Mobile Phone Technology

Lecture 8: CSE 490c
Announcements

• Sign up to demo programming assignment one
Mobile Money Technology

- Financial accounts associated with mobile phone
- Over the counter (OTC) agents are available for Cash In, Cash Out
Sending Money [To a Registered User]

**Step 1**
Select Mobile Money

**Step 2**
Select Send Money to

**Step 3**
Select Mobile User

**Step 4**
Enter Mobile Number

Documentation for MTN Uganda
Sending Money [To a Registered User]...

Step 5
Enter Amount

Step 6
State reason

Step 7
Confirm details
Confirm entry:
Ush 15000 to
0772645131:
Reason: Tspt
OK

Step 8
Enter MM Pin

Currency: Uganda Shilling (Ush)
Sending Money [To a Registered User]…

Step 9

Transaction confirmed

Step 10

Balance confirmation!
Implementation using SMS

• Does SMS work for mobile money?

• Send as a text message:
  • TO: 2065431695 AMT: 1000.00 PIN: 1234

• Multiple issues, some are partially addressable
  • Usability
  • Spoofing
  • Message interception
  • Multiple rounds may be needed for confirmation
USSD Protocol

• Networking: Post cards vs. phone calls
• Session opened between mobile operator and handset
  • Can be opened in either directions
  • Fixed size messages with header and text payload
  • Phone number (short code) can trigger USSD app
• Timeouts on operations
• Session time out
USSD Protocol

1. User dials "+123#<SEND>

2. TCAP Begin
   invoke
   MAP_PROCESS_UNSTRUCTURED_SS_REQUEST

3. User presses 1<SEND>

4. TCAP Continue
   invoke
   MAP_UNSTRUCTURED_SS_REQUEST

5. User presses 1<SEND>

6. TCAP Continue
   invoke
   MAP_UNSTRUCTURED_SS_REQUEST

7. User presses 15.00<SEND>

8. TCAP End
   return result (last)
   MAP_PROCESS_UNSTRUCTURED_SS_REQUEST
Security of Mobile Money

• Connection between handset and tower
• Encrypted transport to MNO Servers
• Secure banking operations
• As secure as the GSM System
Sim Card

- **Smart Card**
  - Integrated Circuit on card form
  - File system, programs, operating system, parameters

- **Sim Card**
  - Smart Card for handset to communicate with base station
  - Power and communication provided by handset
  - Issued by mobile operator
  - Each Sim Card is unique
Sim Card Data

• ICCID, Integrated Circuit Card Identifier
  • Identifier of the SIM card itself
• IMSI, International Mobile Subscriber Identity
  • Identify Subscriber and Network
• Authentication Key \( (K_i) \)
  • Unique, 128 bit key for authentication
  • Secret, not readable
• Location area identity
• SMS Messages and Contacts
Tower validating a phone
Establishing a connection

• Handset (Sim Card) and tower must share a secret to prove identity and allow a connection to be established
  • A session key is then created for secret communication

• Sim Card has the Authentication Key, and Tower can look it up from the subscriber data base

• However the handset can’t send the key, since someone could be listening
Challenge Response Algorithm

- Simcard sends IMSI (subscriber identity)
- Tower looks up secret key, \( K_t \)
- Tower generates random 128 bit number \( X \)
- Tower sends \( X \) to handset
- Tower computes \( F_t = A(K_t, X) \)
- Handset computes \( F_h = A(K_h, X) \)
- Handset sends \( F_h \) to Tower
- If Tower confirms that \( F_h = F_t \), communication is established
Cryptography

- Function $A$ is a non-invertable hash function
  - If you know $x$, you can compute $A(x)$
  - If you know $A(x)$, you can’t figure out $x$
- To the eavesdropper, both $X$ and $F$ look random
- 128 bits is big enough that brute force probably won’t work
- Different ciphers $A$ have been used in the GSM standard
- Many studies have been done on extracting secrets from Sim cards and attempting to clone Sim cards
Mobile Money in a SimCard

• Since the SimCard can have programs, Mobile Money can implemented on the Sim Card

• Similar Menu Based operations to USSD
  - But more flexibility in interface, or response
  - Can implement cryptography for encoding
  - Can use encrypted SMS or USSD as a communications mechanism

• Will generally rely on SMS receipts to acknowledge transaction
Thin Sims
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
Communication between Person and 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
Communication between Person and Thin SIM
Checking mobile money balance
Thin Sims: WHY

- Cell phone unlocking
- Distribution of apps
  - Equity Bank, Mobile Money, Kenya
  - Community Health Worker application, Medic Mobile
- Malicious Installation