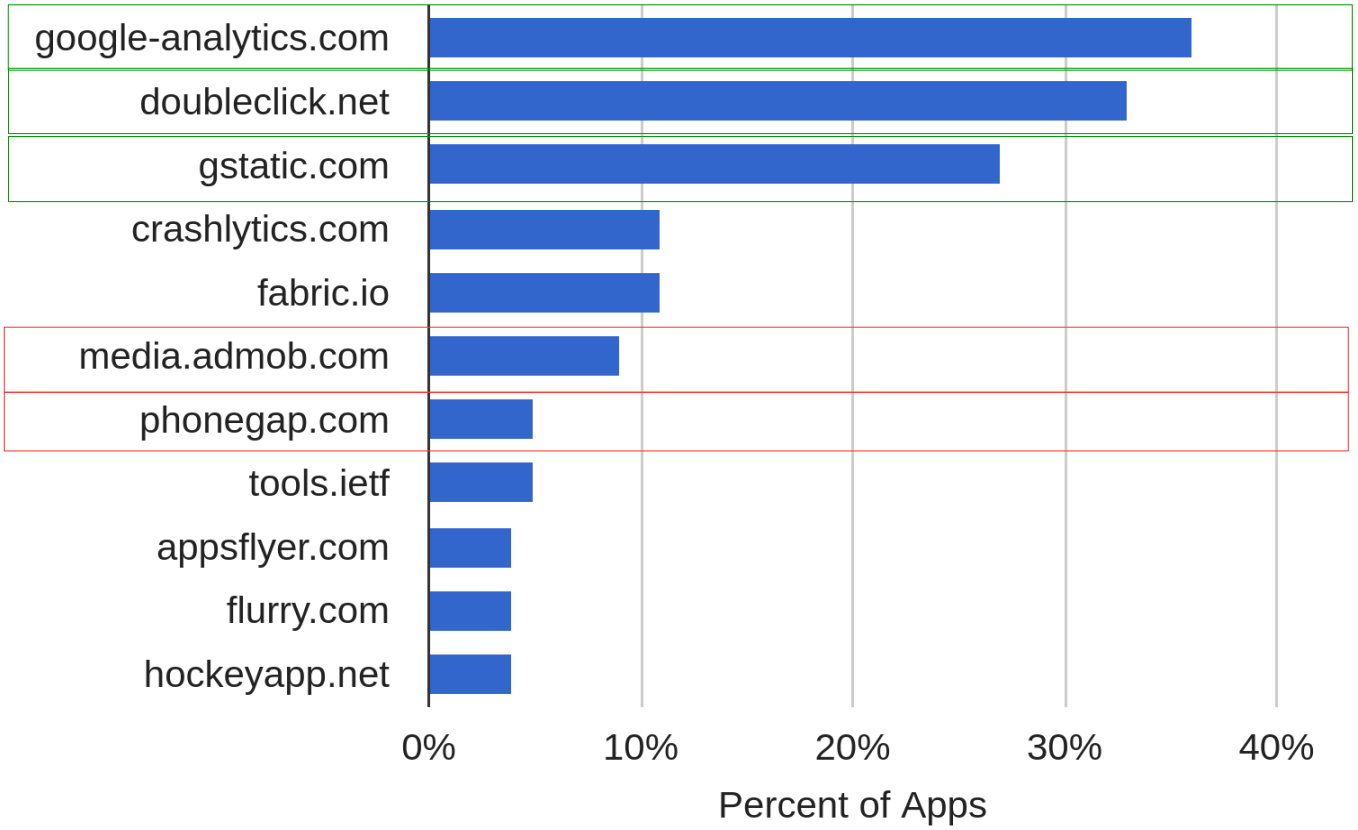
Availability
reliable access to services

Data Loss
DoS
Device Theft

Android apps contain numerous HTTP URLs.

