Telecom Security - lessons learned (or not)?

Personal review on the last 7 years

Harald Welte

hardwear.io 2015 Keynote

About

- Linux Kernel / bootloader / driver / firmware developer since 1999
- Former core developer of Linux packet filter netfilter/iptables
- Comms / Network Security beyond TCP/IP
    - OpenPCD, librfid, libmtrd, OpenBeacon
    - deDECTed.org project
    - Openmoko - FOSS smartphone with focus on security + owner device control
    - OpenBSC as network-side FOSS GSM Stack
    - OsmocomBB - device-side GSM protocol stack + baseband firmware
- practical security research / testing on baseband side and telecom infrastructure side
- running a small team at sysmocom GmbH in Berlin, building custom tailored mobile communications technology

Disclaimer

- This presentation is not intended to insult any participant
- No companies or individuals will be named
- However, the collective failure of the mobile industry cannot be ignored, sorry.
- Many of the issues we have today could have been avoided extremely easily, there really is no excuse...

Terminology / Perspective

- Many people speak about *hardware security* but mean *embedded systems security*
- Embedded systems today (Android, etc.) are more complex than PCs 10 years ago, so that's not primarily hardware security but classic software security
- Actual hardware security (tamper protection, avoiding information leakage via side-channels, preventing glitching, ...) is a very narrow topic, too
- There's a lot of deeply-embedded firmware in between, what I consider the area in biggest need of attention.

Mobile / Telecom Security

Main areas:

- Phone-side baseband security
- Air interface security
- Radio Access Network Security
- Back-haul network security
- Core network security
- Interconnect security

Phone-side baseband security

- Since 2009, there are accessible tools to run your own GSM/GPRS network to attack phones (OsmoBTS, OpenBSC, OsmoSGSN, etc.)
- baseband exploiting via malformed air interface messages has been shown multiple times during the last 5 years (Ralf-Philipp Weinmann, others)
- some stack/chip vendors started large-scale security code audits, but by far not the entire industry
- Still 100% closed/proprietary environment with very limited amount of research/attacks
- Summary: Some improvement, but a long way to go

Air interface security

- Some operators have rolled out A5/3 encryption
- Spec is broken and permits semi-active down-grade attacks
- Industry took 7 years from A5/3 specification to first interop test -> fail.
- Summary: Nice try, but way too late and way too little

Radio Access Network Security

- Still no standard practise to do penetration testing on BTS, NodeB, eNodeB
- Equipment makers putting pressure on operator to cancel already scheduled penetration tests!
- Sometimes there are very basic / superficial tests as part of a tender
- No single known/documented/public case where an operator or a equipment maker consistently pen-tested all of their equipment
- Summary: No visible change from 7 years ago

Core Network Security

- See Radio Access Network Security
- Occasional pen-testing is performed and reveals horrible implementation bugs in affected equipment (MSC/VLR/HLR/SGSN)
- Summary: No visible change from 7 years ago

As all core network elements are software implementatiosn these days, this is 100% a software security topic!

Interconnect Security

- Still no standard practise to have packet filter / firewall / IDS / IPS like functionality for SS7/SIGTRAN interfaces
- I don’t know of any operator who has any idea about what actually is happening on their roaming interfaces
- No matter how many clearly suspicious/malicious messages you get from a roaming/interconnect partner, it triggers no alarm
- Only fraud gets detected from a certain scale onwards and triggers investigation
- Summary: No visible change from 7 years ago

Telco vs. Internet-driven IT security

mobile industry today has security practises and procedures of the 20th century

- no proper incident response on RAN/CN
- no procedures for quick roll-out of new sw releases
- no requirements for software-upgradeability
- no interaction with hacker community
- no packet filtering / DPI / IDS / firewalls on signalling traffic
- active hostility towards operators who want to do pen-testing
- attempts to use legal means to stop researchers from publishing their findings

this sounds like medieval times. We are in 2015 ?!?

Real-world quotes

The following slides indicate some quotes that I have heard over the last couple of years from my contacts inside the mobile industry. They are not made up!

Quote: Disclosure of Ki/K/OPC

"we are sending our IMSI+Key lists as CSV files to the SIM card supplier in China"

Quote: RRLP

"RRLP? What is that? We never heard about it!"

Quote: SIM OTA keys

"we have no clue what remote accessible (OTA) features our sim cards have or what kind of keys were used during provisioning"

Quote: Malformed

"we have never tried to intentionally send any malformed message to any of our equipment"

Quote: Roaming

"We are seeing TCAP/MAP related attacks/fraud from Operator XYZ in Pakistan. However, it is more important that European travellers can roam into their network than it is for Pakistanis to roam into our network. Can you see while the roaming agreement was only suspended for two days?"

Quote: SIGTRAN IPsec

"we are unable to mandate from our roaming partners that SIGTRAN links shall always go through IPsec - we don’t even know how to facilitate safe distribution of certificates between operators"

Quote: NodeB / IPsec

"We mandated IPsec to be used for all of the (e)NodeB back-haul in our tender, the supplier still shipped equipment that didn't comply to it. Do you think the CEO is going to cancel the contract with them for that?"

Quote: Government / independent study

"Govt: We put out a tender for a study on overall operator network security in our country. Everyone who put in a bid is economically affiliated or dependent on one of the operators or equipment suppliers, so we knew the results were not worth much."

Quote: Technical Staff

"15 years ago we still had staff that understood all those details. But today, you know, those experts are expensive - we laid them off."

