# THIN SIM-BASED ATTACKS ON MOBILE MONEY SYSTEM

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



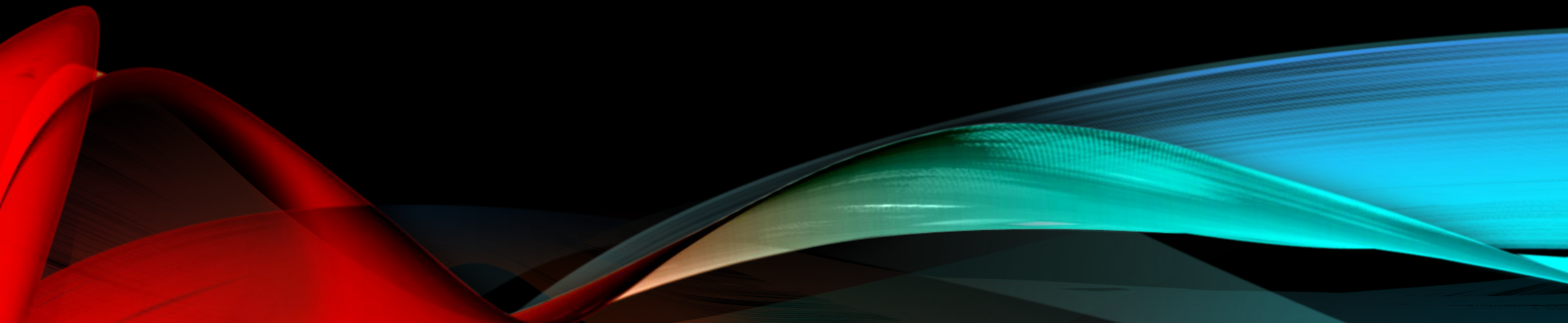



# GOALS

Investigate security vulnerabilities introduced by thinSIMs

Propose possible defenses for these vulnerabilities

# BACKGROUND



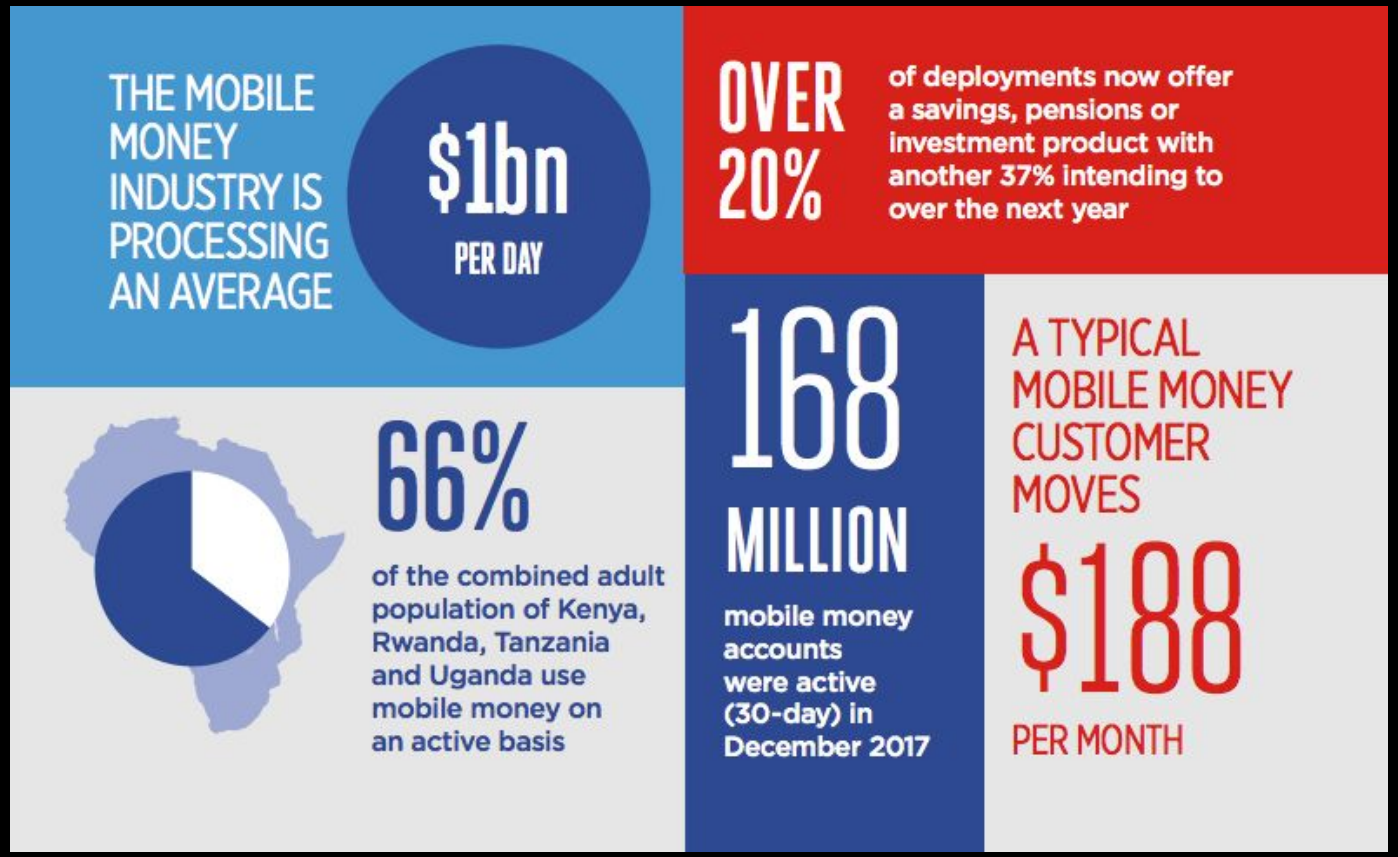
# MOBILE MONEY

# MOBILE MONEY



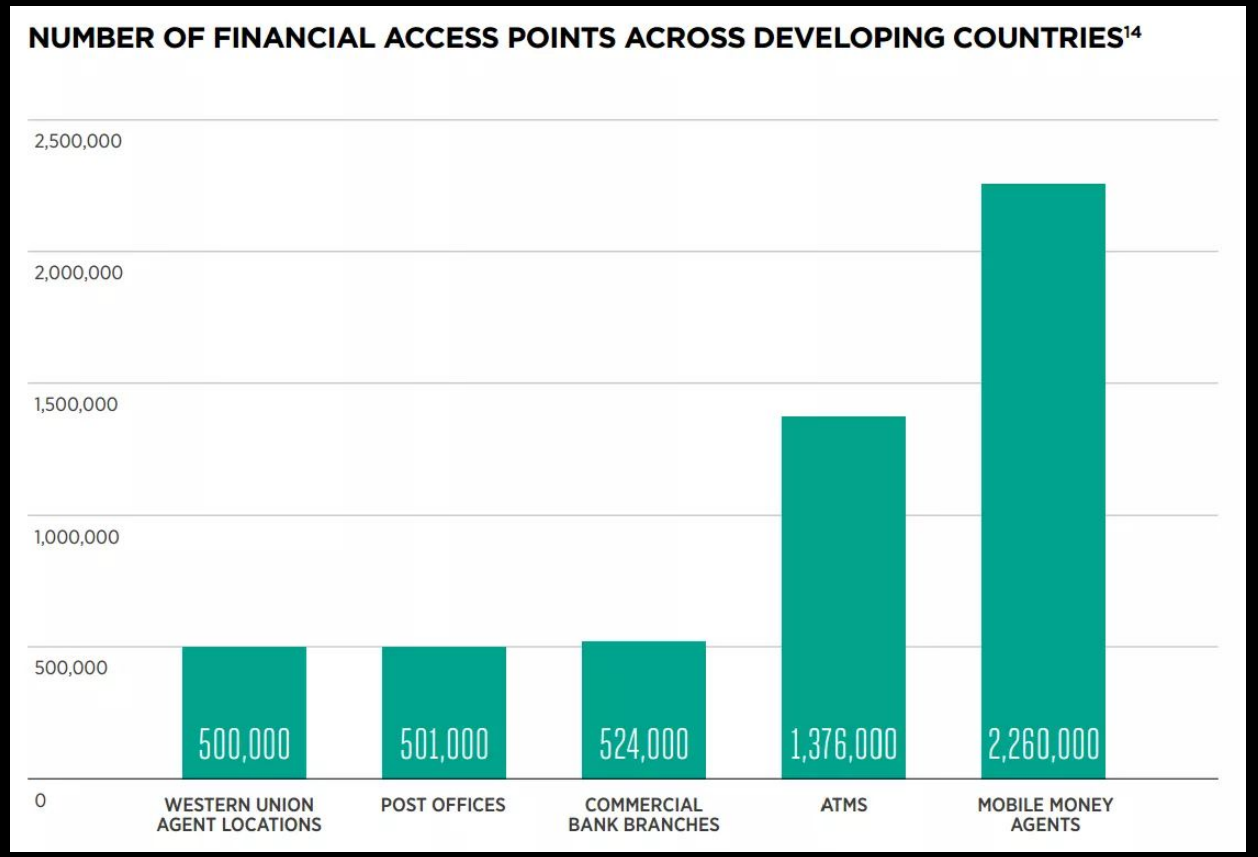

Source: GSMA (2017)