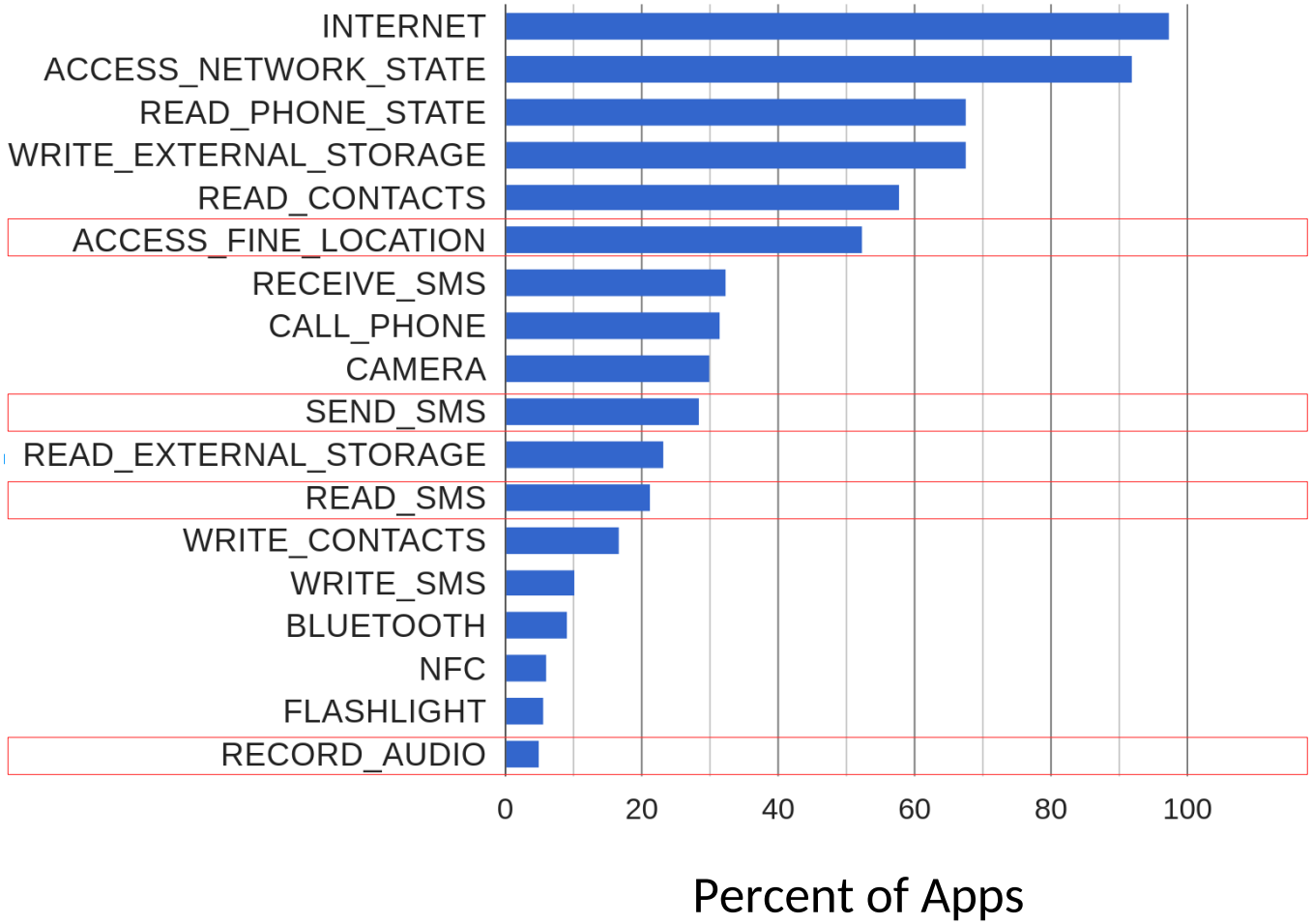


...and known tracking libraries

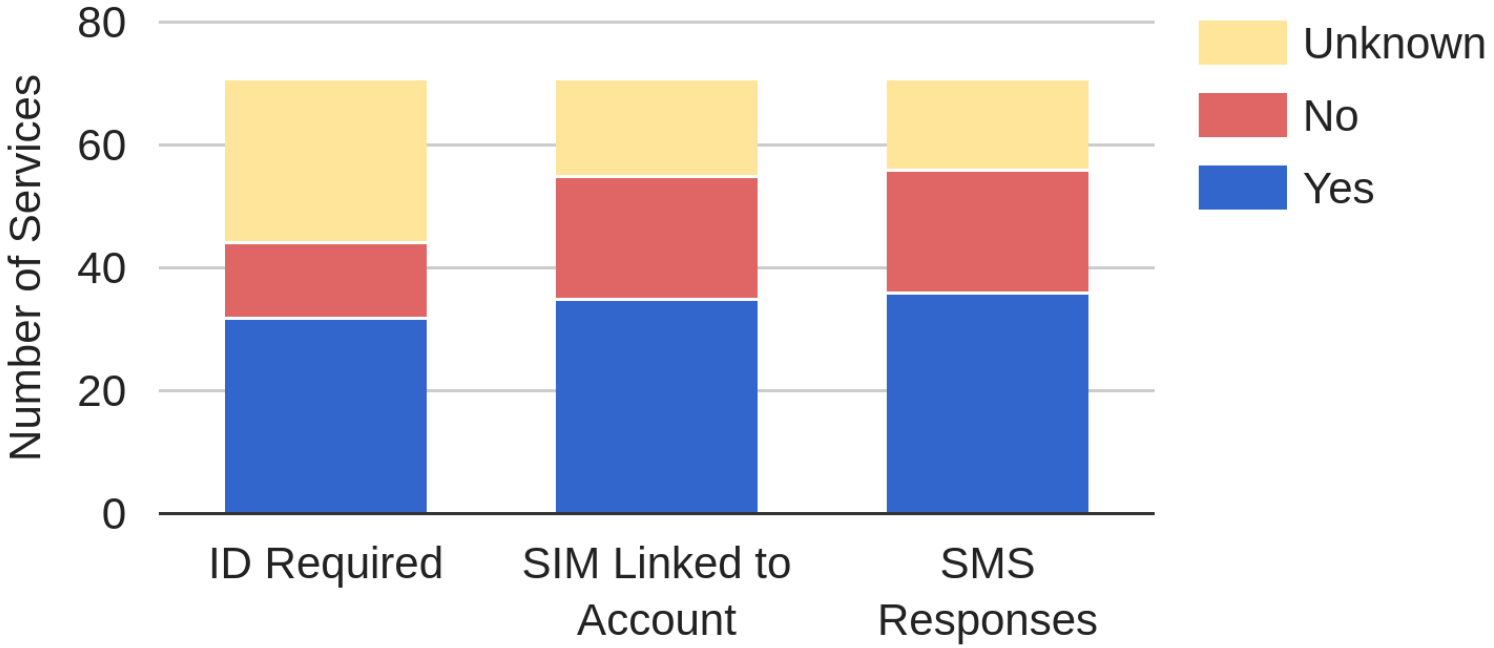


Chen et al., Oakland 2016.

Over-privilege



Manual Analysis of 71 Services



Developer Interviews

- **Goal**: Understand the source of vulnerabilities
- Contacted 249 email addresses
- **Location**: Nigeria, Kenya (2), Uganda, Zimbabwe, Colombia (2)
- **Organizations**: Bank (2), Telco (3), Software Company (2)
- Mostly large organizations

