Nethemba
all about security

New trends in public and massively used technologies

Pavol Lupták
Lead Security Consultant, Nethemba s.r.o.

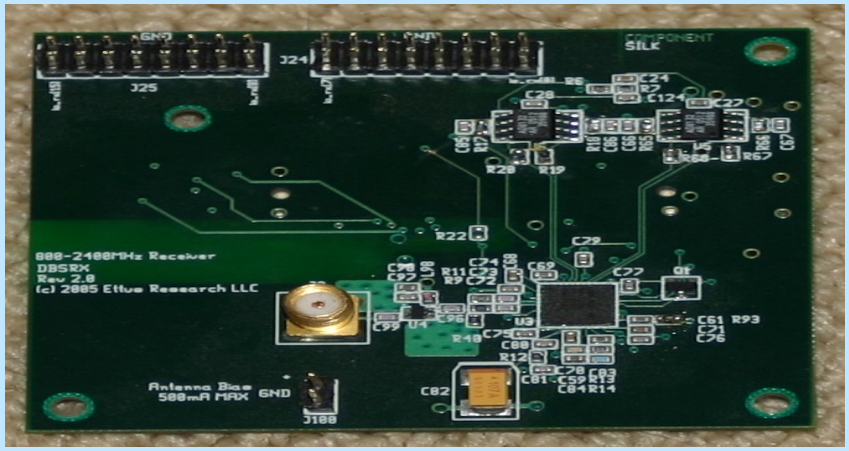
TOC

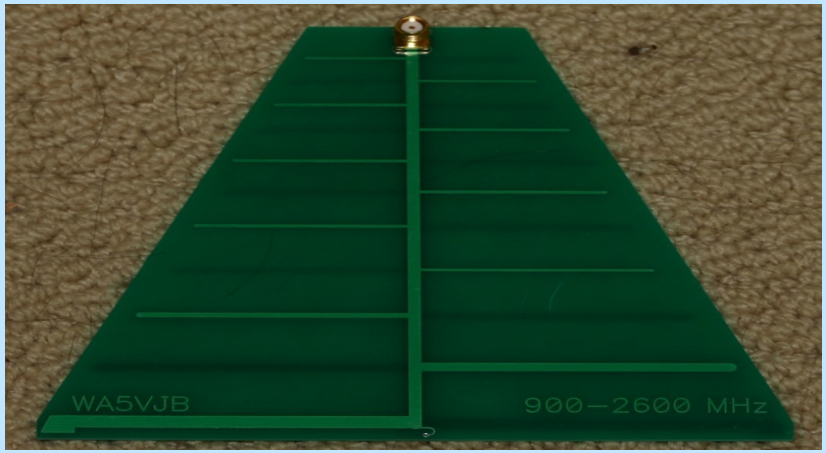
- GSM/3G security
- Mifare Classic/DESFire
- Biometric passports
- Hitag2 a Keeloq
- Vulnerabilities in public SMS tickets
- Slovak e-toll
- **Security events in the near future**

Cracked GSM – can anybody easily intercept anybody?

- Presentation of A5/1 cracking session – GSM vulnerability session was canceled in Berlin during 26C3
- Your mobile communication between you phone and BTS is encrypted using A5/1 which was theoretically cracked in 1997. practically in 2007 by Steve D. Hulton.
- It is possible to create special A5/1 rainbow tables that can be consequently used for cracking your intercepted encrypted GSM call.
- Using public available and sold device (USRP2) and suitable daughter board receiver - GSM cards (for about $2000), it is possible completely passively and anonymously (without a notice!) intercept a consequently cracked arbitrary GSM communication, USRP2 can be used for creating own BTS using public available OpenBTS implementation that can be misused for gaining full control (MITM) over given mobile phones and mobile network
- Security of GSM is broken, mobile operators **still ignore this fact(!)** and threat your privacy with possibility of unprivileged trivial intercepting (more than 4 billions people are affected in more than 200 countries
- Can be this security issue solved by more secure A5/3 encryption?

USRP2 and „daughter board“ GSM cards





“More secure” encryption used in 3G (A5/3) is also cracked

- A5/3 Kasumi was supposed to be „more secure“ version of „MISTY“ cryptosystem used in 3G networks
- Adi Shamir (RSA author) published a practical attack against A5/3 Kasumi last year
- His attack paradoxically works against “more secure” A5/3 Kasumi, but not against “less secure” MISTY
- He was able to crack 3G communication during 2 hours on the common PC
- **All 3G networks are vulnerable, there is no secure solution**

Do you still trust in your GSM/3G communication?