# MOBILE MONEY



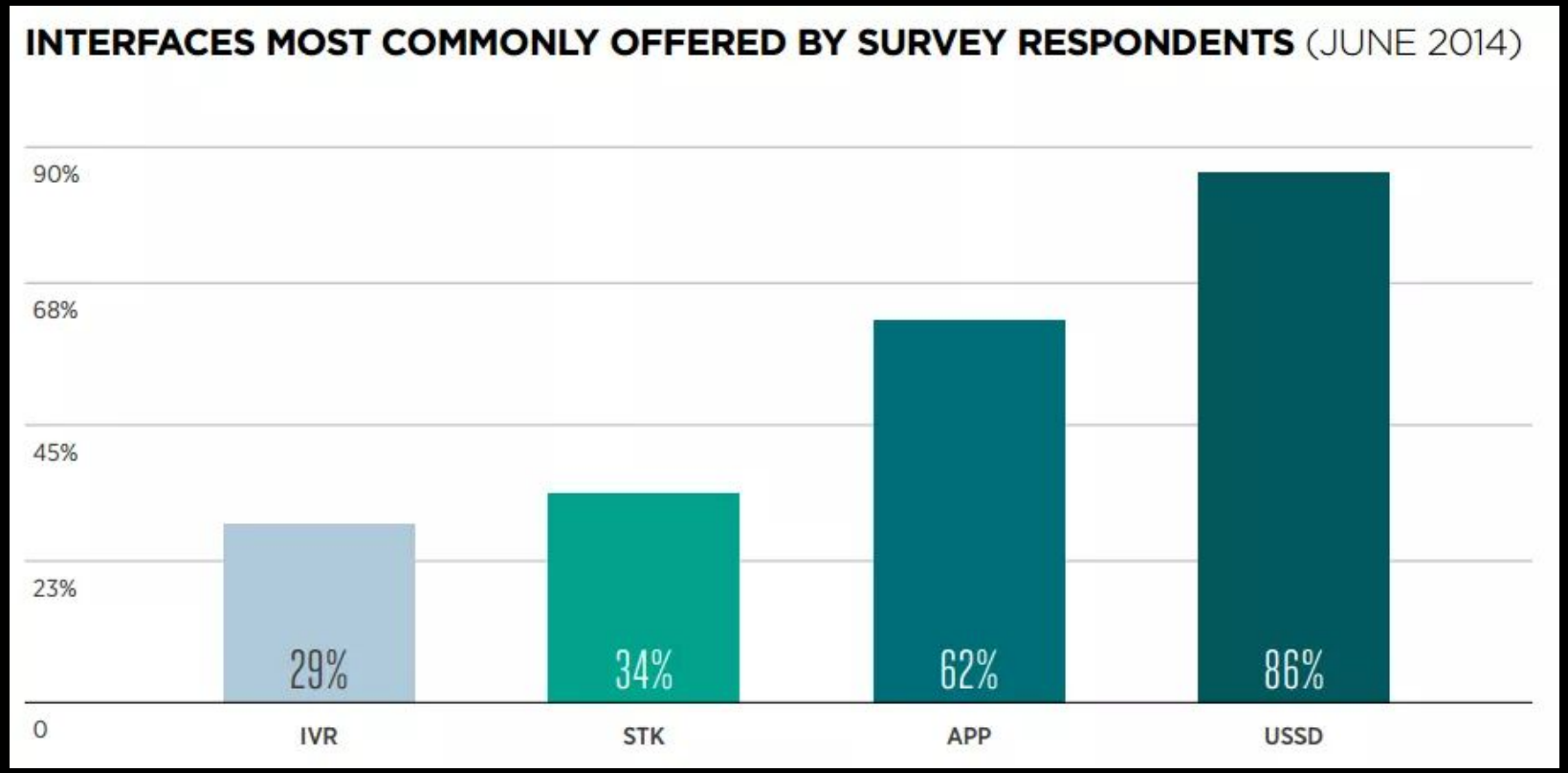

Source: GSMA (2017)

# MOBILE MONEY




Source: GSMA (2015)

# MOBILE MONEY



# MOBILE MONEY: PLATFORMS

## Smart Phone Apps

- Richest UI
- Easy to develop for
- Requires no cooperation from phone companies
- Requires data
- Requires a smart phone

## Sim ToolKit Apps

- Runs on any hardware
- Does not require data
- Menu based UI
- Requires cooperation from the phone company
- Requires a special SIM card

## USSD

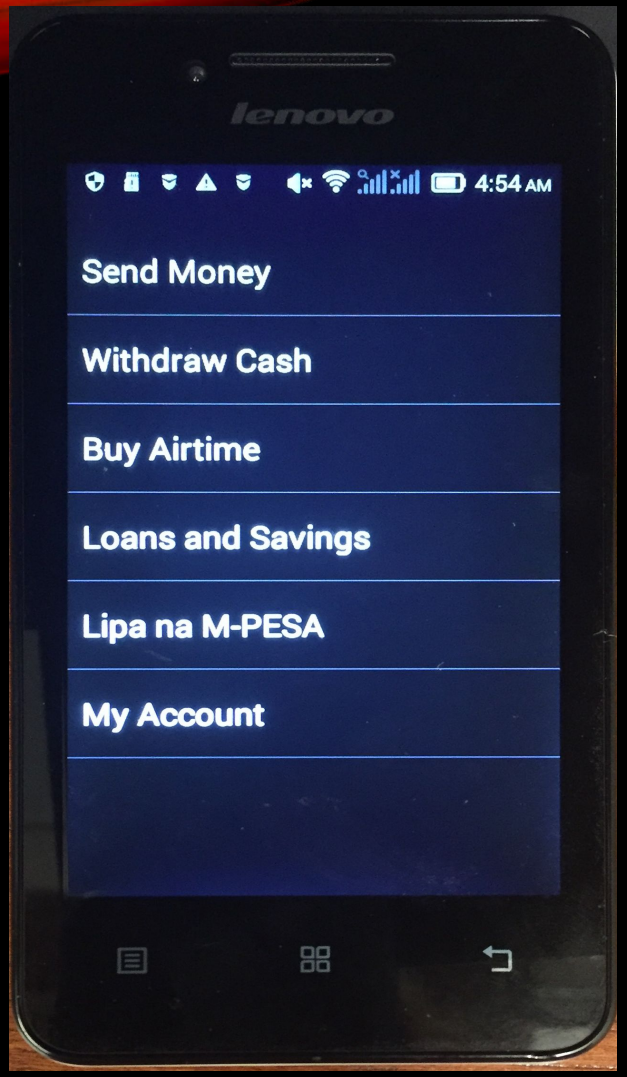
- Runs on any hardware
- No SIM card requirements
- Standardized UI
- Does not require data
- Less carrier cooperation required
- Text only interface

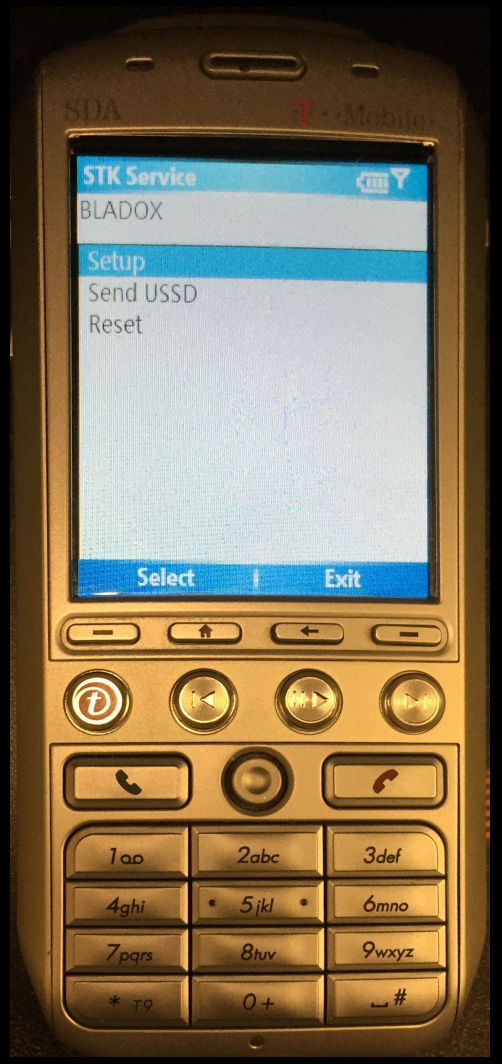
# SIM CARDS

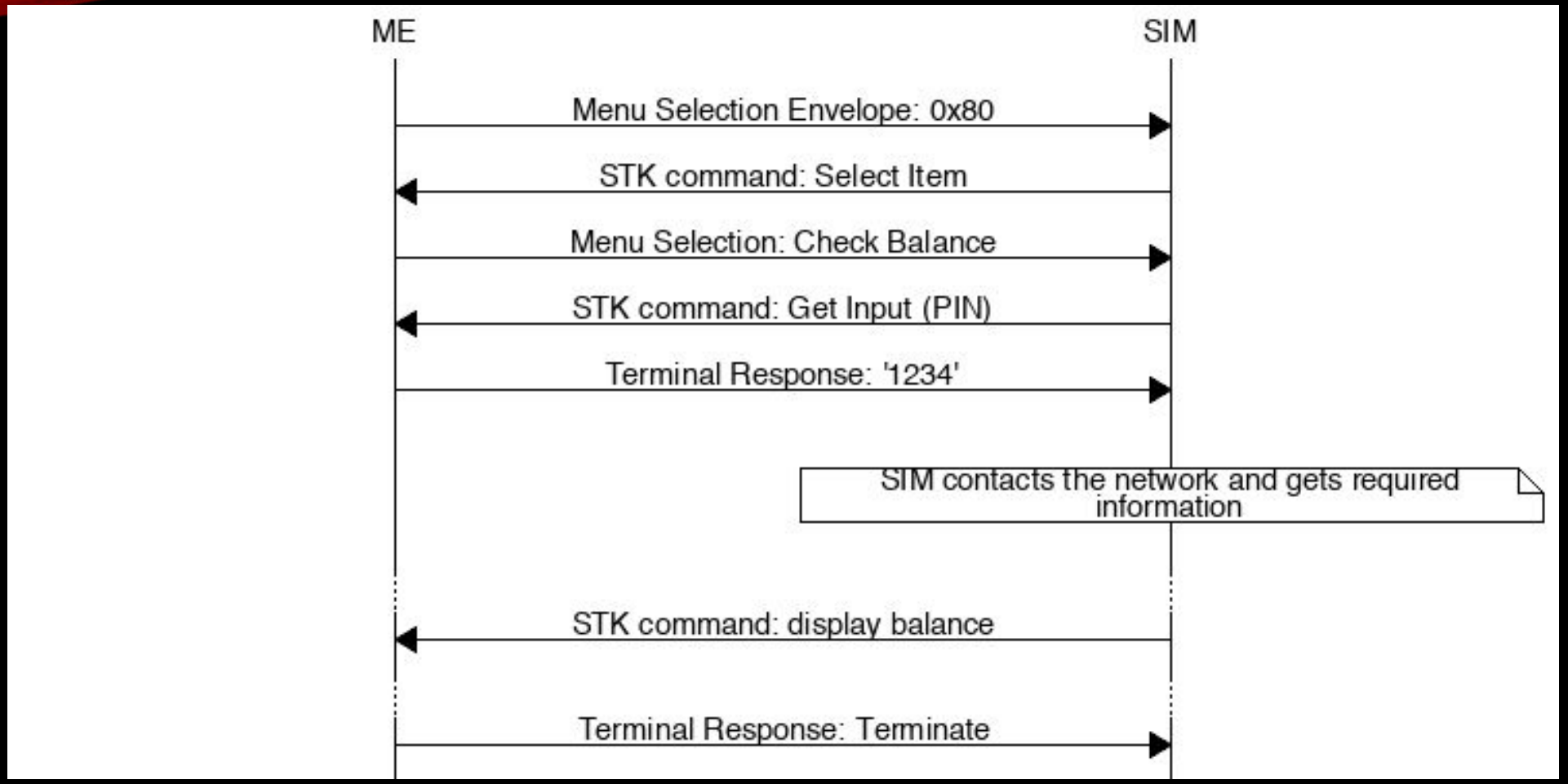
- Identify users on the network
- Authenticate the device on the network
- Call Control
- Run Sim Toolkit (STK) apps