Developer Interviews

1. Stack Overflow used "*almost in all projects*"

2. External Libraries

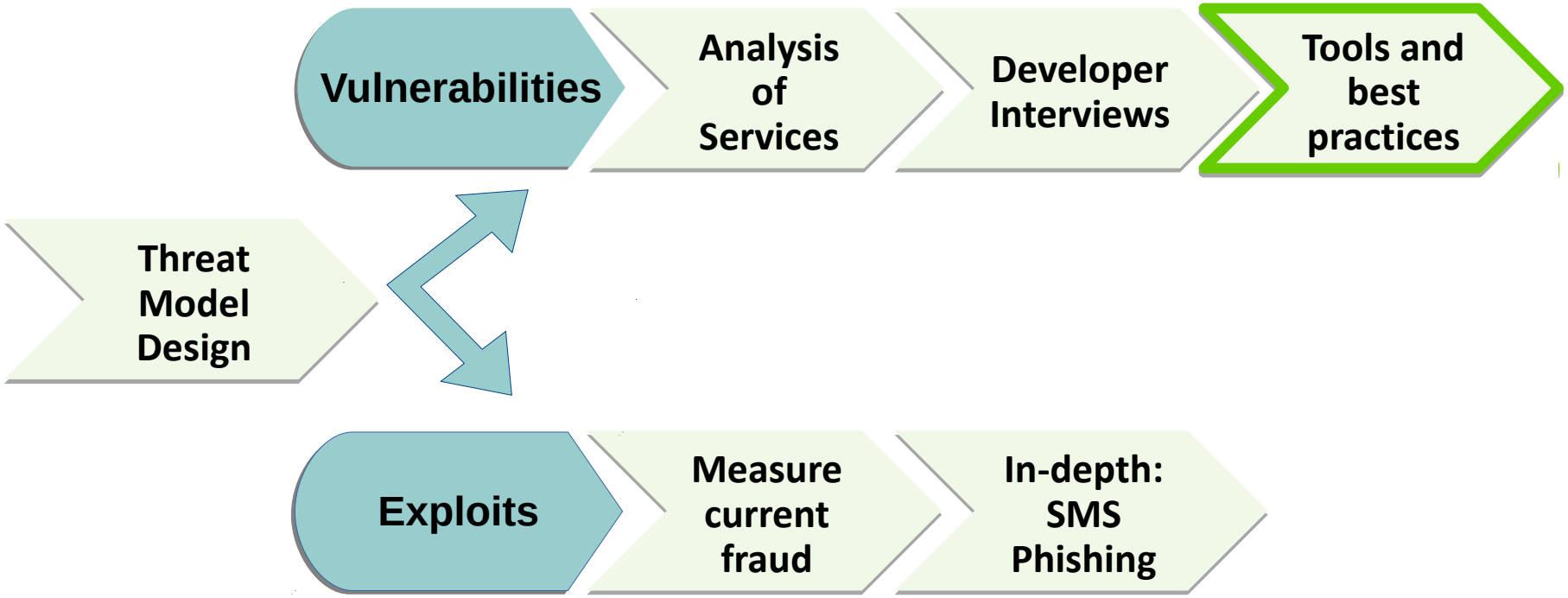
> I don't believe there is anything that's perfect and free. If you include someone's library and it is very good, you have to ask yourself why is he giving it out for free?

Developer Interviews

3. Partners and Regulations

You will find a market where a gang of criminals exposed a particular human hack and made off with 2 million dollars. Then there will be this uproar and the government will just make a piece of regulation that requires customers to go to the customer service location and present 7 forms of ID and their mother's DNA…That's emerging markets for you.

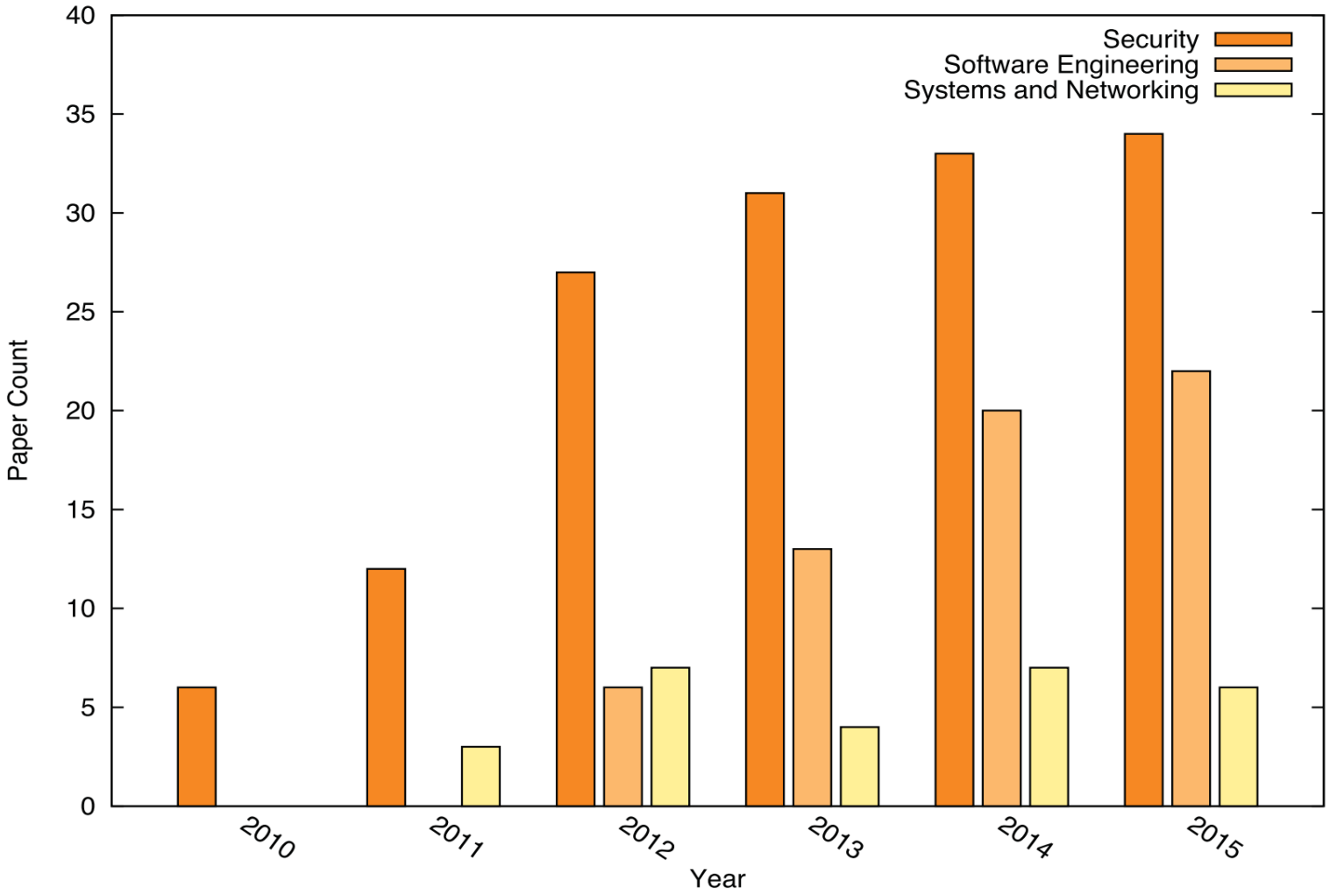
We did one crazy one in West Africa where they didn't use any [encryption]. We made them sign documents seven ways to Sunday because we were worried about [security]. What you'll find in these markets is that you have an IT person, and you are forced to work to their level of expertise.



