

Railway: Security aspects

Charles Brookson

Chairman ETSI TC CYBER

charles@zeata.co.uk Zeata Security Ltd

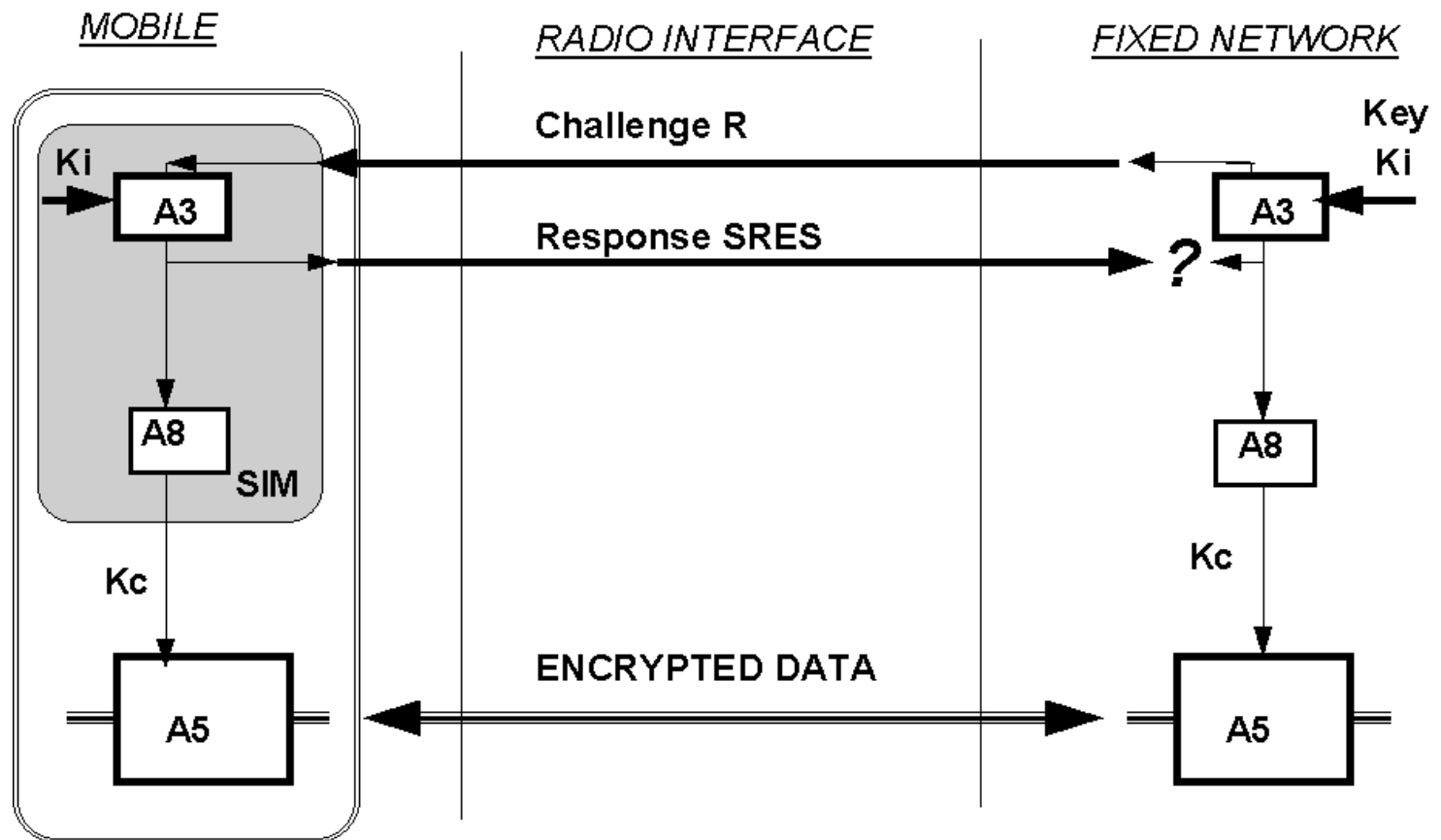
Background on Security

- ETSI – many groups involved in Security
 - Algorithms, TC CYBER, Radio (TETRA etc.), NFC, Smart Cards and many more
 - New security overview white paper
- 3GPP
 - Third Generation Partnership project
 - GSM, 3G, 4G, 5G
 - Includes Security and some specific issues (SA3)
- www.3gpp.org www.etsi.org

Security in GSM

- Authentication
 - Uses SIM card and Authentication algorithm
- User and signaling privacy
 - Uses A5 algorithms
 - GPRS uses GEA algorithms
 - Other data system uses EDGE
- Encryption is only to the base station
- Very old, designed security in 1986

What does GSM security look like?



GSM security issues

- A5/1 can be broken in a few minutes (rainbow Table, Karsten Nohl)
 - GSMA recommends A5/3, A5/4 for Operators
- Some authentication algorithms broken:
 - COMP128 -1, -2, -3
 - GSMA recommends A5/3, /4
 - A5/1 **NO!** A5/2 REMOVED from Mobiles!
- Some protocol weaknesses
 - Man in the middle attack (SDRs, Cheap Base Stations)

What happens if you?