Quote: Baseband chip vendor

"We have no clue what version of our protocol stack with what modifications are shipped in which particular phones, or if/when the phone makers distribute updates to the actual phone population"

The A5/3 disaster

Nobody cares to implement it

- May 2002: A5/3 spec first released. Target: supported in handsets and networks in 2004.
- May 2007: SA WG3: lack of BSS vendors supporting A5/3 (5 years later!!!)
- January 2009: First discussions with phone makers on A5/3 interop tests
- November 2009: 10 handsets from 7 manufacturers being tested on a live A5/3 network

After the track record of A5/2 and A5/3, they seem to be on a *fast track* to improve.

The overall algorithm disaster

- Advances in security require algorithms to be replaced and key lengths to grow
- Nobody in the GSM world seems to have realized such a basic cryptographic truth
- Infrastructure vendors reluctant to make algorithms software-upgradeable. They'd rather sell ten-thousands of new BTSs
- Operators never made it a requirement to do in-field algorithm upgrades. Why would they?
- Internet analogy: Who would ever want to use more than 40-bit RC4 encryption in his SSL implementation and upgrade that?

2009: GSMA starts to think

- November 2009, 3GPP TSG SA3 WG, GSMA Liaison Report: *The meeting considered the need to ensure that future infrastructure algorithm updates will be exclusively software based*
- About one decade too late for anyone with even remote knowledge of real-world cryptographic deployment
- Six years after the A5/2 cryptanalysis paper
- Seven years after A5/3 has been specified

Telco vs. Internet

still remember the days of analog modems, UUCP, BBSs, Usenet?

- the culture gap between Internet vs. Telco has always existed
- it didn't change much during the last decades
- analogy: The "IBM priests" mainframes vs. personal computing in 1970ies/1980ies
- IETF vs. ITU
- open participation vs. closed club

Research in TCP/IP/Ethernet

Assume you want to do some research in the TCP/IP/Ethernet communications area,

- you use off-the-shelf hardware (x86, Ethernet card)
- you start with the Linux / *BSD stack
- you add the instrumentation you need
- you make your proposed modifications
- you do some testing
- you write your paper / proof-of-concept and publish the results

Research in (mobile) communications

Assume it is before 2009 (before OpenBSC/OsmocomBB) and you want to do some research in mobile comms

- there is no FOSS implementation of any of the protocols or functional entities
- almost no university has a test lab with the required equipment. And if they do, it is black boxes that you cannot modify according to your research requirements
- you turn away at that point, or you cannot work on really exciting stuff
- only chance is to partner with commercial company, who puts you under NDAs and who wants to profit from your research

GSM/3G vs. Internet

- Observation
  - Both GSM/3G and TCP/IP protocol specs are publicly available
  - The Internet protocol stack (Ethernet/Wifi/TCP/IP) receives lots of scrutiny
  - GSM networks are as widely deployed as the Internet
  - Yet, GSM/3G protocols receive no such scrutiny!
- There are reasons for that:
  - GSM industry is extremely closed (and closed-minded)
  - Only very few closed-source protocol stack implementations
  - GSM chipset makers never release any hardware documentation

Testing/Auditing just like in the IP world

- Learn and adapt from the Internet security world
- Encourage all kinds of testing and audits rather than prevent them
- Fuzzing+Pentesting all protocols on all levels

- I'm not aware of any of the well-known GSM security researchers having been invited to equipment vendors to do sophisticated testing/attacks/audit
- That's inefficient use of existing skills!

Change the way of thinking

- Give up the idea that certain interfaces are not exposed
- TCAP/MAP/CAP are exposed to anyone with SCCP (SS7) access
- This includes all government agencies world-wide, as they can easily force domestic operators to give them access!
- Governments / regulators should put strong security requirements on domestic operators to secure those interfaces against attacks
- This is critical infrastructure that the general public, industry and even government/administration increasingly relies on
- Multiple lines of defenses, not one or zero

Skill building

- We need more teaching/training in academia to generate independent experts, without vendor affiliation
- Theoretic lectures are boring. Practical experiments / lab exercises required to get students excited / interested
- Very few universities have been provided with sufficient equipment to run / experiment / play with their own GSM/3G networks
- As long as it is much easier to research TCP/IP than mobile protocols, majority of the brain power will focus on TCP/IP
- Open Source implementations are critical for experiments!

Less mono-culture

- Very few equipment vendors and protocol stack vendors
- Even less vendors of ASN.1 / CSN.1 code generators
- Finding an exploitable bug in one of the 2-3 major ASN.1 code generators will permit you to exploit pretty much any equipment independent of the vendor

Procedures / incident response

- start to adopt scheme like CVE, vulnerability databases
- be prepared to rapidly roll out updates to all elements in the operator infrastructure
- have specs that require sufficient spare FPGA / DSP / CPU / RAM resources in hardware to ensure software-upgradeability of components

Long-term maintenance/upgradeability

- Just having the capability for secure upgrades is only the start
- manufacturers need to commit to *decades* of security fixes and updates for infrastructure parts that are often used ten years and more.
- unless that's required from before the purchase, they won't do it
- source code escrow mandatory in case of manufacturers going out of business
- Operators need to bring those requirements to their tenders!

Summary

- A lot of tools are available for 7 years now
- They have not been used as much as they could
- Operators and Equipment makers still largely ignorant of the problems
- We are still at the tip of the iceberg

Thanks

Thanks for your attention. I hope we have time for Q&A.