PART 2: DEVELOPER TOOLS

Goals for Developer Tools

- **Resources for Best Practices**
  - Document domain-specific security practices
- **Developer Self-Assessment Tools**
  - Build tools to provide relevant feedback on potential vulnerabilities in Android and USSD apps
  - Leverage prior research on automated Android analysis
  - Combine manual developer analysis for nuanced issues, such as PIN recovery



35 static analysis tools since 2011

8 dynamic analysis tools since 2012

Source: Reaves et al.

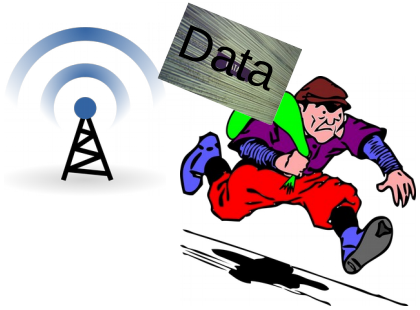
Framing

Device Loss/Theft

1. How are users authenticated?
2. Account tied to SIM?
3. Account recovery?

Man-in-the-Middle

1. How is data encrypted?
2. Are offline transactions permitted?



Customers Stealing Data

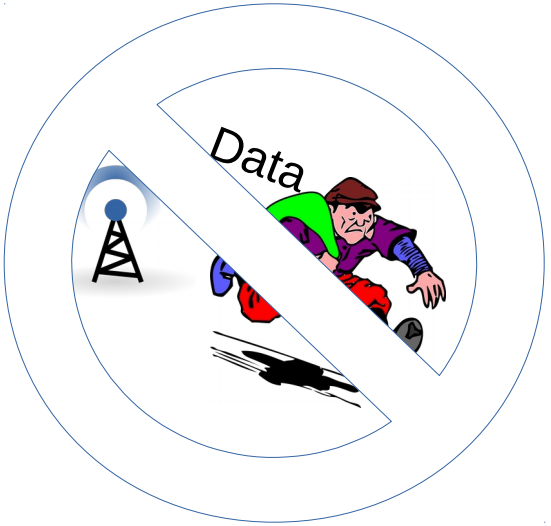
1. SSL/TLS?
2. Are zero-rated URLs properly protected?

