Mobile Authentication
Subspace Travel

Markus Vervier

May 28th, 2015
Markus Vervier / @marver

Background in security for over 10 years

Main interests:
- Firmware
- Network Security
- Mobile Networks
- Finding Bugs
- Security Design

Working as Security Researcher and Penetration Tester for LSE Leading Security Experts GmbH
Intro / What it’s all about

Topics of this Talk
Authentication (Birds Eye)

May we Borrow your Identity for a While?

SIM Access
Baseband
Adding Features
Goodie
Conclusion

Mobile Authentication Subspace Travel
Mobile Authentication Subspace Travel

Topics of this Talk

- Authentication in mobile networks
- How millions of devices are exposing SIM-Cards
- How to have fun with baseband firmware
- Using this to forward mobile network authentication
- SIM-Card authenticates a user / his contract
- Provider AuC and SIM-Card share a secret key $K_i$
- Challenge-Response Network-Authentication between Mobile-Equipment (ME) and Network
- Users have no access to $K_i$

$^1$Source: UMTS Security, Valtteri, Niemi and Kaisa Nyberg
May we Borrow your Identity for a While?

A Misconception

SIM Access
Baseband
Adding Features
Goodie
Conclusion

May we Borrow your Identity for a While?
A Misconception

Naive Idea: Authentication is secured by having a "secure" SIM device that does it
Naive Idea: Authentication is secured by having a "secure" SIM device that does it.
Naive Idea: Authentication is secured by having a "secure" SIM device that does it

Temporary Authentication tokens are derived from the secret key $K_i$ on the SIM

Then they leave the SIM!

They are valid on their own for a time!
whoami

Intro / What it’s all about
May we Borrow your Identity for a While?

SIM Access
SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM
SIM-Card-Access Demo
Command-APDU
Response-APDU
Enter AT+EAUTH
SIM-Card-Access via BT-SAP
Dial Up Networking
USB Modem Demo
A Blackhat Telco Operator
A Blackhat Telco Operator
Baseband

SIM Access
Baseband manages the SIM-Card
- Sends command APDUs to the SIM-Card and processes responses
- Passes stuff like SMS, SIM- Tookit, etc. to the AP
No direct access to SIM by AP

But there are indirect methods:

- AT-Command-Interfaces accessible via Bluetooth / USB
- Vendor specific: Internal Android RIL calls
SIM-Card-Access via AT+CSIM

Command Syntax:
AT+CSIM=<length>,<command>

Response Syntax:
+CSIM:<length>,<response>

Nobody listened to security advice from 3GPP 27.007: “Care must be exercised in AT commands that allow the TE to take unintentionally control over the SIM-MT interface (e.g. +CSIM);”
Unprivileged Apps can Talk to the SIM

- Should have no SIM access without privileges
- AT-Command-Prompt found on /dev/pts/XX on MTK-Devices
- Bug: Permissions 0777 on older Alcatel Android devices!
- Unprivileged apps can query the SIM-Card via AT+CSIM
- Also other methods for SIM-Access at other vendors (Samsung Galaxy S2 / S3)
whoami

Intro / What it’s all about

May we Borrow your Identity for a While?

SIM Access

SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM

SIM-Card-Access Demo

Command-APDU
Response-APDU
Enter
AT+EAUTH
SIM-Card-Access via BT-SAP
Dial Up Networking
USB Modem Demo
A Blackhat Telco Operator
A Blackhat Telco Operator

Mobile Authentication Subspace Travel
Command-APDU

whoami

Intro / What it's all about

May we Borrow your Identity for a While?

SIM Access

SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM
SIM-Card-Access Demo

Command-APDU

Response-APDU
Enter
AT+EAUTH
SIM-Card-Access via BT-SAP
Dial Up Networking
USB Modem Demo
A Blackhat Telco Operator
A Blackhat Telco Operator
Baseband

AT+CSIM=46,"00|88|00|80|11|FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"

CLA (Class)
P1 (Algorithm)
Lc (Length of Payload)

INS (Command)
P2 (Key Reference)
RAND

Mobile Authentication Subspace Travel
whoami

Intro / What it's all about

May we Borrow your Identity for a While?