# SIM TOOLKIT (STK) APPLICATIONS

- Run on the SIM card
- Consists of menus and input prompts
- Defined by GSM 11.14


lenovo
4:54 AM
Send Money
Withdraw Cash
Buy Airtime
Loans and Savings
Lipa na M-PESA
My Account


STK Service
BLADOX
Setup
Send USSD
Reset
Select
Exit




STK message flow

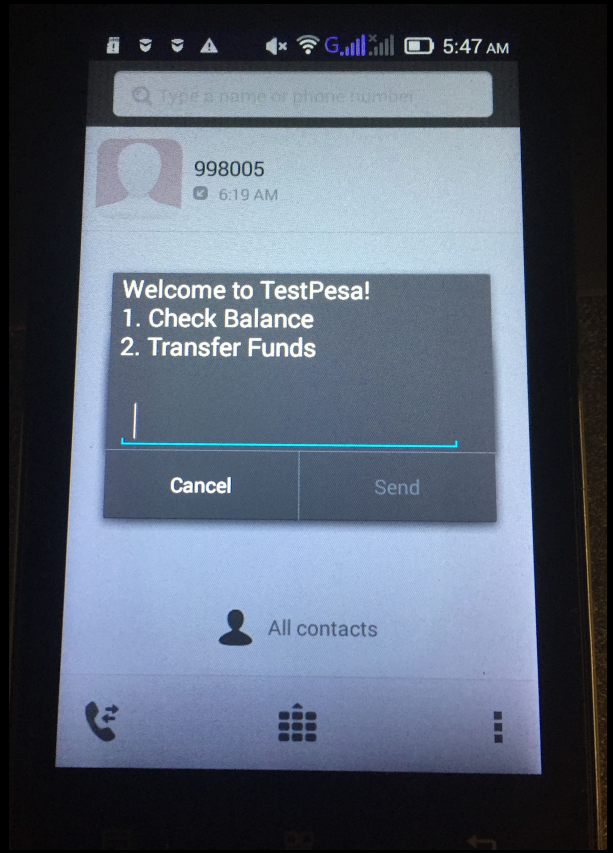
# MESSAGE STRUCTURE

D0 19 81 03 01 21 81 82 02 81 02 8D 0E 04 43 68 65 63 6B 20 42 61 6C 61 6E 63 65 90 00

0xD0 - Proactive STK command
- 0x19 - length (25 bytes)
- 0x81 - Command details tag
  - 0x03 - length
  - 0x01 - command number
  - 0x21 - DISPLAY TEXT
  - 0x81 - RFU
- 0x82 - Device identity tag
  - 0x02 - length
  - 0x81 - src: SIM
  - 0x02 - dst: Display
- 0x8D - Text string tag
  - 0x0E - length (14 bytes)
  - 0x04- encoding
  - 43 68 65 63 6B 20 42 61 6C 61 6E 63 65 - "Check Balance"

# UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD)

- Dialed like a voice number
- No records are stored on the device
- Provides a text only interface

