mobile security

EECE 571B “Computer Security”

Konstantin Beznosov

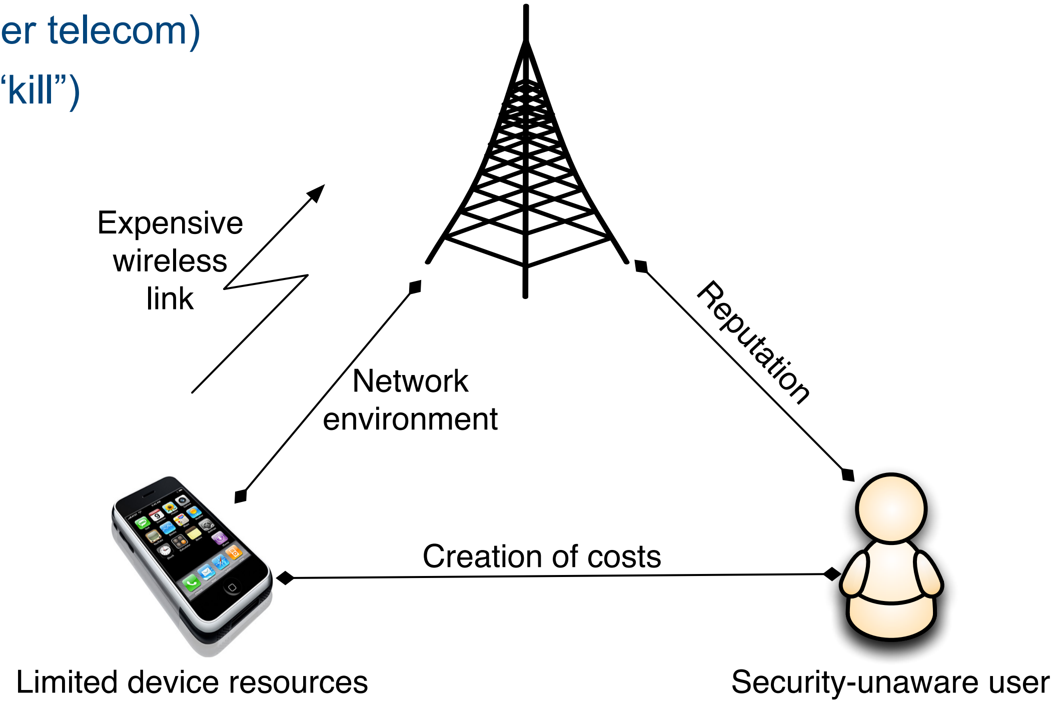
what’s mobile (smart)phone?

- mobile phone
  - any mobile device that contains a smartcard that is controlled by a mobile network operator (MNO)
- smartphone
  - contains an MNO smartcard with a connection to a mobile network, and
  - has an operating system that can be extended with third- party software.

specifics of mobile security

- In what sense is research on the security of mobile devices different from common security research?

1. creation of cost
   - billed events (e.g., premium services)
   - payment systems involving mobile phones (SMS, NFC)
2. network environment
   - strong connection (MNO and its influence/control of the device)
   - firmware update (critical and expensive over telecom)
   - remote device management (also remote “kill”)
3. Limited device resources
   - compared to desktops
   - CPU & memory
     - e.g., ID algorithms
   - battery
4. expensive wireless link
   - in distributed computations
5. reputation of the MNO



adopted from [1]

threats

- eavesdropping
- DOS
- device tracking
- device impersonation

attack vectors

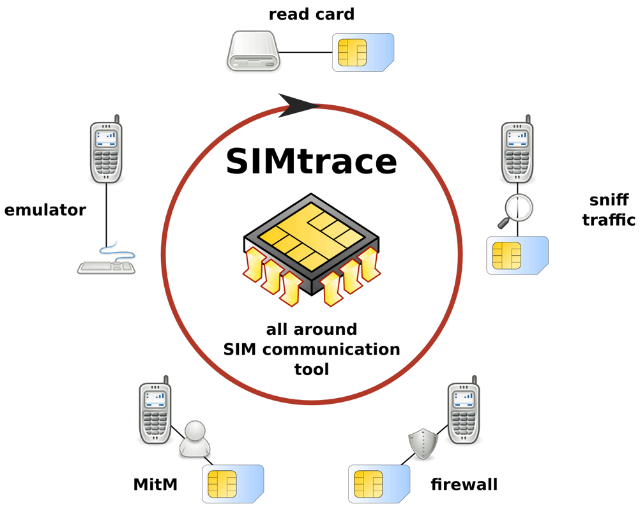
- hardware-centric
- device-independent
- software-centric
- user layer

