Thin Sim-Based Mobile Money Attacks

Rowan Phipps, Shrirang Mare, Peter Ney, Jennifer Rose Webster, Kurtis Heimerl
Goals

Investigate security vulnerabilities introduced by thinSIMs

Propose possible defenses for these vulnerabilities
What do SIM cards do

- Identify users on the network
- Authenticate the device on the network
- Call Control
- Run Sim Toolkit (STK) apps
What are STK apps

- Run on the SIM card
- Consists of menus and input prompts
- Defined by GSM 11.14
Normal SIM app operations
What is USSD

Unstructured Supplementary Service Data

● Dialed like a voice number
● No records are stored on the device
● Provides a text only interface
What is USSD

*123#  Connects to the USSD service at 123

*123*1#  Connect to the USSD service at 123 and enters 1 at the first prompt
Thin Sims

Bladox Turbo SIM

2FF Form Factor

3FF Form Factor

4FF Form Factor

TAISYS SIMoME ®
Thin Sims

- Field installable
- Contains all the functionality of a sim card
- Allows third party apps
- Free from carrier restrictions
- Can read and modify all communication between the phone and the sim card
Reasons For Installation

- Distribution of apps
- Cell phone unlocking
- Malicious Installation
The Rise of M-Pesa

- Founded by Safaricom in 2007
- Transfers the equivalent of 44% of the Kenyan GDP
- Has since expanded to many other countries.
- Runs primarily through an STK app
Equity Bank

- Tried to launch their own stk based mobile money platform
- Decided to use thin SIMs to distribute their app
- Safaricom opposed this citing security concerns
- Court ruled in favor of Equity bank in 2015
An app running on the thin SIM
App running on the original sim card with a thin SIM installed
What if the thin SIM is not friendly?
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
M-Pesa STK app attack

Safaricom and Airtel both have sim app based mobile money platforms that facilitate large amounts of trade however we primarily focused on M-Pesa.

The attack takes place in two phases:

1. Steal Credentials
2. Make fraudulent payments
Phase 1: Get Credentials

Phone

Thin Sim

Sim card
Phase 1: Get Credentials

1. Transparently passes STK commands
Phase 1: Get Credentials

1. Transparently passes STK commands
2. Listens until the sim asks for the user’s PIN
Phase 1: Get Credentials

1. Transparently passes STK commands
2. Listens until the sim asks for the user’s PIN
3. Stores the response
Phase 2: Make Payments

Phone

Thin Sim

Sim card
Phase 2: Make Payments

1. Status Update

Phone  Thin Sim  Sim card
Phase 2: Make Payments

1. Status Update

2. Spoof Transaction
Phase 2: Make Payments

1. Status Update

2. Spoof Transaction

3. SMS Callback
Phase 2: Make Payments

1. Status Update
2. Spoof Transaction
3. SMS Callback
4. Send silent SMS
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
Call Control

Call Control Mechanism: Allow

Call (123) 456 7890

Allow, unmodified
Call Control Mechanism: Modify

Call (123) 456 7890

Redirect to:
(111) 222 3333
Call Control sounds harmless enough right?
Call Control attacks

- Call tracking for targeted advertising, surveillance, or blackmail
- Phishing attacks
- Premium rate calls
- Redirect USSD calls
USSD Attack

This attack also consists of two phases

1. Steal Credentials
2. Make Transactions

Requires the attackers to set up their own USSD service.
USSD Attack Phase 1

- Legitimate USSD Service
  *1234#

- Attacker’s USSD Service
  *5678#
USSD Attack Phase 1

1. Call *1234#
2. Redirect to *5678#
USSD Attack Phase 1

1. Call *1234#
2. Redirect to *5678#
3. Send Payment Details
USSD Attack Phase 1

1. Call *1234#
2. Redirect to *5678#
3. Send Payment Details
4. Error

Legitimate USSD Service
*1234#

Attacker’s USSD Service
*5678#
USSD Attack Phase 2

1. Call *5678#

Legitimate USSD Service
*1234#

Attacker’s USSD Service
*5678#
USSD Attack Phase 2

1. Call *5678#
2. Payment details

Legitimate USSD Service
*1234#

Attacker’s USSD Service
*5678#
1. Call *5678#
2. Payment details
3. Make transaction

USSD Attack Phase 2

Legitimate USSD Service
*1234#

Attacker’s USSD Service
*5678#
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
Thin SIM Capabilities

- Intercept, modify and create stk commands
- View responses to stk commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user’s knowledge
- Track location updates
- Perform GSM authentication actions
- Read data from the sim card including the IMSI and phonebook.
Possible Defenses
Possible Defenses

- Disable call control
  - Requires modifying the standard
- Disable the ability to silence outgoing sms and USSD
- Discourage the use of thin sims by allowing third party apps on carrier sims
- For STK and USSD: Send confirmation code via sms
Summary

Developed two proof of concept attacks against mobile money utilising thin Sims.

Demonstrated the Thin Sims have the potential to be dangerous and to discourage their usage.

Finally, we proposed possible defenses and explained why other defenses are infeasible.
Questions?