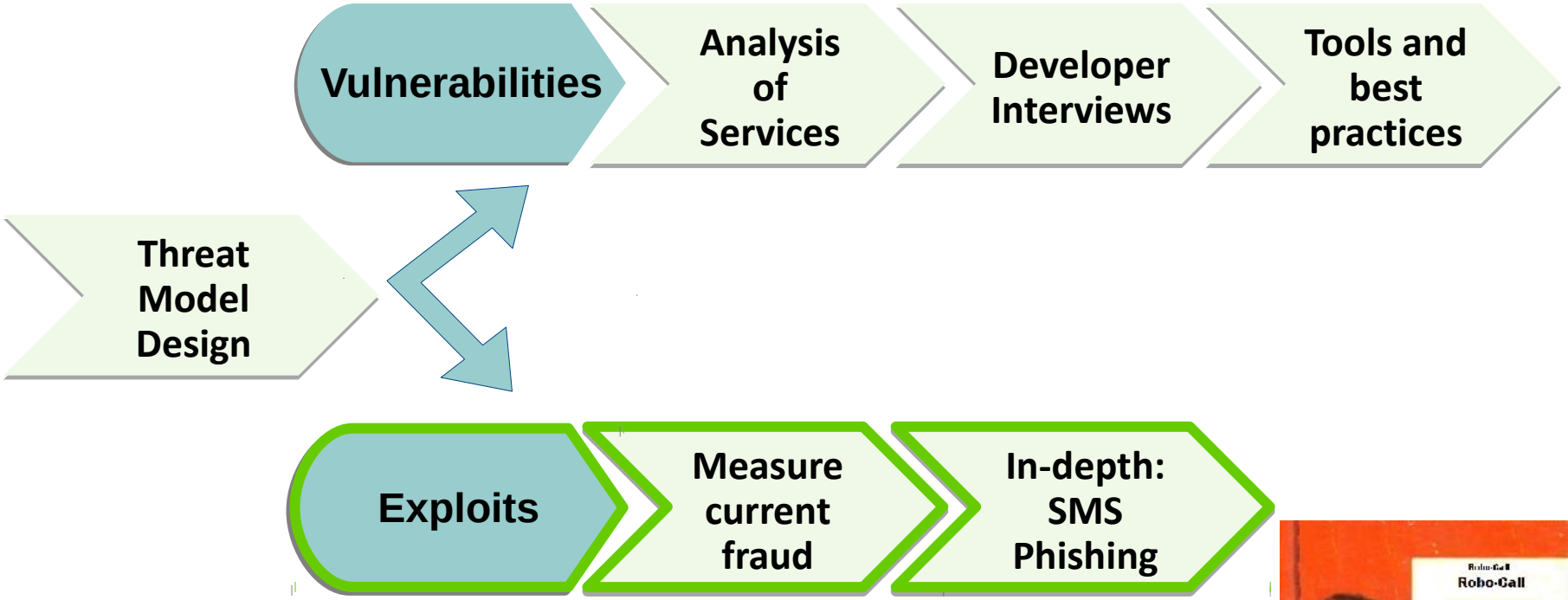
Mapping Responses to Analysis

	4-digit PIN	Account Linked to SIM	Incorrect SSL/TLS	…
Usability				
No memory	½	✓	✓	
Infrequent errors	½	✓	✓	
Security				
Resilient to throttled guessing	✗	✓	✗	
Resilient to phishing	✗	✓	✗	
Scalability				
No cost per user	✓	½	✓	
Compatible	✓	✓	✓	

Sample output for Developer tools

- Key Issues:
  - SSL/TLS vulnerability
  - Data storage on Device
- Particular threats:





PART 3: FRAUD IN MOBILE MONEY

SMS-driven Fraud

fraud /frawd/ *n.*

1. wrongful or criminal deception intended to result in financial or personal gain

'He was convicted of fraud.'

spam /spam/ *n.*

1. unwanted or intrusive advertising on the Internet

'Well could I have her spam instead of the baked beans then?'

Source: OED

SMS-driven Fraud

- 7.6 billion mobile connections
- 4.7 billion unique subscribers

- Transactions SMS
- Payments and dues
- One-time pins
- Account recovery SMS

Research Questions

- ☑ What types of fraud are occurring over SMS
- ☑ What are System-level indicators to detect fraud
- ☑ Different telco and user level fraud detection methods
- ☑ Fraud detection in Android vs. feature phones

Spam Blocking

Automatic

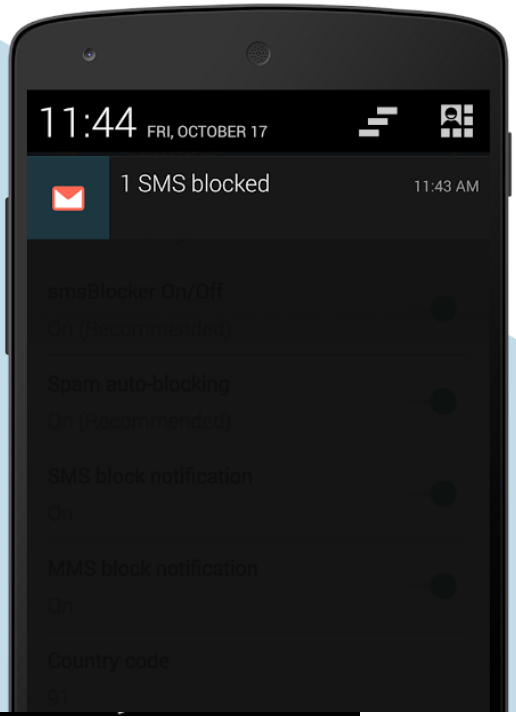
Award winning Spam Auto-Block technology

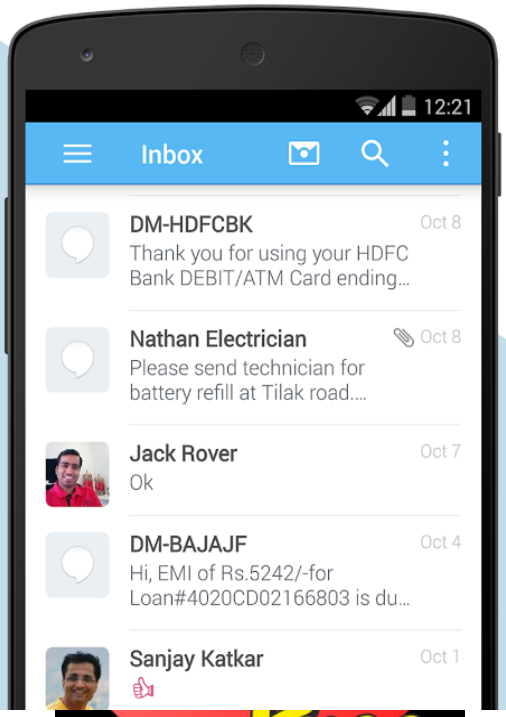
Spam-free Inbox

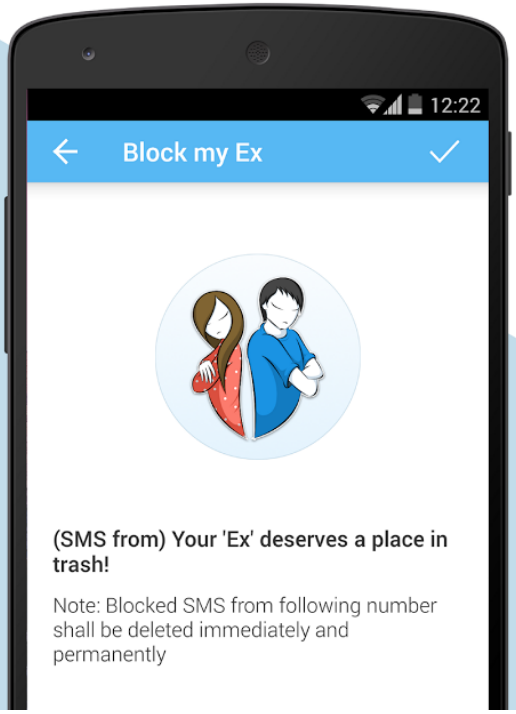
Get only messages that you want

Block my Ex

Best way to get rid of text from BF/GF (Prm.)