hardware-centric attacks

- intercepting MNO smartcard communication
  - removing the SIM lock of the iPhone
  - MITM attacks
- attacking the device
  - attacks via debugging functionality
    - Joint Test Action Group (JTAG)
- confidentiality attack with forensic analysis
  - borrowed device
  - owned device (buying, stilling, finding)

osmocomSIMTRACE

http://simtrace.osmocom.org

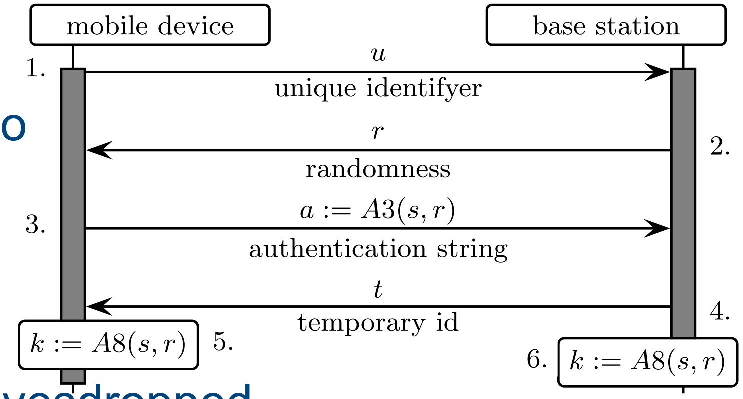


monitor, analyze and use the power of SIM

device-independent attacks (1/3)

1. attacks on GSM protocol

- developed 25 years ago -- immature asymmetric crypto
- encode for transmission + encrypt
- A5/2 was weakened for use in non-Western countries
  - session key *k* can be derived by breaking A5/2
    - all conversation (with any encryption) can be eavesdropped
- no network authentication
  - *k* for previously recorded conversations can be derived with rogue base station



mobile device

base station

1. u unique identifyer

2. r randomness

3. $a := A3(s, r)$ authentication string

4. t temporary id

5. $k := A8(s, r)$

6. $k := A8(s, r)$

adopted from [1]

2. SMS infrastructure (circuit-switched GSM) flaws

- DOS on voice service in large cities by web-SMS interface
- paging channel can overload the network
- RQ: how can the SMS infrastructures robustness be improved?

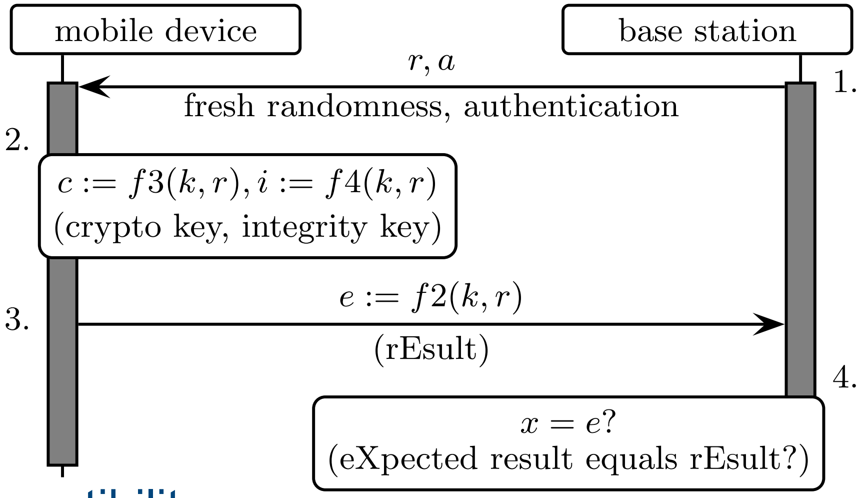
3. MMS infrastructure (packet-switched GPRS) flaws

- batteries drained 22 faster in ready mode
- regular UDP packets keep phone in ready mode
- use rogue MMS relay/server (targeted) or operator’s IP address ranges (opportunistic)

device-independent attacks (2/3)