SIM Access
SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM
SIM-Card-Access Demo
Command-APDU

Response-APDU
Enter
AT+EAUTH
SIM-Card-Access via BT-SAP
Dial Up Networking
USB Modem Demo
A Blackhat Telco Operator
A Blackhat Telco Operator

Baseband

+CSIM: 32, "04799AFC|13083F18786C33995BB8|9000"

SRES

APDU Result Code

Kc
Enter `AT+EAUTH`

- **Problem:** AT+CSIM does not work on recent devices
- **Solution:** Vendors added new commands to help
- **Dedicated commands for authentication:** `AT+EAUTH` and `AT+ESIMAUTH`
- **Used for EAP-SIM / EAP-AKA** e.g., to authenticate to a WiFi using a SIM
- **Also used to retrieve authentication to connect to a mobile network**
whoami

Intro / What it's all about

May we Borrow your Identity for a While?

SIM Access

SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM
SIM-Card-Access Demo
Command-APDU
Response-APDU
Enter AT+EAUTH

SIM-Card-Access via BT-SAP

- Purpose: Interoperability Car↔Phone
- Solution: Sim Access Profile
- Allows remote SIM usage via Bluetooth
- Specified in Bluetooth DOC: SAP_SPEC
- Great! A Specified way to leak your network authentication!
Dial Up Networking

- USB or Bluetooth
- Works via AT-Commands
- Exposes a serial device
- Present on millions of older mobile phones
- Often exposed without user notification and interaction
- What could possibly go wrong?
Dial Up Networking

- USB or Bluetooth
- Works via AT-Commands
- Exposes a serial device
- Present on millions of older mobile phones
- Often exposed without user notification and interaction
- What could possibly go wrong?
Dial Up Networking

- USB or Bluetooth
- Works via AT-Commands
- Exposes a serial device
- Present on millions of older mobile phones
- Often exposed without user notification and interaction
- What could possibly go wrong?
May we Borrow your Identity for a While?

**Intro / What it’s all about**

- **SIM Access**
  - SIM-Usage
  - Retrieving Authentication
  - SIM-Card-Access via AT+CSIM
  - Unprivileged Apps can Talk to the SIM
  - SIM-Card-Access Demo
  - Command-APDU
  - Response-APDU
  - Enter AT+EAUTH
  - SIM-Card-Access via BT-SAP
  - Dial Up Networking
  - USB Modem Demo

**A Blackhat Telco Operator**

- Baseband

![Image](image)

- How many systems in the world are part of botnets?
May we Borrow your Identity for a While?

SIM Access
- SIM-Usage
- Retrieving Authentication
- SIM-Card-Access via AT+CSIM
- Unprivileged Apps can Talk to the SIM
- SIM-Card-Access Demo
- Command-APDU
- Response-APDU
- Enter AT+EAUTH
- SIM-Card-Access via BT-SAP
- Dial Up Networking
- USB Modem Demo

A Blackhat Telco Operator

- How many systems in the world are part of botnets?
- Over 9000 for sure!
How many mobile phones are connected regularly to these systems via USB?
A Blackhat Telco Operator

whoami

Intro / What it’s all about

May we Borrow your Identity for a While?

SIM Access

SIM-Usage
Retrieving Authentication
SIM-Card-Access via AT+CSIM
Unprivileged Apps can Talk to the SIM
SIM-Card-Access Demo
Command-APDU
Response-APDU
Enter
AT+EAUTH
SIM-Card-Access via BT-SAP
Dial Up Networking
USB Modem Demo
A Blackhat Telco Operator

How many mobile phones are connected regularly to these systems via USB?

A lot!
May we Borrow your Identity for a While?