- Have no authentication, and use A5/1?
- Communications can be eavesdropped, intercepted, modified and deleted **within a few minutes** by finding the A5/1 key.

Security

UK rail comms are safer than mobes – for now – say infosec bods

Industry told to harden systems to prevent future train smash carnage



30 Apr 2015 at 11:57, [John Leyden](#)




Analysis Last week's warning that Britain's railway systems could be susceptible to hacking has triggered a debate among security experts.

Prof David Stupples of City University London made headlines last week with a [warning](#) that plans to replace the existing (aging) signalling system with the new European Rail Traffic Management System (ERTMS) could open up the network to potential attacks, particularly from disgruntled employees or other rogue insiders. "Major disruption" or even a "nasty accident" could ensue if miscreants were able to plant malware on the system, the computer scientist warned.


More like this

Scada


Most read



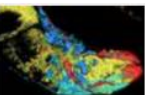
Obey Google, webmasters, or it will say you can't be trusted




Google man drags Emacs into the 1990s



Google drops a zero-day on Microsoft: Web giant goes public with bug exploited by hackers



Boffin's anti-worm bot could silence epic Mirai DDoS attack army



WebAssembly: Finally something everyone agrees on – websites running C/C++ code

Spotlight



A high-speed train, blurred to indicate motion, travels along a track through a lush green landscape. The train is silver with a red stripe. The track is flanked by dense green trees and bushes. A tall antenna tower is visible in the background. The sky is a mix of blue and white clouds.

A FORMAL ANALYSIS OF ERTMS TRAIN TO TRACKSIDE PROTOCOLS

TOM CHOTHIA

JOERI DE RUITER
UNIVERSITY OF BIRMINGHAM

RICHARD J. THOMAS

Attack scenarios

- Ignore insecure signaling protocols (ERMTS) and equipment
- **Radio - You can talk to all to everyone in 10 minutes**
 - Break A5/1 in 10 minutes (online available)
 - Use a Software Defined Radio to Transmit
 - Speak over GSM-R
 - Cost 500 Euros
- **Other scenarios you can imagine?**
 - Tell trains to go through RED
 - Signaling changes
 - Nuclear waste, carriage of dangerous materials?

3G and 4G

- Is much better:
 - Authentication uses stronger algorithms
 - Uses mutual authentication to overcome man in the middle.
 - Stronger encryption for privacy
 - Much stronger than GSM (designed in a new climate of Export Control)

“Political” issues

- Lawful Interception
- Export control of algorithms
 - Wassenaar agreement, restrictions
- Responsible disclosure system for security incidents - Hackers
- EU Directives
 - NIS Directive, Privacy Mandate
 - Data Protection - General Data Protection Regulation 2018
 - Consent, Fair processing notice, Accountability and privacy by design.
 - Individuals may start litigation, fines up to 4 percent turnover!

New 3GPP Group

- www.3gpp.org SA6 Mission Critical Systems
 - SA6 is responsible for the definition, evolution and maintenance of technical specification(s) for application layer functional elements and interfaces supporting critical communications (e.g. Mission Critical Push To Talk), including:
 - Relevant application architectural aspects (including both network and terminal aspects)
 - Definition of reference points for interactions between application functional elements
 - Allocation of application functions to particular subsystems and elements
 - Generating information flows between reference points within scope
 - Identification of application protocols

3GPP drives GSM-R to a new track - August 5, 2016

- ETSI Press Release – on the FS_FRMCS study item.
- At the recent 3GPP SA plenary, a study item was approved - to investigate the requirements for a new railway communication system, as a successor to the GSM-R service.
- GSM-R is facing a number of challenges:
 - The system life-cycle is coming to an end, with vendor support uncertain beyond 2030,
 - Extra capacity is required in some areas to support railway operations,
 - The rollout of European Rail Traffic Management System (ERTMS) has increased the strain on the GSM-R network
- To have a successor technology in place by 2020 for trials and by 2022 for deployment, the International Railway Union (UIC) have published a user requirement specification in their paper “Future Railway Mobile Communication System - FRMCS” (see S1-161250).

Short term strategy

- Need a stronger algorithm than A5/1
 - Move to A5/3, prefer A5/4 (128 bits)
 - ***Now agreed by GSMA and 3GPP end 2017***
- Need to change keys, introduce authentication
 - Look at GSM to see if authentication with embedded SIM is possible for uplift of security
 - See if another key changing protocol is possible to increase security
 - Mutual Authentication possible (3GPP SA3?)

Medium and Long term strategy

- Get involved in SA6 and FRMCS
 - Introduce the enhancements required in the specifications to support services
 - ***Send along Standards experts***
 - ***Need to put in your security requirements to those making standards***
- Look at the possibility of 3G and 4G systems
 - Business models, Upgrade path etc.
 - Stronger security, mutual authentication

Conclusion

- Are we in a **dangerous** place?
 - Opinions welcome!
- Need to have a short term strategy to deal with the issues now
- Need a medium and long term strategy for the evolution
- Need to be involved now to contribute to Standards.