Universal Mobile Telecommunications System (UMTS)

- fixes
  - encryption and encoding in correct order
  - encryption algorithm updated to KASUMI (improved parameter choices)
  - all communication over the air link has been encrypted within the network
  - network is authenticated to the mobile
  - the mobile can verify randomness freshness


mobile device
base station
1.
r, a
fresh randomness, authentication
2.
$c := f3(k, r), i := f4(k, r)$
(crypto key, integrity key)
3.
$e := f2(k, r)$
(rEsult)
4.
$x = e?$
(eXpected result equals rEsult?)

adopted from [1]

- yet
  - mobile unique ID is sent in clear
  - roll-back attack possible due to backward compatibility
  - new vulnerabilities
    - well-timed low volume DoS on signalling/control plane
    - jamming of Presence Service causes a chain reaction that blocks all IMS services

device-independent attacks (3/3)

5.side channels

- examples: cache hits or misses, memory access, power consumption, etc.
- extracting key material
- side channel attacks on SIM cards (through hardware or software)

6. back end systems

- Hiptop/Sidekick mirrors data on MNO for web access
  - password protected
  - social engineering attack to gain access to MNO internal system
  - prominent names -> phone numbers
  - web app vulnerability to reset account password on mirrored data
- Home Location Register (details of each subscriber)
  - (75%-93%) DoS via brining HLR down
- other: on GPRS and on MMS infrastructure

software-centric attacks: malware

Cabir propagated automatically on Symbian OS in 2004

adversary objectives

- information or identity theft, espionage
  - collect and forward information to the attacker
- eavesdropping
  - capture voice calls & record conversations via the microphone
- make the user to pay
  - use of (voice or SMS) premium services
  - blackmailing (“ransomware”)

- mobile botnets
  - DDoS attack on 911 call-centers
- DoS attacks on mobile devices
  - corruption of essential data in difficult to reach locations (E^{2}PROM)

software-centric attacks: messages and browsing

- SMS vulnerabilities
  - SMS parser in Siemens S55 (Chinese characters, local firmware update)
  - omitted sanity check of input -> DoS on Nokia phones
- MMS vulnerabilities
  - remote code execution exploit in MMS handling of Windows Mobile CE 4.2
- mobile web browser
  - must support making voice calls and video calls
  - application framework in itself
    - DoS attacks on mobile IE
    - jailbreak of the iPone
    - hacking Android browser
    - using iPhone browser as a dialer

countering mobile malware

- detection
  - signature-based
    - burden on the CPU
    - offload scanning to the cloud
  - static function call analysis
    - at the installation time
    - Android and Symbian
  - App Store model
  - anomaly detection
    - SmartSiren: central proxy analyzes Bluetoooth and SMS communications
    - external VM (replica of the phone) replays instructions
    - detection through battery power consumption analysis
    - changing user behaviour challenges
  - rootkit detection
    - first rootkit on Android (Defcon 2010)
- sofwatre-based attestation
  - memory printing for retroactively detecting active software

protecting mobile OS

- limited privileges and process isolation
  - PLP
  - Android approach: UIDs and JVMs
  - no hardware support for virtualization
- hardened kernels (porting from desktop OS)
  - address space layout randomization
  - stack protection
  - non-executable writable memory
  - MAC lists
- sound default settings
  - e.g., bluetooth by default?
  - some Symbian smartphones prone to DoS in default configuration
- better update procedures
- software attestation for 3rd party apps
  - Kirin, SAINT, SCanDroid, TaintDroid, PiOS

user interface and attacks

- limitations due to size
  - indicators
  - URL bar disappearing
  - malware performing security actions on user’s behalf
  - CAPTCHAs
- usable security
  - limited pixels and real estate
  - diversity of the user population

expected relevant trends

- payment services and cost creation
- remote device management and update
- costs of communications and computations will decrease
- more processing power and memory, but battery
- security awareness of users?
- heterogeneity?

credits

1. Becher, M., Freiling, F.C., Hoffmann, J.; Holz, T., Uellenbeck, S., Wolf, C. "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Security and Privacy (SP), 2011 IEEE Symposium on, pp.96-111, 22-25 May 2011.