Mifare Classic RFID cards

- Probably the most used cards in the world (more than 1 billion chips in the world, and more than 1 million in Slovakia)
- **Used by public transport companies in London, Bratislava, Košice, Warsaw, Krakow, Sofia, Bucuresti, Malmo, Dutch cities, Luxembourg, ...**
- **Used by all Slovak and Czech ISIC / University ID cards (STU/UK)**
- Parking cards in Bratislava, Plzeň, Krakow, Warsaw, …
- Badge cards to many buildings including parking lots and **swimming pools**
- First vulnerabilities have been published in 2007 during CCC conference in Berlin
- First big hack of “London Oyster cards” by security research from Dutch University Radboud
- First open-source (GNU GPLv2) implementation of Mifare Classic offline cracker released by Nethemba s.r.o. That can be used for cracking and extracting all keys from all Mifare Classic cards
- The main Mifare Classic distributor in Slovakia (EMTEST) was informed 3 months before MFOC public release

Mifare Classic 1kB/4kB cards

Mifare Classic security facts or how these vulnerabilities can be exploited

- Easy cloning/copying of these cards are possible
- Charge arbitrary credit
- 100% card emulation (Proxmark3, Nokia NFC)
- Read sensitive information (names, surnames, credit, expiration dates) – just walk in any tram
- Permanently destroy all cards in certain proximity (e.g. public transport passengers)
- Monitor passenger location/movements

The attacker has full control over the Mifare Classic card's content!

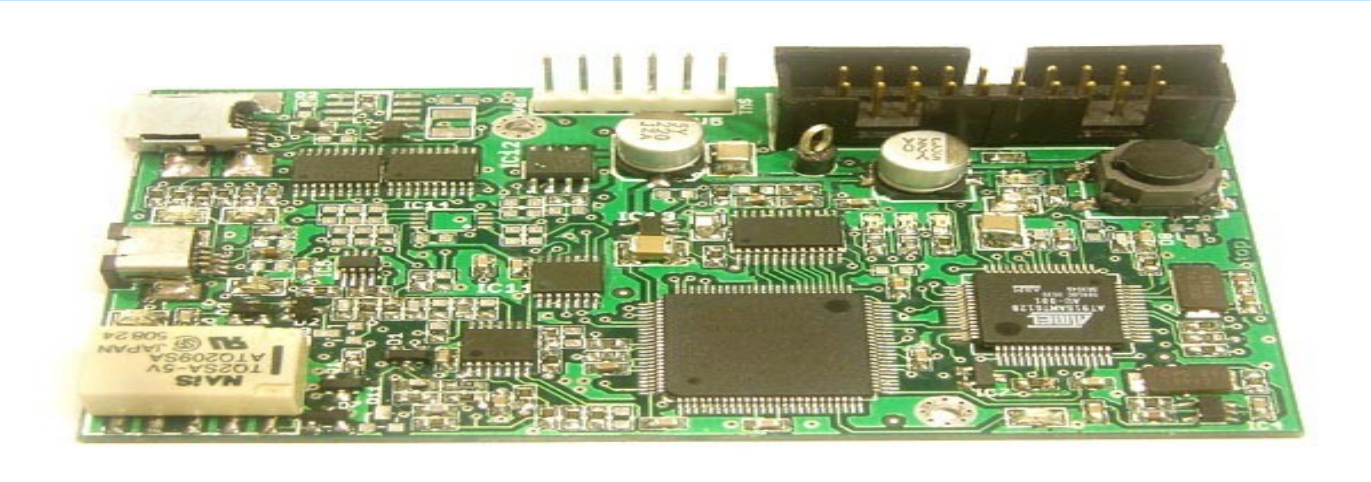
Mifare DESFire

- „secure“ version of Mifare, 3DES/AES is used, supports Mifare Classic emulation
- Used by OpenCard in Prague
- Prague's Library uses vulnerable implementation (authentication based on UID)
- Possible emulation using PicNic (author Tomáš Rosa) http://crypto.hyperlink.cz/picnic.htm

How to emulate Mifare?