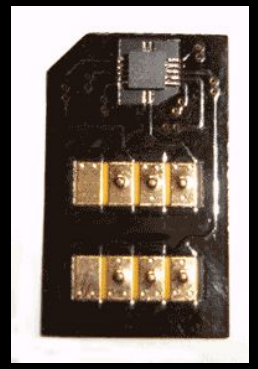


# UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD)

| | |
|---|---|
| *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


SIM card
SIM card
SIM card
SIM card
SIM card
SIM card




2FF Form Factor
3FF Form Factor
4FF Form Factor

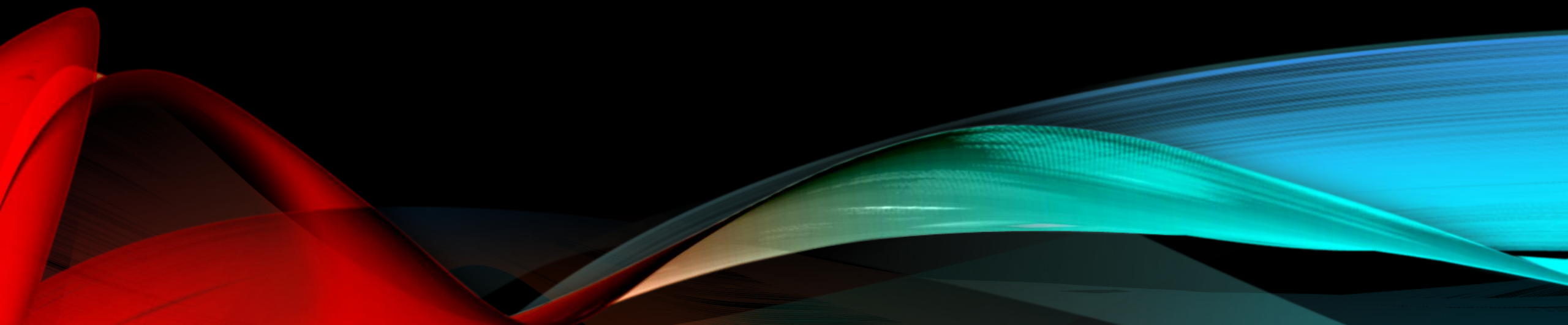
# THIN SIMS: WHAT

- 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

# THIN SIMS: WHY

- Cell phone unlocking
- Distribution of apps
- Malicious Installation

# M-PESA CASE STUDY



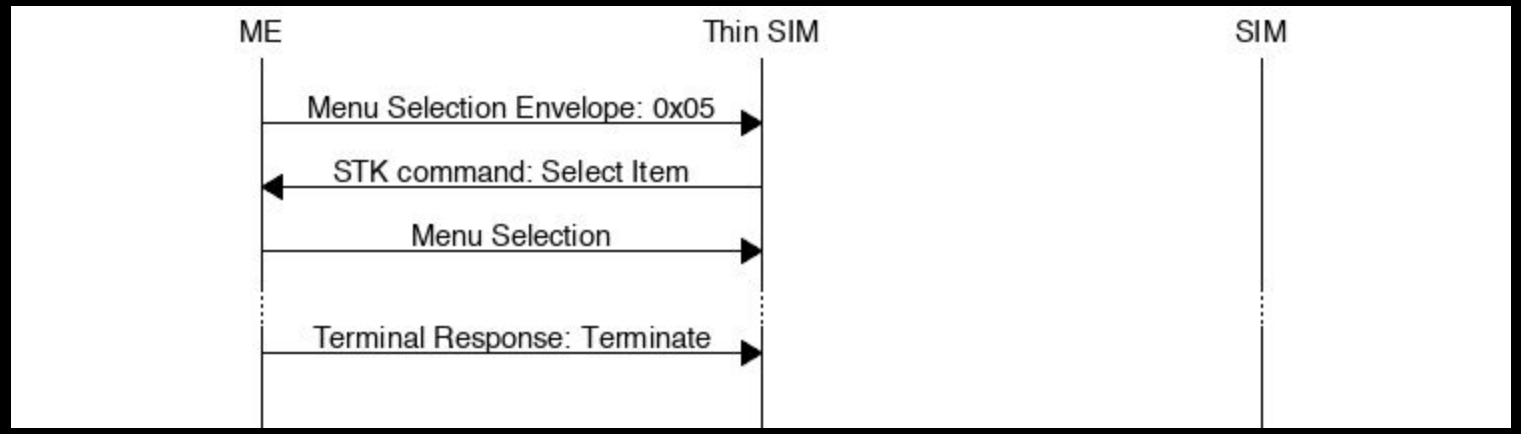
# THE RISE OF M-PESA

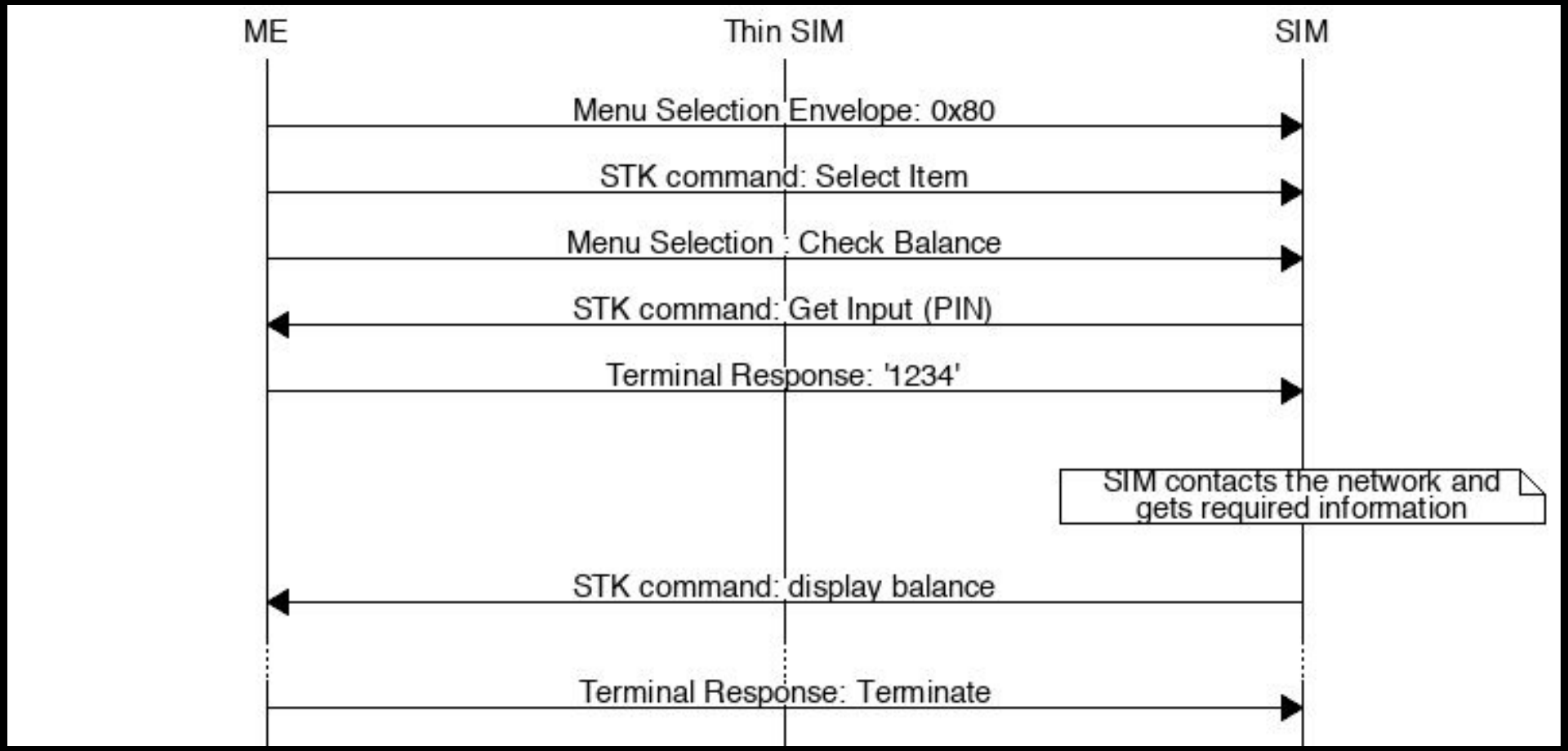
- Founded by Safaricom in 2007
- Transfers the equivalent of 44% of the Kenyan GDP
- Has since expanded to many other countries.
- Runs primarily through an STK app



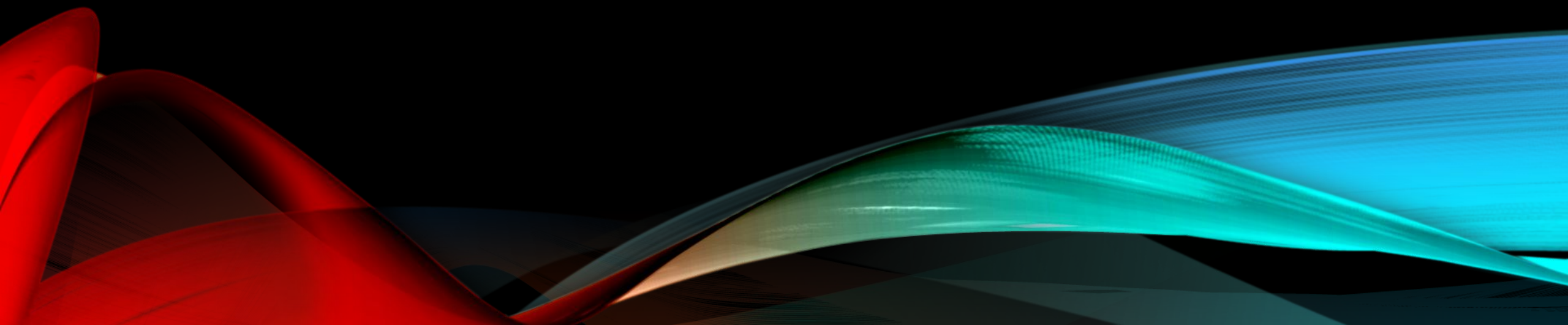
# RISE OF EQUITY BANK

- 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


ME
Thin SIM
SIM
Menu Selection Envelope: 0x05
STK command: Select Item
Menu Selection
Terminal Response: Terminate


ME
Thin SIM
SIM
Menu Selection Envelope: 0x80
STK command: Select Item
Menu Selection : Check Balance
STK command: Get Input (PIN)
Terminal Response: '1234'
SIM contacts the network and gets required information
STK command: display balance
Terminal Response: Terminate

# 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.

# STK APP ATTACK: M-PESA

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





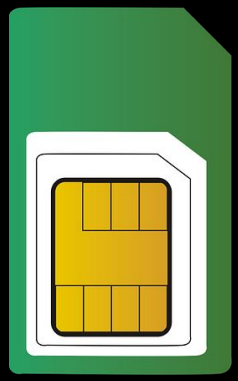

# Phase 1: Get Credentials



Phone



Thin Sim



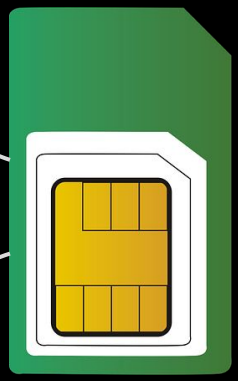
Sim card

# Phase 1: Get Credentials

1. Transparently passes STK commands







Phone

Thin Sim

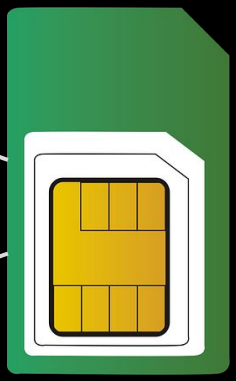
Sim card

# Phase 1: Get Credentials

2. Listen until the sim asks for the user's PIN







"Enter Pin"

"Enter Pin"

Phone

Thin Sim

Sim card

# Phase 1: Get Credentials

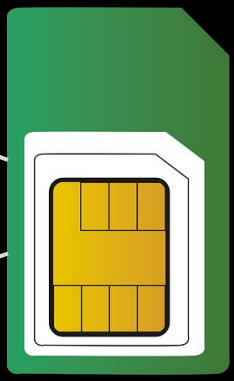
3. Store the response



“1234”



“1234”