SIM Access
- SIM-Usage
- Retrieving Authentication
- SIM-Card-Access via AT+CSIM
- Unprivileged Apps can Talk to the SIM
- SIM-Card-Access Demo
- Command-APDU
- Response-APDU
- Enter
- AT+EAUTH
- SIM-Card-Access via BT-SAP
- Dial Up Networking
- USB Modem Demo
- A Blackhat Telco Operator

A Blackhat Telco Operator

How many mobile phones are connected regularly to these systems via USB?

A lot!

Attacker-Goal: Authenticate to a mobile network using stolen credentials

As seen above: a lot of mobile phones expose their SIM cards

A big pool of vulnerable devices available for malicious purposes!
Baseband

Mobile Authentication Subspace Travel

HITBSecConf2015 - Amsterdam – 22
Acquire valid authentication vectors from a remote SIM
What to do with it?
We can forward authentication to a custom mobile device
Boring - everyone wants off the shelf phones!
So let’s take a stock baseband firmware and modify it!
Mobile Authentication Subspace Travel

Baseband Overview

- Takes care of communication with the mobile network
- Has direct access to the SIM-Card
- Usually proprietary
- Runs on (somewhat) separate CPU
Only a few significant vendors: Qualcomm, MediaTek, Spreadtrum, Marvell and Intel

Focus here: MediaTek Platforms

Other BaseBand vendors are more locked down today

A lot of previous work regarding Qualcomm
MTK Baseband based on Nucleus RTOS
- Loaded at boot-time by the Android-System running on the AP from “/etc/firmware/modem*.img”
- MTK-Linux-Kernel-Module takes care of it
- Firmware on many MTK-Based-Phones not signed
- Logical separation between Baseband/Modem (BP) and Application-Processor (AP)
- Communication between AP and BP: Shared RAM, UART
AP and BP are *logically* separated but they have a lot of intersections
- On the AP side exposed as char devices or via kernel (ioctl).
- Modem-RMMI: AT-Commands
- Debug-Output
- Firmware-Control via AP (Reset, Exception Handling, etc.)
CCCI (Cross Core Communication Interface): Handles data exchange between AP and BP

- Exposed as different kernel drivers on the AP side
- Character devices (/dev/ccc*)
- Low-Level (CPU to CPU Interface called CCIF according to MTK-Docs) for MT6582:
  - 16 Physical channels (8 AP→MD, 8 MD→AP)
  - One 256bytes dual port SRAM
Uncompressed raw binary
- Partial image of the memory space starting at address 0x00000000
- No virtual memory
- Contains a trailer at the end
whoami

Intro / What it’s all about

May we Borrow your Identity for a While?

SIM Access

Baseband

What about it?
Baseband Overview
Baseband Hardware
Baseband Firmware
Interfaces between AP and BP

CCCI / CCIF

Baseband Firmware - Structure

Baseband Firmware - DEMO

Adding Features

Goodie

Conclusion

Mobile Authentication Subspace Travel

HITBSecConf2015 - Amsterdam – 30
Adding Features

Remote SIM
Remote SIM Concept
ShadowSIM
ShadowSIM - Concept
ShadowSIM - Baseband Communication
ShadowSIM - Firmware Modification
ShadowSIM - DEMO
Wait a Minute

Goodie

Conclusion
Goal: Transfer SIM commands to a remote mobile phone – but how?
Remote SIM

- Goal: Transfer SIM commands to a remote mobile phone – but how?
- Modern phones have additional communication channels besides the mobile network
  - Bluetooth
  - Dual-SIM
  - Data Connection of a second SIM
  - WiFi
Goal: Transfer SIM commands to a remote mobile phone – but how?

Modern phones have additional communication channels besides the mobile network

- Bluetooth
- Dual-SIM
- Data Connection of a second SIM
- WiFi

BT-SAP (Sim-Application-Protocol) - works only for short distances

SIM commands can travel through unintended channels i.e. over TCP/IP
Remote SIM Concept

whoami

Intro / What it's all about

May we Borrow your Identity for a While?

