Structural deficits in Telco security

Harald Welte <hwelte@hmw-consulting.de>

gnumonks.org
hmw-consulting.de
sysmocom GmbH

March 21, 2013 / CSO

Outline

About the speaker

- Using + toying with Linux since 1994
- Kernel / bootloader / driver / firmware development since 1999
- IT security expert, focus on network protocol security
- Former core developer of Linux packet filter netfilter/iptables
- Board-level Electrical Engineering
- Always looking for interesting protocols (RFID, DECT, GSM)
- OpenEXZ, OpenPCD, Openmoko, OpenBSC, OsmocomBB, OsmoSGSN
- consulting/freelancing + sysmocom GmbH for custom-tailored GSM solutoins

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...

Telco vs. Internet-driven IT security

mobile industry today has security practieses 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 on signalling traffic
- active hostility towards operators who want to do pentesting
- attempts to use legal means to stop researchers from publishing their findings

this sounds like medieval times. We are in 2012 ?!?

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 overal 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 A5/2 desaster

Brief history

- August 2003: Barkan/Biham/Keller paper on instant ciphertext-only cryptanalysis of A5/2
- April 2006: GSMA initiative to withdraw A5/2. Resistance *mainly from north america*.
- October 2006: SA WG3 formally requests removal of A5/2 from spec
- July 2007: Almost all operators have moved to A5/1
- As long as phones support A5/2, semi-active down-grade attacks against A5/1 can be implemented!

Three years incident response to update the spec! I'm not even talking about the time to update all equipment or until old equipment will be fully phased out.

The A5/1 desaster

history repeats itself

The industry did not learn from the A5/2 incident. History repeated itself:

- Kc generation was not changed between A5/1,2,3
- as long as phones support A5/1, A5/3 can be broken with semi-active down-grade attacks just like A5/2 -> A5/1 before
- There is still no way to disable algorithms of devices in the field, not even by flags on the SIM card

How can an entire industy be so resilient against learning?

The A5/3 desaster

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 desaster

- 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
- Infrastruture 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

ETSI/3GPP security working group(s)

- seem to have done excellent work
- nobody seemed to care about what they say
- A5/4 (128bit) was originally supposed to come together with A5/3 in 2004
  - has been put back as it would affect handset software (so what? there are only about 6 implementations out there. How hard is it to update all 6?) is the only solution of fixing semi-active downgrade attacks
- UMTS AKA over GERAN
  - good idea, but where is the SIM card flag that tells the phone about mutual auth being mandatory?
- Great ideas seem to fall short of being thought-through to the end, and nobody implements them in a timely manner anyway

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

Evolving GSM specification process

- At CEPT, it was government officials of postal/comms ministry equipment vendors didn't even have the right to propose something
- At ETSI, equipment vendors got onto the table Over time, shift of power from operators to equipment manufacturers
- At 3GPP, today we see way too little operator input in standardization
- Interest of users seems completely absent
  - neither professional users (companies worried about industrial espionage, government users, ...)
  - nor consumers in form of consumer protection, privacy, data protection or other organizations seems to be missing completely
- standardization process primarily serves the interest of equipment vendors to get their patented technology into widespread adoption to drive IP licensing revenue

Evolution of operators

- classic operator: Does everything in-house
- common today: Outsource everything
  - billing
  - network administration / operation / servicing
  - network planning
- outsourcing to whom?
  - to the equipment suppliers
  - am I the only one seing a conflict of interests here?

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/GPRS 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 defences, not one or zero

Specifications / Testing

- If specs require any tests, they are *functional* specs
- I've never seen requirements to test for invalid / intentionally malformed messages
- Actively provide equipment (access) to academia and research, invite researchers to test/break things

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 monoculture

- 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-upgradability of components

Engagement with the security community

- Actively engage academic and individual security researchers
- Sueing them is not a solution, this has been tried in the 1990ies in the PC/Software industry
- If you don't provide researchers inexpensive/available hardware, they have to break femtocells and other devices in order to do their legitimate research
- Compare with gaming consoles exploits: All of them have been broken by people who wanted to run Linux and custom software on them. Only PS3 survived much longer, as they provided such means to the users from day 1 (and later removed it, requiring to break the PS3, too)

Thanks

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