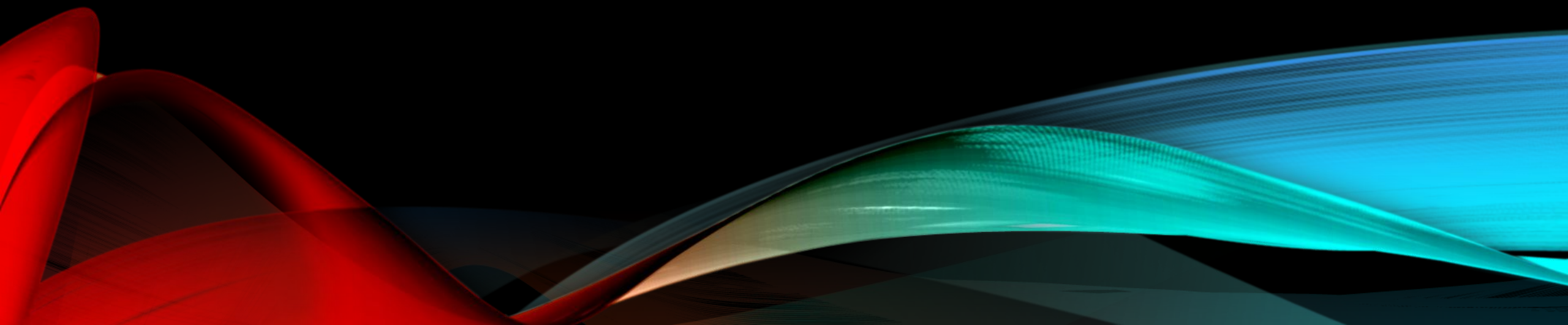


Phone

Thin Sim

Sim card

# STK ATTACK PHASE 1 DEMO



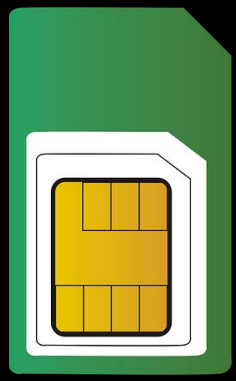
# Phase 2: Make Payments



Phone



Thin Sim



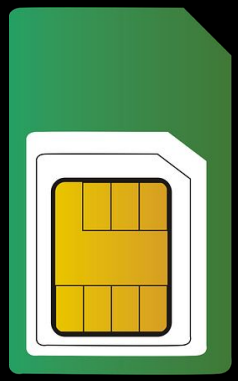
Sim card

# Phase 2: Make Payments



1. Status Update





Phone

Thin Sim

Sim card

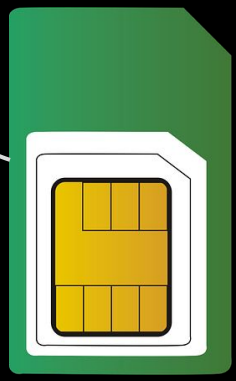
# Phase 2: Make Payments



1. Status Update



2. Spoof Transaction



Phone

Thin Sim

Sim card

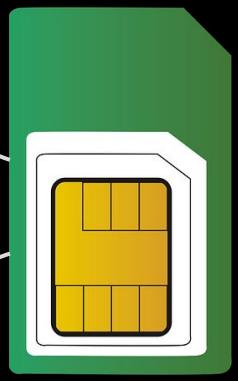
# Phase 2: Make Payments



1. Status Update



2. Spoof Transaction

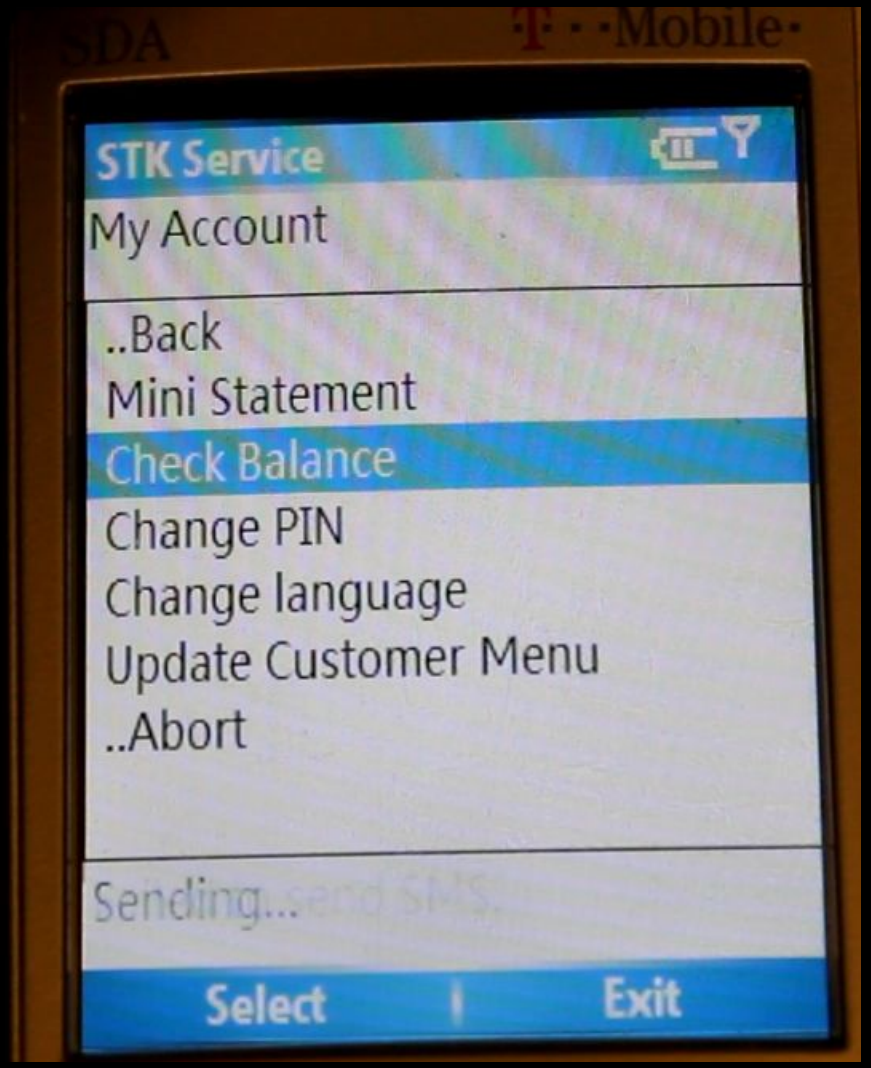


3. SMS Callback

Phone

Thin Sim

Sim card


SDA
T··Mobile·
STK Service
My Account
..Back
Mini Statement
Check Balance
Change PIN
Change language
Update Customer Menu
..Abort
Sending...
Select
Exit

# MESSAGE STRUCTURE

D0 4B 81 03 01 13 00 82 02 81 83 05 0A 53 65 6E 64 69 6E 67 2E 2E 2E 0B 34 01 01 04 81…

0xD0 - Proactive STK command
- 0x4B - length (75 bytes)
- 0x81 - Command details tag
  - 0x03 - length
  - 0x01 - command number
  - 0x13 - Send Short Message
  - 0x00 - RFU
- 0x82 - Device identity tag
  - 0x02 - length
  - 0x81 - src: SIM
  - 0x83 - dst: Network
- 0x05 - Text string tag
  - 0x0A - length (10 bytes)
  - 53 65 6E 64 69 6E 67 2E 2E 2E - "Sending…"
- 0x0B - SMS TPDU tag
  - 0x34 - length (52 bytes)
  - 01 01 04 81… - SMS TPDU

# MESSAGE STRUCTURE

D0 41 81 03 01 13 00 82 02 81 83 05 00 0B 34 01 01 04 81…

0xD0 - Proactive STK command
- 0x41 - length (65 bytes)
- 0x81 - Command details tag
  - 0x03 - length
  - 0x01 - command number
  - 0x13 - Send Short Message
  - 0x00 - RFU
- 0x82 - Device identity tag
  - 0x02 - length
  - 0x81 - src: SIM
  - 0x83 - dst: Network
- 0x05 - Text string tag
  - 0x00 - length (0 bytes)
- 0x0B - SMS TPDU tag
  - 0x34 – length (52 bytes)
  - 01 01 04 81… - SMS TPDU

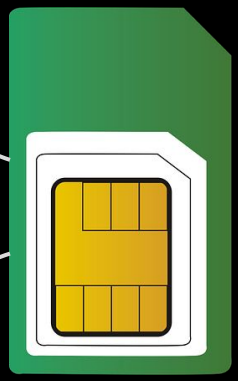
# Phase 2: Make Payments



1. Status Update



2. Spoof Transaction



3. SMS Callback

Phone

Thin Sim

Sim card

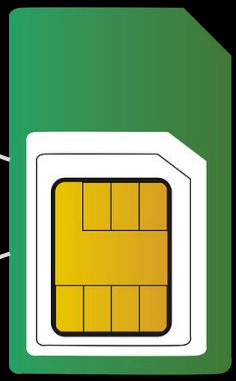
# Phase 2: Make Payments



1. Status Update



2. Spoof Transaction



3. SMS Callback

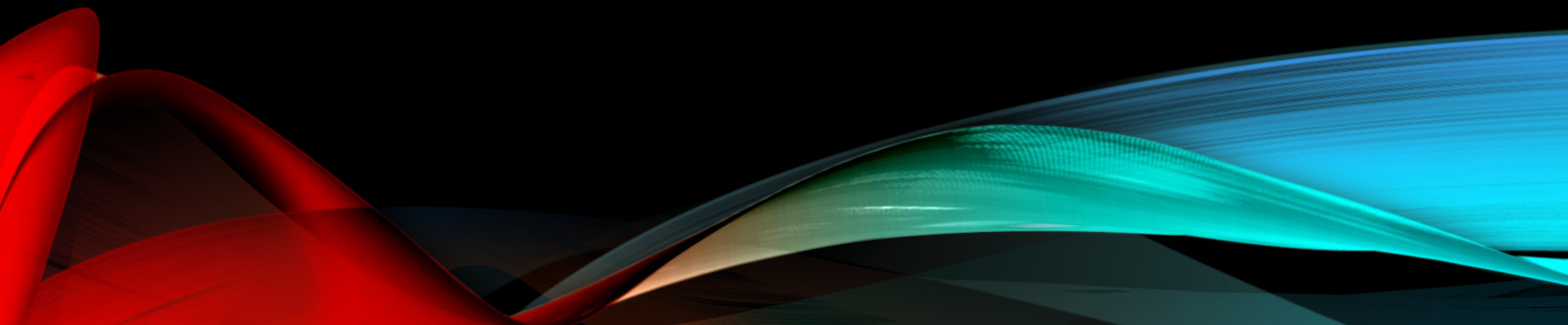
4. Send silent SMS

Phone

Thin Sim

Sim card

# STK ATTACK PHASE 2 DEMO



# THIN SIM CAPABILITIES

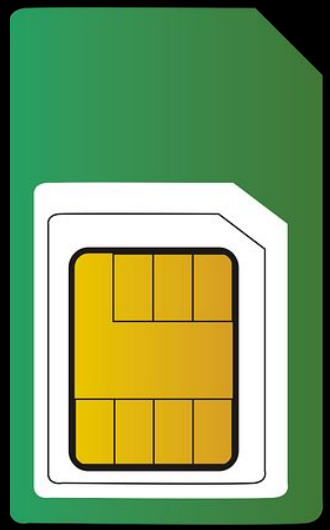
- Intercept, modify and create STK commands
- View responses to STK commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user's knowledge
- Track location updates
- Perform GSM authentication actions
- Read data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