- Proxmark III (hi14asim using command, only UID)
- ACR122 touchatag (only UID, very very slow)
- Nokia NFC based phone (6131, 6212)
- MiKeyCard (www.mikeycard.org)
- PicNic (Tomáš Rosa specific hardware)
- Huayu phone (can emulate even UID?)
- Icarte adapter with an iPhone

Proxmark III a Touchatag reader



Biometric RFID passports

- All EU passports (including Slovak ones) have RFID 72kB chip, contain a lot of sensitive information (your JPEG photo, personal data from your passport, your fingerprint, ..)
- Using MRZ code (Passport number + Birth date + Passport expiration date) it is possible to read almost all data from the passport (except EAC and fingerprint) using cheap and public available Touchatag reader (it costs 30 € only)
- Birth date can be usually revealed from public sources (social networks :-), passport expiration date is 10 years (just 3650 possibilities). How the passport number is generated?
- Older passports (without EAC) can be easily cloned or emulated using Nokia NFC phone
- A special private key is necessary for reading personal fingerprint – it is possible to gain this information using covert channels attacks (time analysis of voltage/current differences during RSA computations), in case of potential breach, **it will be possible to read all your fingerprint and other sensitive informations!**

Biometric RFID passports II.

- It is possible to create an “imperfect” passport clone (without public AA key and fingerprint) using JCOP v4.1.72 k smart card – question is - how official readers do process “imperfect” cards?
- Possibility of relaying attacks (transparent MITM)

Biometric RFID passports with fingerprint information

Reading of biometric passport

Slovak police claims *“it is not possible to read biometric passports”, „Passport information can be read using a special reader only, chip is a passive element“*.

Do you still feel safer with your biometric RFID passports?

Hitag2

- Chip used in many cars (Renault, Opel, Peugeot, Citroen)
- Broken technology since HAR2009
- It is possible to crack the intercepted communication (from USRP2) using SAT solvers (open-source implementation http://minisat.eu) - pseudo-boolean solver

Keeloq

- Cipher used in many car keys (Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Volkswagen Group, Clifford, Shurlok, Jaguar)
- Broken 2 years ago http://www.cosic.esat.kuleuven.be/keeloq/
- It can be cracked in 2 days on 50 dual core servers
- Keeloq communication can be sniffed by USRP

Other broken RFID technologies

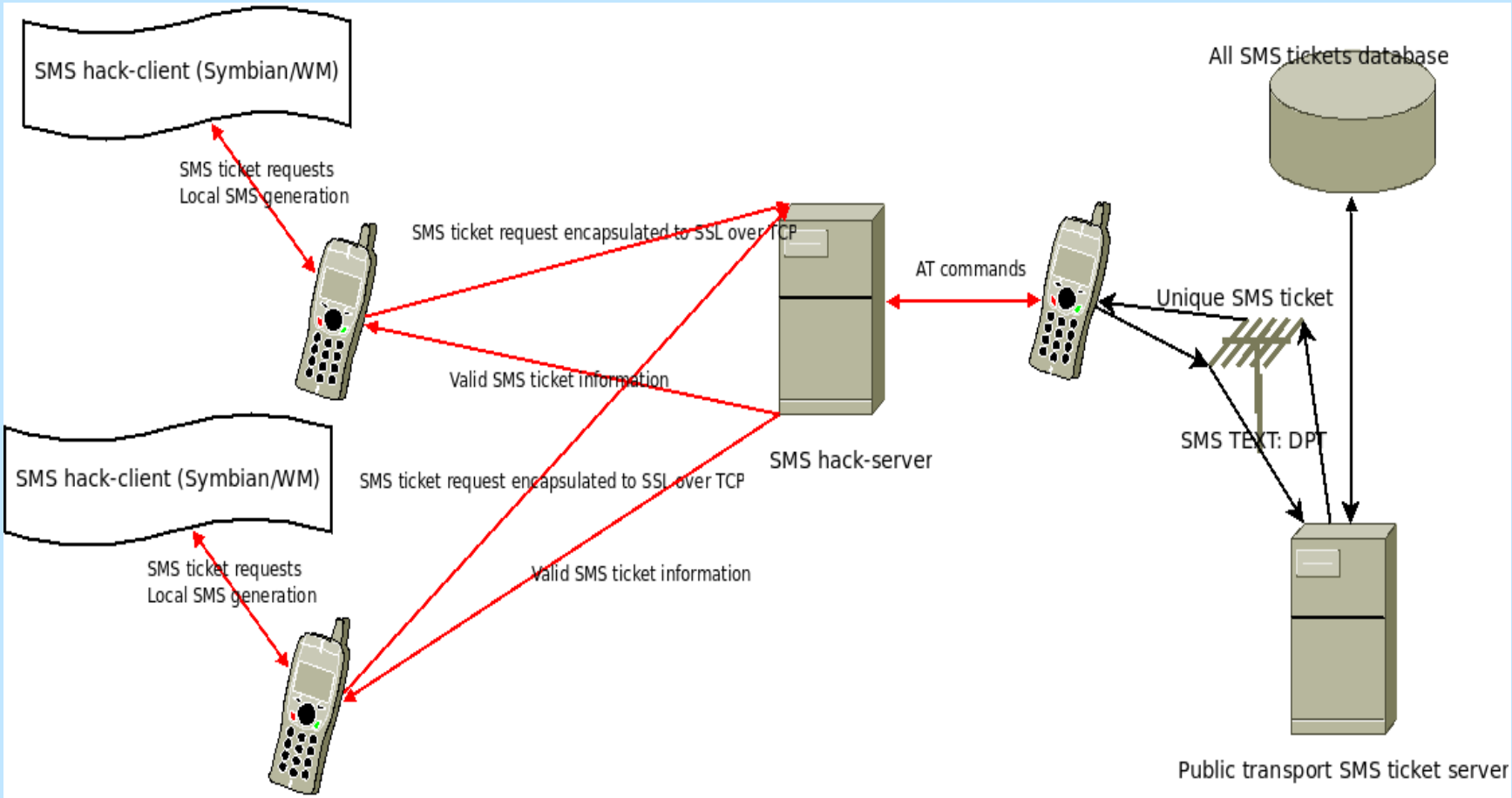
- **Hitag2** - „badge“ cards, car keys for Renault / Opel / Peugeut / Citroen
- **Legic Prime** – payment cards
- **Mifare UltraLight** – ski-cards
- **HID Prox** – massive use
- **Biometric passports** – all that do not use EAC, can be easily cloned