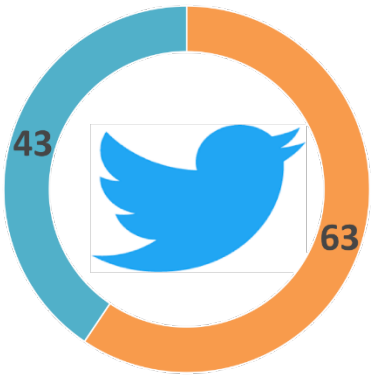


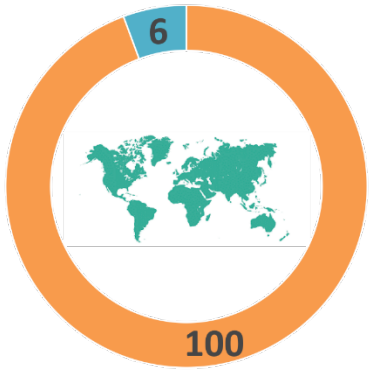


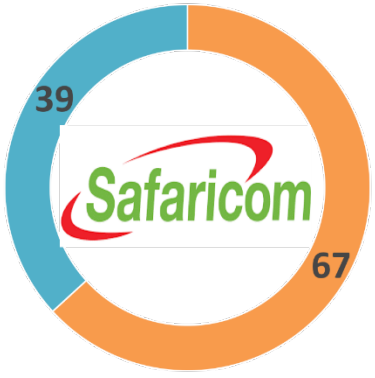


Preliminary Findings

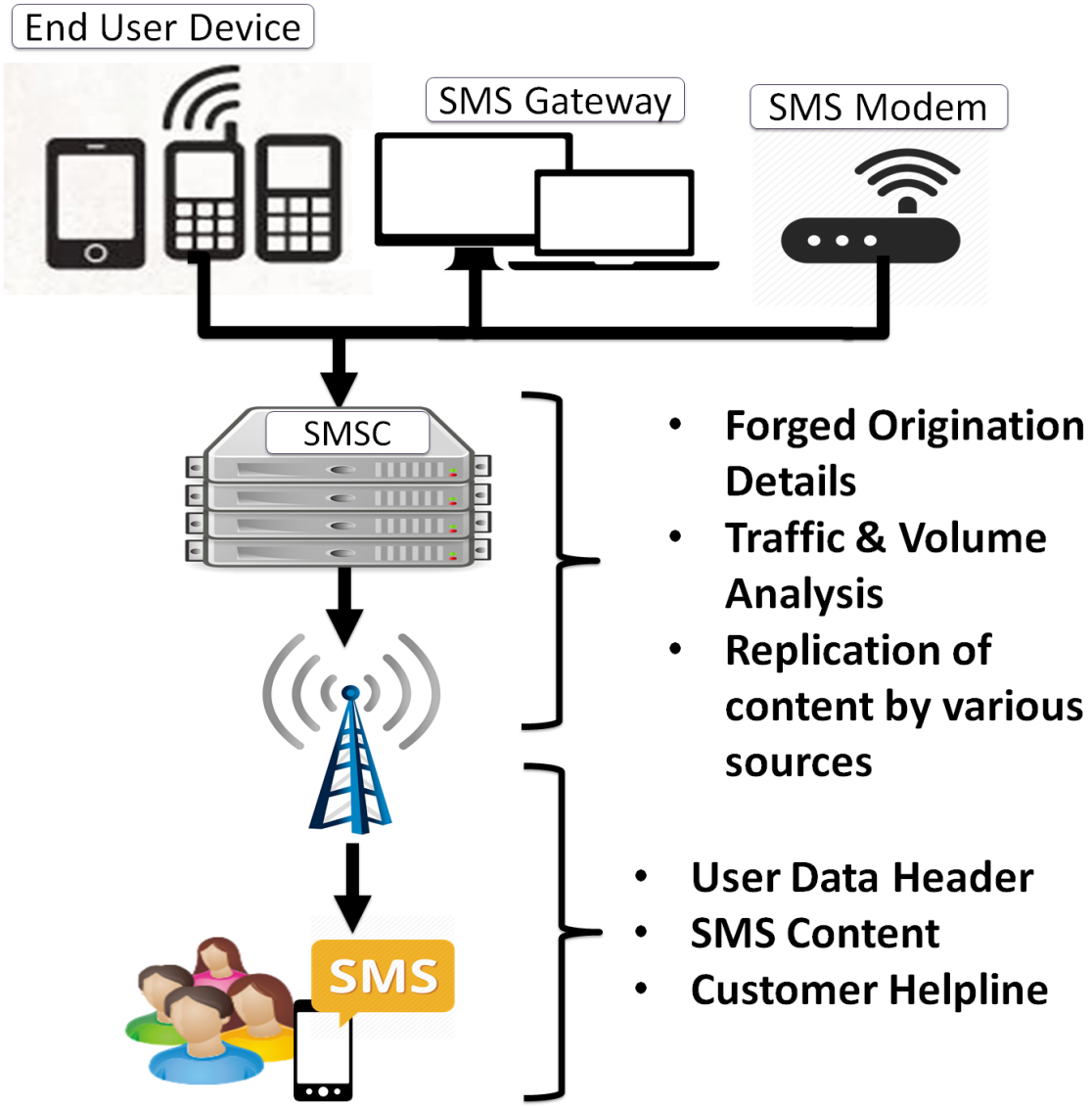
- We collected 106 SMS Examples

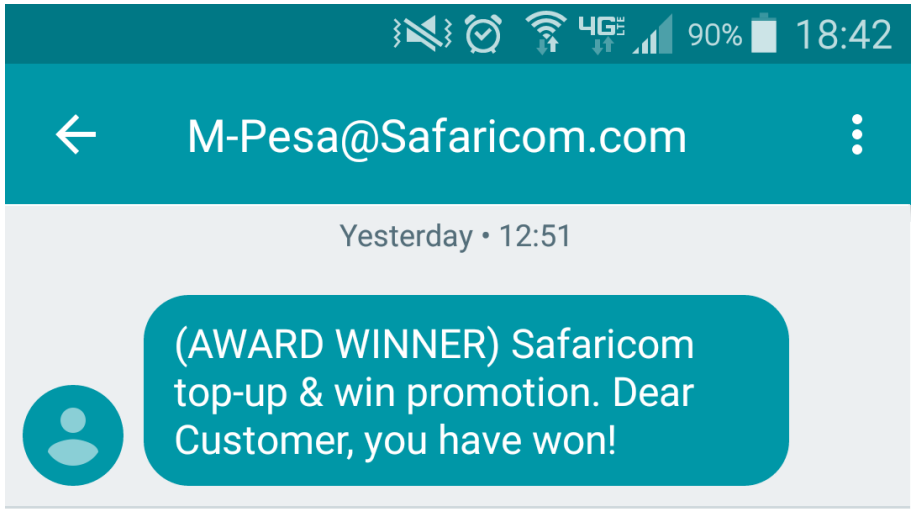


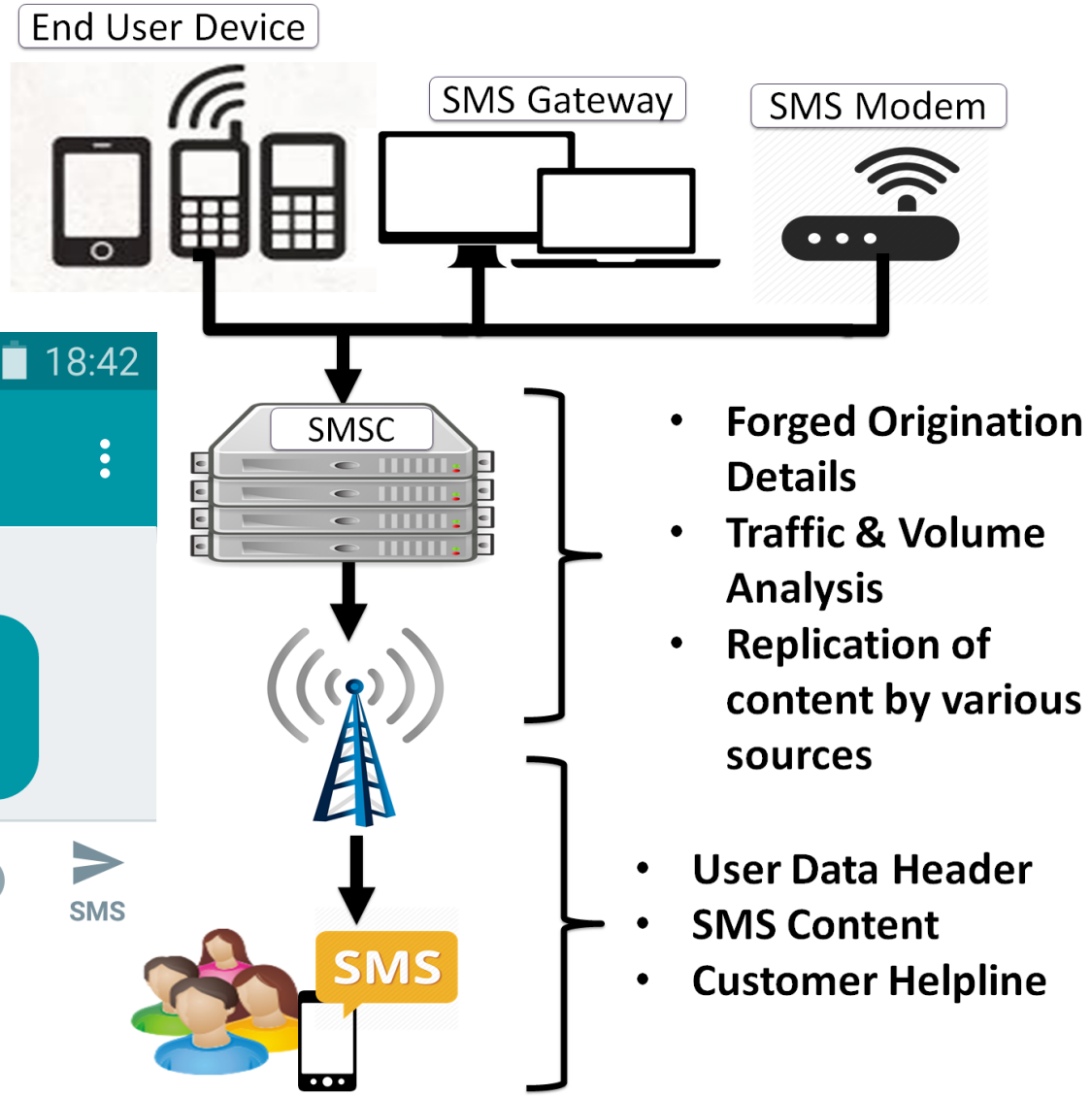




- Major categories: promotions, receipts, and loan offers


End User Device
SMS Gateway
SMS Modem
SMSC
SMS
• Forged Origination Details
• Traffic & Volume Analysis
• Replication of content by various sources
• User Data Header
• SMS Content
• Customer Helpline



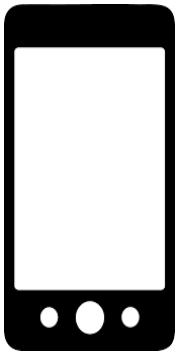


- **Forged Origination Details**
- **Traffic & Volume Analysis**
- **Replication of content by various sources**

- **User Data Header**
- **SMS Content**
- **Customer Helpline**

Safaricom

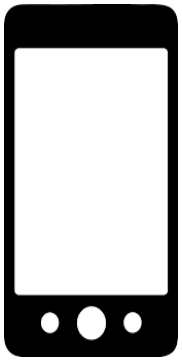
KGK49RRT70 Confirmed. You have received Ksh16,065.00 from SAM CASTLE on 20/7/16 at 5:20 AM. New M-PESA balance is Ksh16,115.00. Buy goods with M-PESA.