# THIN SIM CAPABILITIES

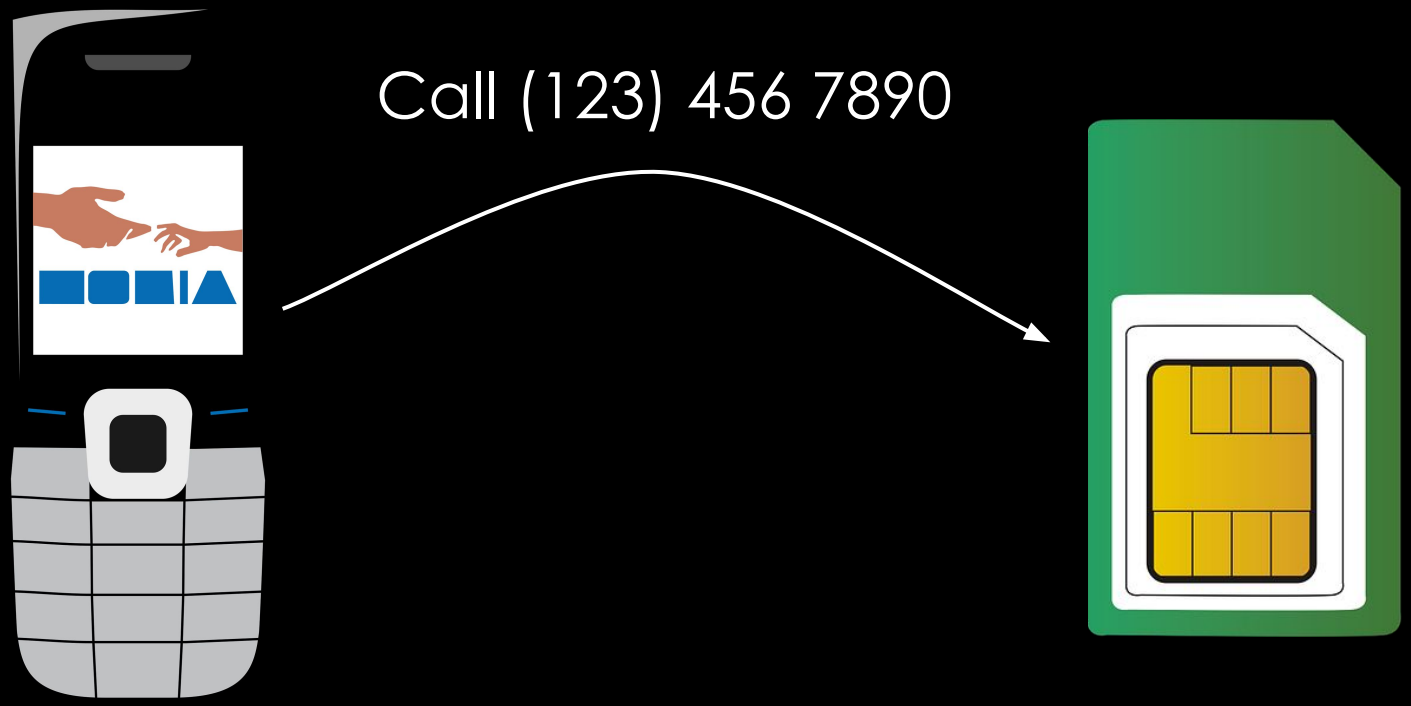
- Intercept, modify and create STK commands
- View responses to STK commands in plain text
- Send SMS with or without notifying the user
- Log and redirect calls (both voice and USSD)
- Make USSD calls without the user's knowledge
- Track location updates
- Perform GSM authentication actions
- Read data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