There are no secure RFID cards, just cards that have not been cracked yet...

Vulnerabilities in public SMS transport tickets

- Typical example of **bad security architecture** – there is no secure binding between the passenger and his SMS ticket
- SMS ticket can be easily generated, distributed and shared by many people
- Using sophisticated detection of geographical collisions and possibility to forge sender number in SMS message or call, **it is almost impossible to reveal this attack (and definitely not economical from Public transport companies)**
- Vulnerable SMS systems in big cities – Košice, Bratislava, Prague, Vienna, Warsaw..
- Bratislava public transport company has been informed about this vulnerability before its deployment, Prague public transport company threated us with legal process
- Bratislava public transport company decided to use “one-day” SMS ticket that **significantly decreases the implementation complexity of this attack**

SMS hacking system architecture



Security of Slovak e-toll system

- Extremely expensive non-transparent project paid by tax-payers
- We have contacted Skytoll company **regarding possible security analysis in order gain more security information about this technologies** – they received our request, but with no response
- **Proprietary project, non-public proprietary closed security –** we can just guess how it works exactly from the security point of view
- We don't know if this proprietary solution is secure or not, but **we know that this technology is relied on already security broken and dangerous technologies:**
  - **GSM –** can be in real time jammed, cracked, intercepted, spoofed, ...
  - **GPS –** can be in real time jammed or spoofed (GPS spoofing)
- Necessity of openness public projects (that are paid by the government money) – **all information about security specification, used protocols, algorithms, ciphers should be public!**

OBU GPS/GSM unit

It is possible to avoid toll fees using public available GPS jammers!

Summary

- Increasing complexity of information technologies implicates a lot of vulnerabilities and potential attacks
- **In case of secure technologies**, **new theoretical attacks appear**
- A lot of current theoretical attacks become practical
- Many technologies are vulnerable because they are **proprietary and closed,** where mutual **feedback is missing from the technical community and independent security researchers**
- In case of massively used technologies, there is always a **need of objective and independent security audit**

Only open technologies can be really supposed to be secure (otherwise you never can be sure of security…)

Security events in the near future

- 23-26.11 Deepsec (great schedule, but expensive)
- 29-30.11 Confidence 2.0 in Prague
- 27-31.12 27C3 in Berlin

Don't hesitate and come!

Thanks for your attention!

Any questions?