KKJ6A94PXJD Confirmed.You have received Ksh 4,530.00 from SAM CASTLE on 29/11/16 at New M-PESA balance is Ksh *(PENDING)* Pay bills via M-PESA.

Receipts

Shinda Ma-Mili na Stori Ibambe! Dial *460# to get more information on the Shinda Ma-Mili Promotion. Hit your STORO target and stand a chance to win.

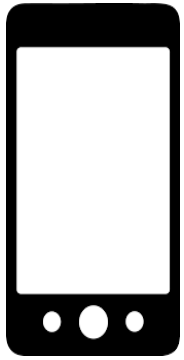


Shinda Ma-Mili na Stori Ibambe!Dial 0780000520 to get more information on the Shinda Ma-Mili Promotion. You're the lucky win.of ksh100,000 DOT PAY ANY!

Promotions

Safaricom

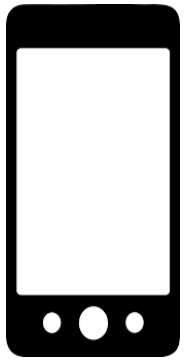
Dear Customer, we have applied a rollover fee of Ksh 337.50 on your loan which is now overdu.Your loan balance is Ksh 5,171.29 and due date was 10/04/16.



Loans

Dear Customer, your M-Shwari loan limit is Kshs. 1,000. To access your limit, present your ID at a Safaricom shop to update your details. http://bit.ly/2aVHAgJ

DA10HM222 Confirmed. Your M-Shwari loan request is approved. New M-PESA balance is Ksh 1,155.00.



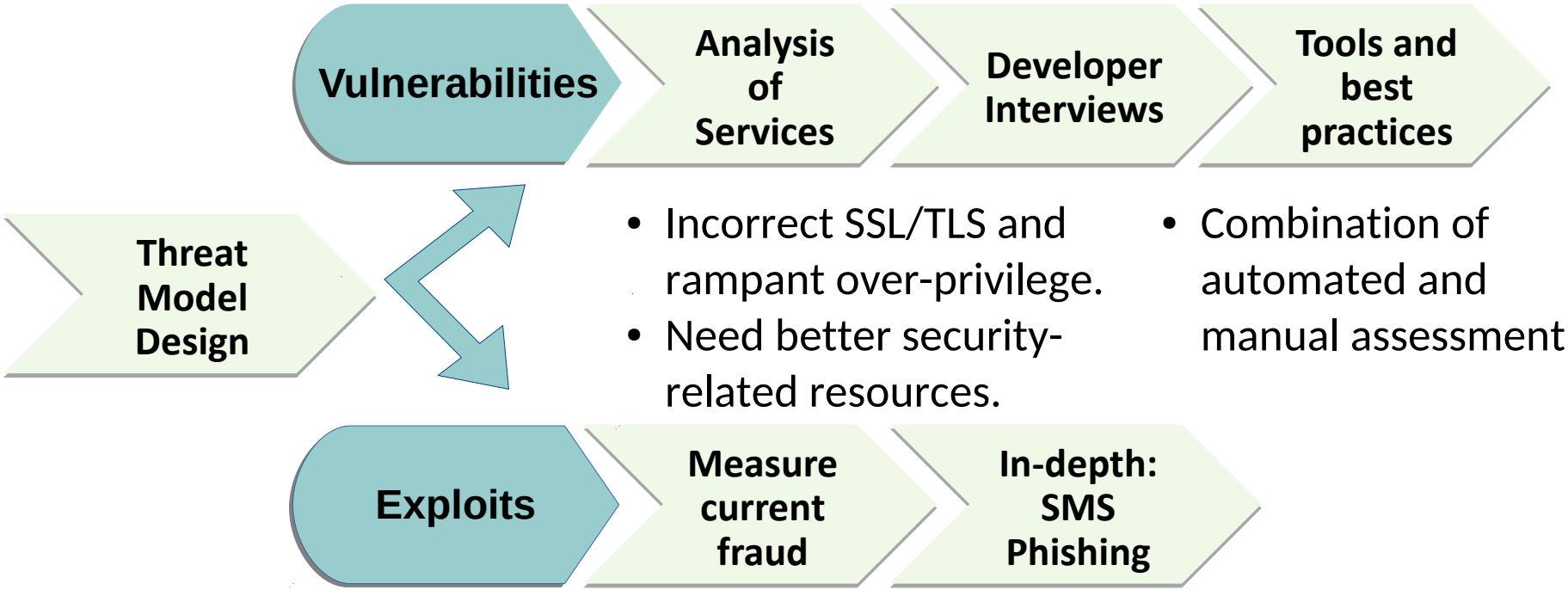
Loans

Dear Customer KCB M-PESA Soft loan now is Available at 0.5%interest 15%saving. KSH. 50,000 100,000 250,000 Call/text on: 0789783835 KCB Making the Difference.

Next Steps

- A user study to collect a larger data corpus.
- Understand people's ability to detect phishing SMS.
- Develop and deploy SMS-fraud detection and mitigation tools.

CONCLUSIONS

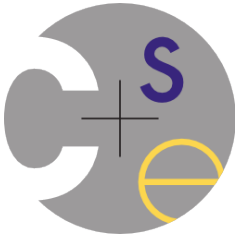


- Incorrect SSL/TLS and rampant over-privilege.
- Need better security-related resources.

- Combination of automated and manual assessment.

- Phishing is common in practice.
- Main categories are promotions, loans, and fake receipts.
- URLs and phone numbers (not misspellings) indicate fraud.
- Twitter is a valuable data source.

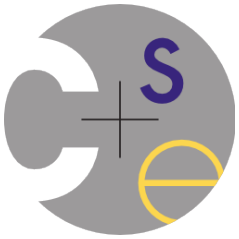
Thanks to the ICTD Lab and Collaborators



Questions

Sam Castle
University of Washington
Seattle, USA

UNIVERSITY of WASHINGTON



DIGITAL FINANCIAL SERVICES
RESEARCH GROUP