# CALL CONTROL



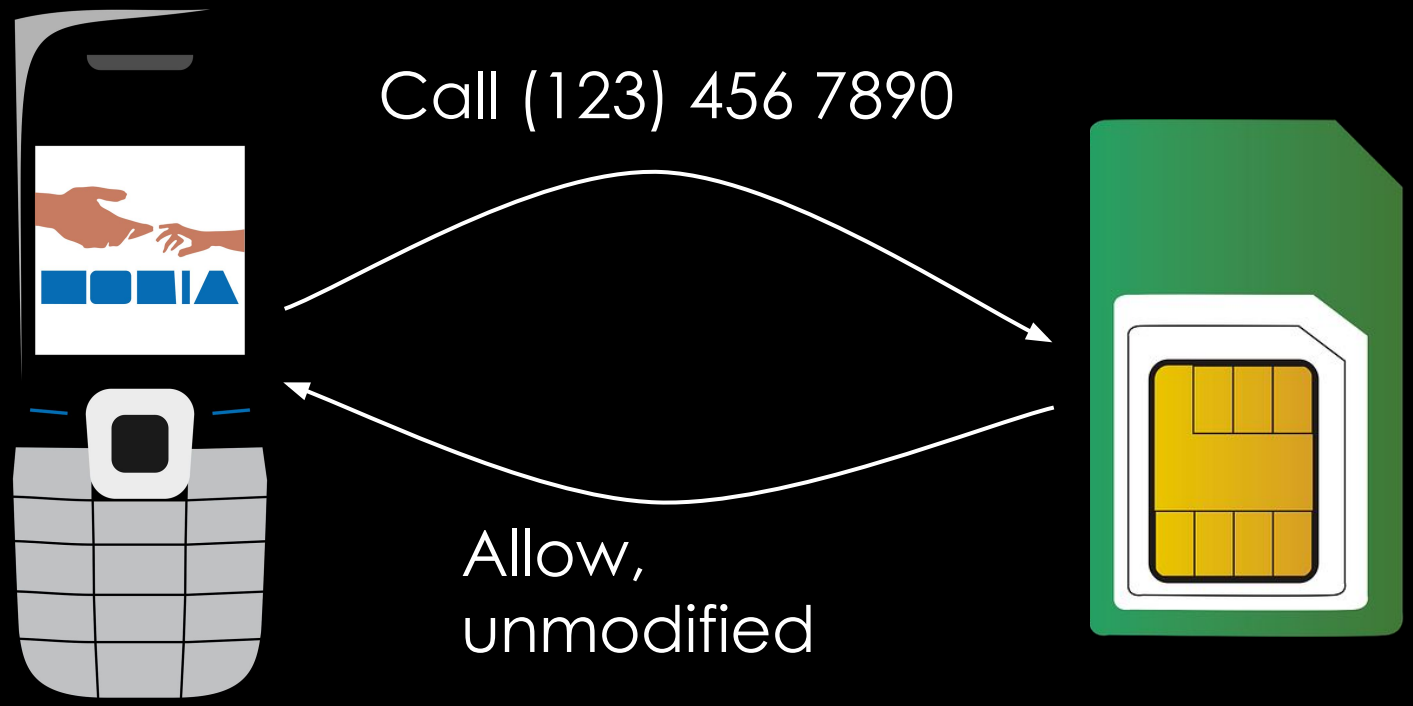


# CALL CONTROL



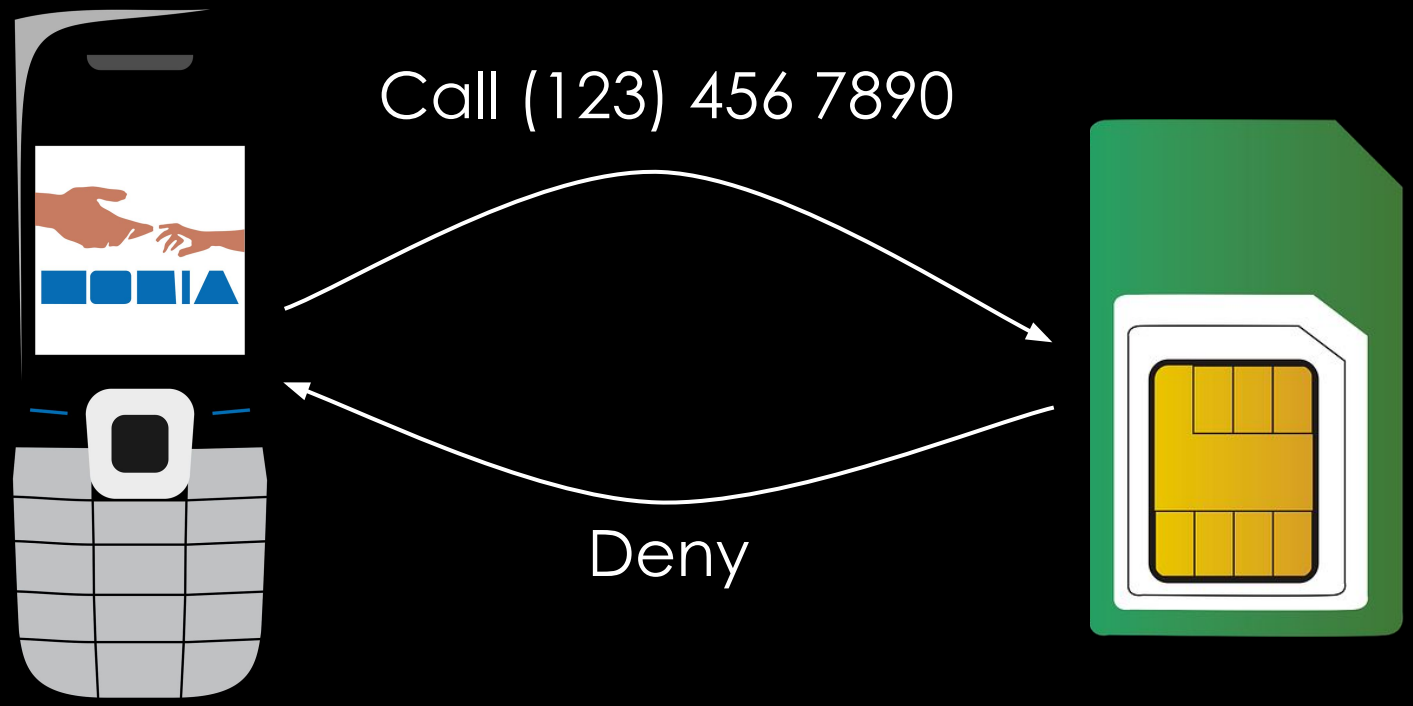

Call Control Mechanism: Allow

# CALL CONTROL



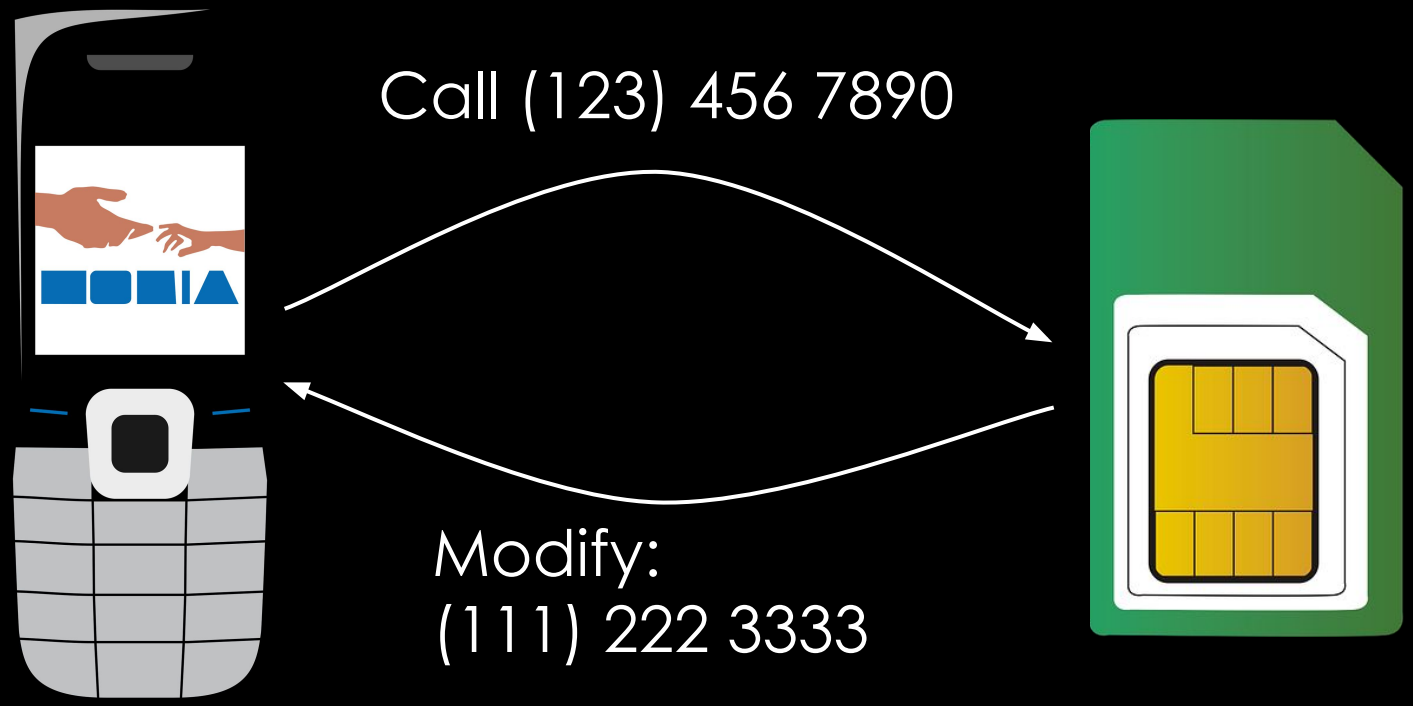

Call Control Mechanism: Allow

# CALL CONTROL



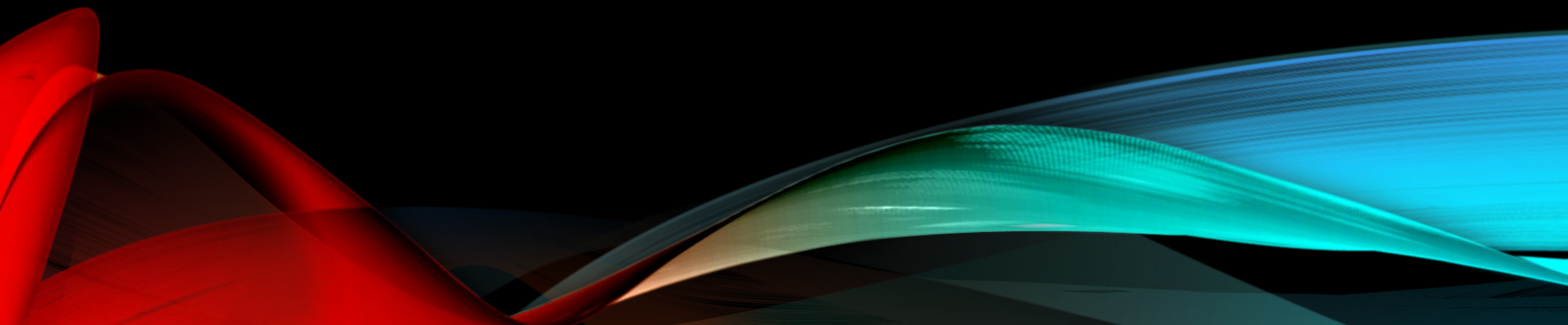

Call Control Mechanism: Allow

# CALL CONTROL




Call Control Mechanism: Allow

# CALL CONTROL SOUNDS HARMLESS ENOUGH RIGHT?



# CALL CONTROL ATTACKS

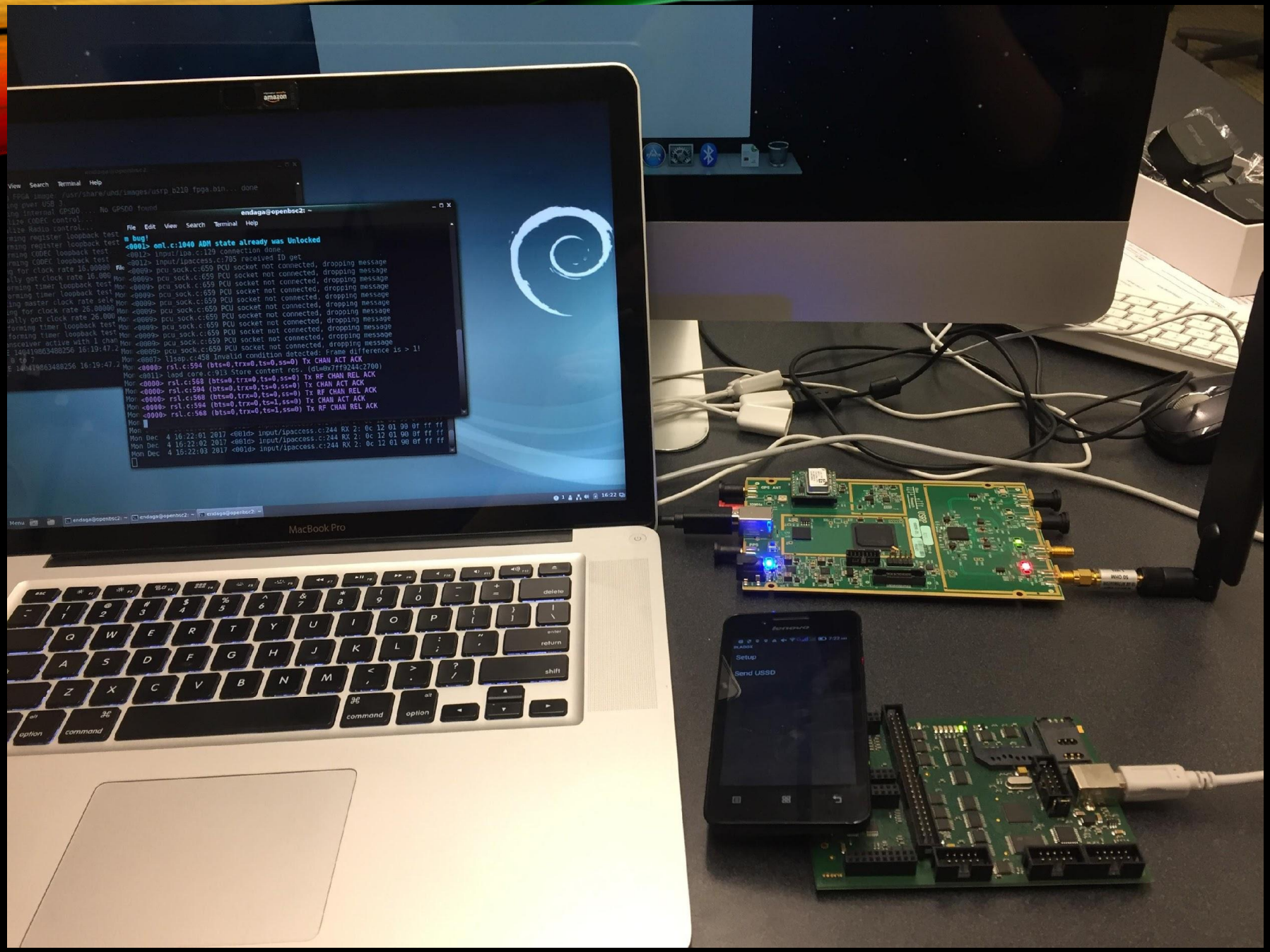
- Call tracking for targeted advertising, surveillance, or blackmail
- Phishing attacks
- Premium rate calls
- Redirect USSD calls

# 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.

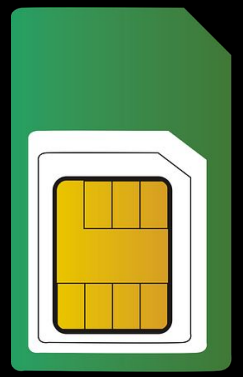

endaga@openbsc2: ~
File Edit View Search Terminal Help
m bug!
<0001> oml.c:1040 ADM state already was Unlocked
<0012> input/ipa.c:128 connection done
<0012> input/ipaccess.c:705 received ID get
<0009> pcu_sock.c:659 PCU socket not connected, dropping message
<0007> l1sap.c:458 Invalid condition detected: Frame difference is > 1!
<0000> rsl.c:594 (bts=0,trx=0,ts=0,ss=0) Tx CHAN ACT ACK
<0011> lapd_core.c:913 Store_content_res.: (dl=0x7ff9244c2700)
<0000> rsl.c:568 (bts=0,trx=0,ts=0,ss=0) Tx RF CHAN REL ACK
<0000> rsl.c:594 (bts=0,trx=0,ts=0,ss=0) Tx CHAN ACT ACK
<0000> rsl.c:568 (bts=0,trx=0,ts=0,ss=0) Tx RF CHAN REL ACK
<0000> rsl.c:594 (bts=0,trx=0,ts=1,ss=0) Tx CHAN ACT ACK
<0000> rsl.c:568 (bts=0,trx=0,ts=1,ss=0) Tx RF CHAN REL ACK
Mon Dec 4 16:22:01 2017 <001d> input/ipaccess.c:244 RX 2: 0c 12 01 90 0f ff ff
Mon Dec 4 16:22:02 2017 <001d> input/ipaccess.c:244 RX 2: 0c 12 01 90 0f ff ff
Mon Dec 4 16:22:03 2017 <001d> input/ipaccess.c:244 RX 2: 0c 12 01 90 0f ff ff
MacBook Pro
Setup
Send USSD