SIM Access

Baseband

Adding Features

Remote SIM

Remote SIM Concept

ShadowSIM

ShadowSIM - Concept

ShadowSIM - Baseband

Communication

ShadowSIM - Firmware

Modification

ShadowSIM - DEMO

Wait a Minute

Goodie

Conclusion
- Allows usage of remote SIM-Cards
- Download from:
  https://github.com/shadowsim/shadowsim
Allows usage of remote SIM-Cards

Download from:
https://github.com/shadowsim/shadowsim

Implements a virtual SIM-Card by patching the Baseband-Firmware of a Mediatek 6573 phone:

1. Identify the code that enables SIM-Access
2. Change it to send APDUs to the AP and read Response-APDUs
Allows usage of remote SIM-Cards

Download from:
https://github.com/shadowsim/shadowsim

Implements a virtual SIM-Card by patching the Baseband-Firmware of a Mediatek 6573 phone:
1. Identify the code that enables SIM-Access
2. Change it to send APDUs to the AP and read Response-APDUs

Implement a native Android-Application that processes APDU-Commands:
1. Read a Command-APDU sent by the Baseband
2. Send them over TCP to a remote system having SIM-Access
3. Write the Response-APDU back to Baseband
ShadowSIM - Concept

whoami
Intro / What it's all about
May we Borrow your Identity for a While?
SIM Access
Baseband
Adding Features
Remote SIM
Remote SIM Concept
ShadowSIM
ShadowSIM - Concept
ShadowSIM - Baseband
Communication
ShadowSIM - Firmware Modification
ShadowSIM - DEMO
Wait a Minute
Goodie
Conclusion

Mobile Authentication Subspace Travel

1. Execute Command-APDU
2. Send Command-APDU + GET RESPONSE
3. Send Response-APDU + Response-Code
4. Transfer Response-APDU

SIMServer
TCP
Android Process (Native)
Shared Mem
Baseband

HITBSecConf2015 - Amsterdam – 35
First idea: Use one of the UARTs as a communication channel to AP

Was a bad idea: UART communication is done asynchronous in Baseband, so lots of work writing and registering your own handler

Easier: Using shared memory

Vendor application for debugging: mdlogger already uses shared memory for log transfer

Source code is published, so changing it for our purpose was easy
Things that help:
- Lots of assertions and debugging strings in the code
- MediaTek firmware for various devices sometimes has Debug-Symbols
- MediaTek reuses code a lot (made it easier to compare different firmwares)
- No obfuscation

In general the code is quite well structured and functionality is abstract - this makes patching easier
Mobile Authentication Subspace Travel
I'M NOT FINISHED WITH YOU YET.
Goodie

May we Borrow your Identity for a While?

SIM Access

Baseband

Adding Features

Goodie

Hardening

SIM Application Toolkit (STK / SAP)

Patching - DEMO

Conclusion
What else can we patch?

Objective: Have a more secure baseband firmware.
Best way: Create a new one from scratch.
In the meantime: Patch existing ones.
Always an improvement for security: Reducing the attack surface
So let’s turn off stuff!
Can work outside of user control
"value added services"
OTA commands sent to / via your SIM
Used for attacks and surveillance
Probably unwanted in "hostile" environments
Conclusion
■ Credentials can be acquired from a SIM card
■ On many devices even over USB
■ Dual-Use:
  ◆ Bad: Bad guys may steal your network identity
  ◆ Good: New applications that free users from SIM cards, allow them to share SIM cards

■ Non-Repudiation is gone for good – a SIM-Card in a mobile phone proves nothing
■ When your security model is from the 80s chances are high it doesn’t work anymore
■ If YOU have ideas on what features to add / remove in a baseband firmware, contact me!
THANK YOU

I'M OUTTA BULLET POINTS...

ANY QUESTIONS?