Legitimate USSD Service
*123#

Attacker's USSD Service
*654#





USSD Attack Phase 1

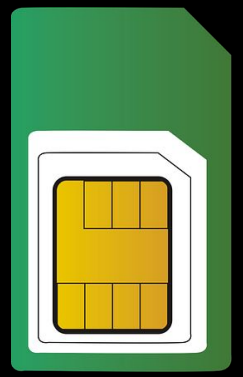
Legitimate USSD Service
*123#

Attacker's USSD Service
*654#



1. Call *123#





USSD Attack Phase 1



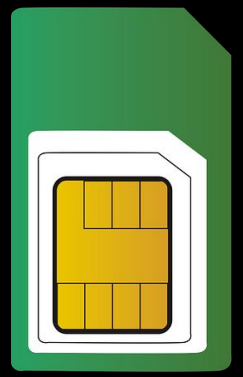
Legitimate USSD Service
*123#

Attacker's USSD Service
*654#

1. Call *123#

2. Redirect to *654#





USSD Attack Phase 1



Legitimate USSD Service
*123#

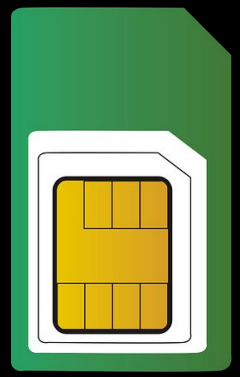
3. Send Payment Details

Attacker's USSD Service
*654#

1. Call *123#

2. Redirect to *654#





USSD Attack Phase 1



Legitimate USSD Service *123#

3. Send Payment Details

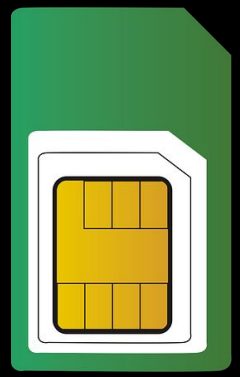
4. Error

Attacker's USSD Service *654#

1. Call *123#

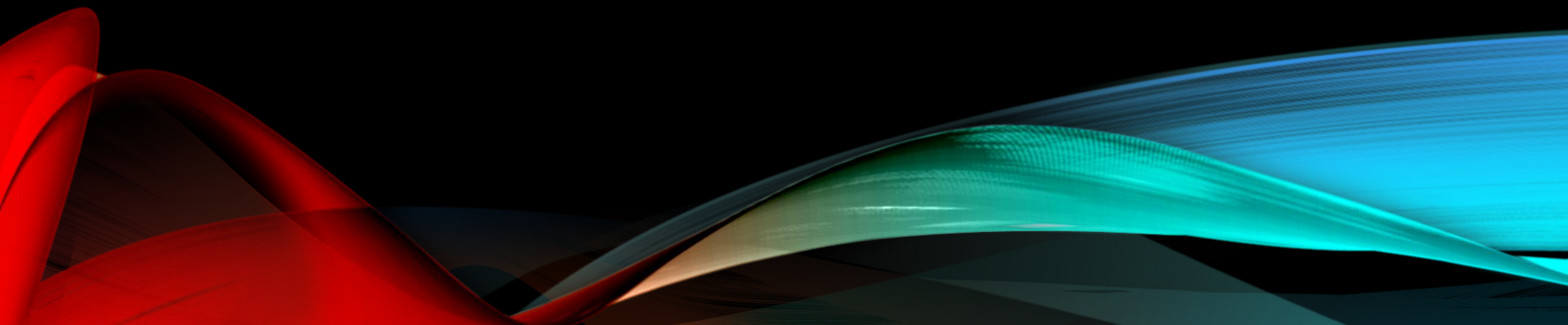
2. Redirect to *654#





USSD Attack Phase 1

# USSD ATTACK PHASE 1 DEMO

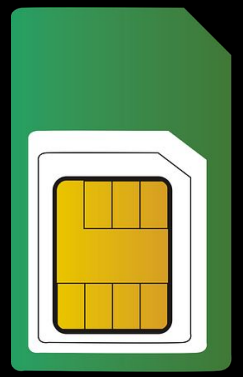




Legitimate USSD Service
*123#

Attacker's USSD Service
*654#





USSD Attack Phase 2

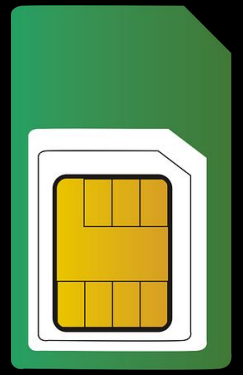


Legitimate USSD Service *123#

Attacker's USSD Service *654#

1. Call *654#





USSD Attack Phase 2



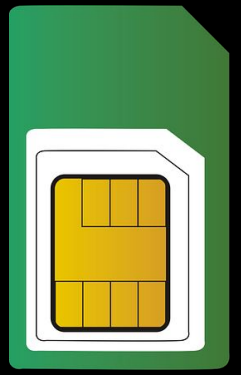
Legitimate USSD Service *123#

Attacker's USSD Service *654#

1. Call *654#

2. Payment details





USSD Attack Phase 2



Legitimate USSD Service *123#

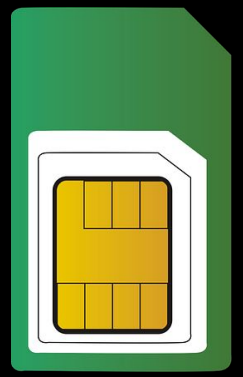
Attacker's USSD Service *654#

1. Call *654#

2. Payment details

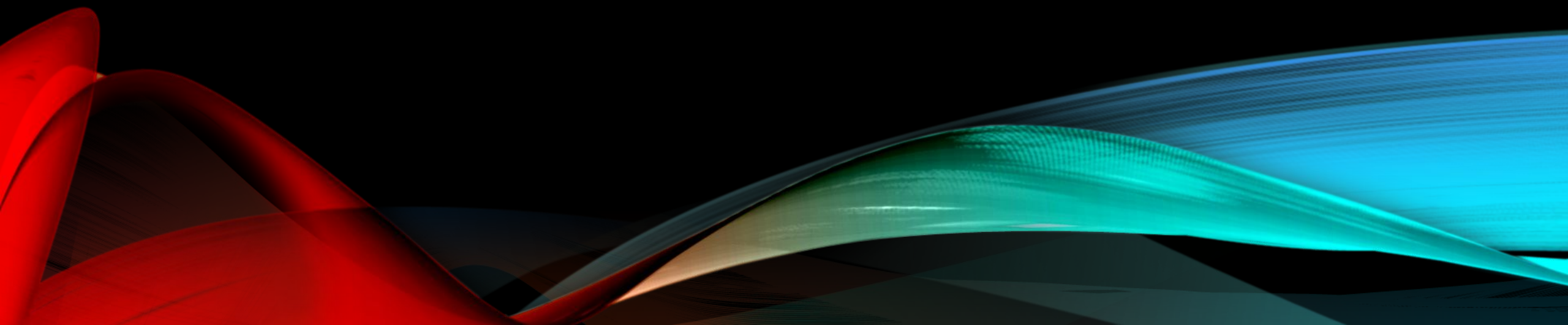
3. Make transaction





USSD Attack Phase 2

# USSD ATTACK PHASE 2 DEMO



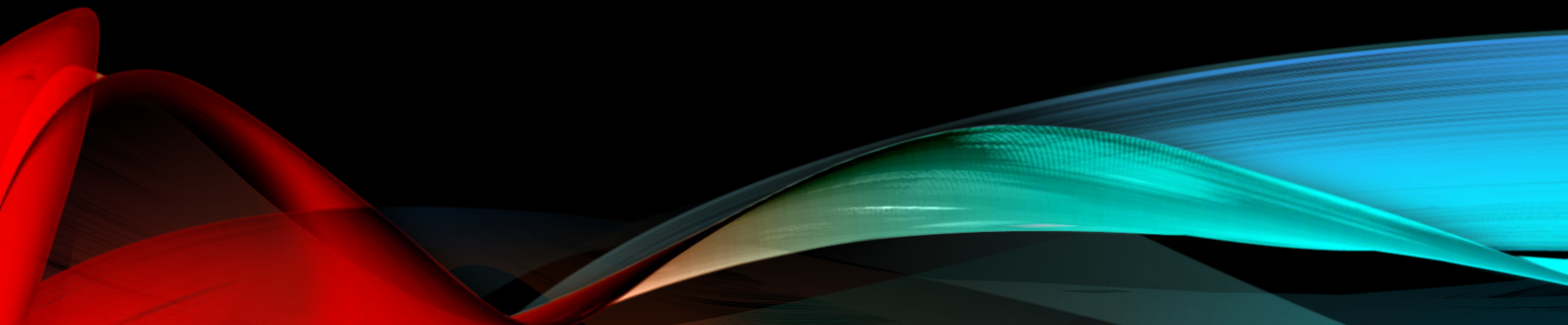
# THIN SIM CAPABILITIES

- 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 SIM cards
- For STK and USSD: Send confirmation code via SMS
- For USSD: require the user to enter in a value shown on the display

# 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 SIM cards
- For STK and USSD: Send confirmation code via SMS
- For USSD: require the user to enter in a value shown on the display
- Encrypt the traffic between the SIM card and the phone

# FURTHER READING

- http://ictd.cs.washington.edu/docs/papers/2018/phipps_compass2018.pdf
- ETSI TS 131 111
- ETSI TS 102 221
- ETSI TS 102 223