Secure Systems Group, Aalto University

Mikko Kiviharju, SSG / Finnish Defence Research Agency (FDRA)
Christina Lassfolk, NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)
Hannu H. Kari, National Defence University, Finland
Sanna Rikkonen, FDRA

Evolution of Cryptographic Key Management in Cellular Standards for European Railways(*)

- Railway infrastructure communications needed to **prevent trains from crashing**
- Railways in Europe rely on cellular networks and standards for their network security
- Manual **key management** and integrity-related services are **a concern** in **old GSM-R**
- **LTE-R not sufficient**, but **5G R16 IIoT service-based architecture** should be adopted

Introduction

- Railway infrastructure communications **prevent trains from crashing**
- Onboard and trackside communications: trackside includes balises (RFID-tags buried within the tracks to provide location information).
- Railways communication standards have usually three layers: application (e.g. ERTMS Subset 026), messaging (e.g. Euroradio) and carrier (e.g. GSM-R) layers
- In Europe and Eastern Asia, carrier layer relies on cellular technologies

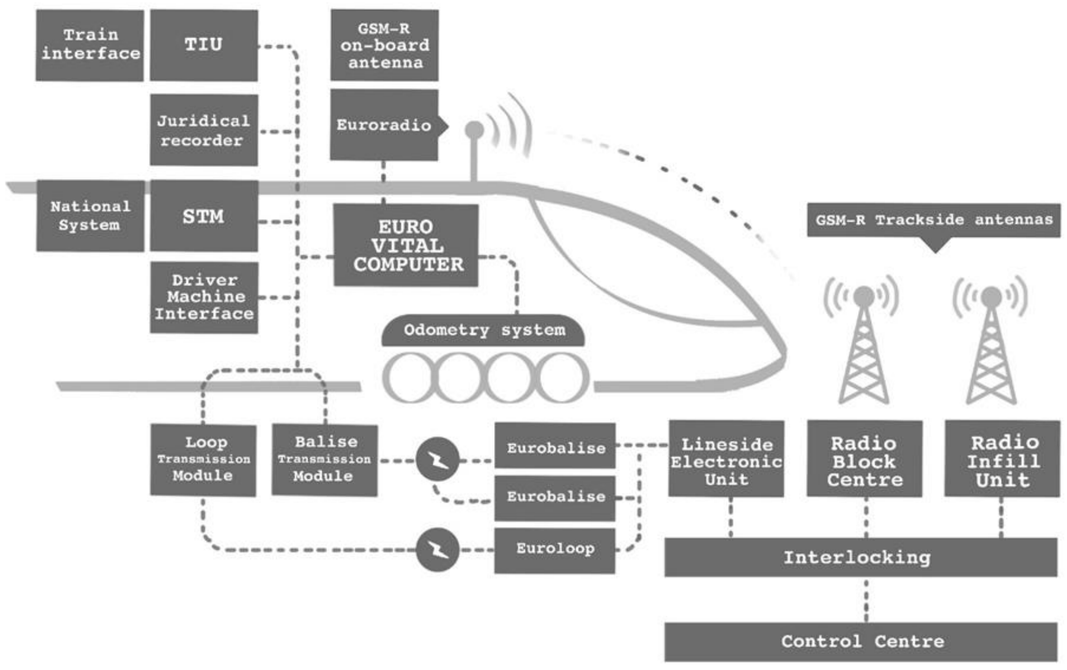

Figure 1: Railway infrastructure communications in European standards. European Rail Traffic Management System (ERTMS) defines the standards used to control communications in different subsystems in countries abiding to the standard. Similar standards are also evolved e.g in Eastern Asia.

Security of the trackside comms

- Current ERTMS signalling system version (ECTS Level 2) specifies GSM-R with **manual key management** as the carrier layer.
- GSM is confidentiality oriented, train management integrity-oriented.
- GSM known issues: e.g. **IMSI-catching** and **old cryptography** standards for message integrity.
- **Inter-protocol security** between carrier and messaging layer not properly analyzed
- Balise system **"security" is** based on **physical access only** (need to be on the RFID programming range).
- Where to go next? Are the choices satisfactory?

Standards evolution

- GSM-R is being replaced by the 4G-technology LTE-R (Long-Term Evolution for Railways) in Eastern Asia
- Europe is waiting for the 5G-version (Future Railway Mobile Communication System, FRMCS)
- Security-wise, **LTE-R** is GSM ***evolution***, **5G** is a complete **overhaul**
- FRMCS (and 5G) have a **service-oriented layer**: it is possible to realize application-specific security on top of carrier operator security

Cryptographic security

- We evaluated the known cryptographic shortcomings in ERTMS signalling (Euroradio over GSM-R) against future possibilities, such as the 4G LTE-R and 5G FRMCS, in Table 1.
- 5G-technologies offer: more variety in cryptographic management; more integrity functionality; a specific IIoT security framework;…
- Balise functionality is replaced with multiple concurrent systems.
- 5G supports public-key schemes, but not full PKI

Security concern	ER/GSM-R	ER/LTE-R	FRMCS/5G
Small block length of authentication tags	-	-	+
Lack of modern cryptographic primitives	-	~	+
Lack of cryptographic protection in balises	-	-	~
Heavy key management (resulting from symm. key)	-	-	+
Lack of public-key use and management	-	-	~
Manually managed key material	-	-	+
Key authentication	-	-	+
Network authentication	-	~	+
Service authentication	-	-	+
Downgrading attacks	-	-	+
RBC identification	-	~	+
RBC handover keying	-	~	+
IMSI catching	-	-	+
RRC idle mode security	-	-	+
Legend			
- does not mitigate the security concern at all			
+ security concern is fully mitigated			
~ it is implementation, case or definition dependent if and to what extent this is mitigated			

Table 1: Cryptographic concerns in ERTMS. The ERTMS signalling (Euroradio over GSM-R) shortcomings and their relevance in the upcoming standards, LTE-R (a 4G-technology) amd FRMCS (a 5g technology)

(*) Presented in CyCon 2022, 14th International Conference on Cyber Conflict, "Keep Moving" (2.6.2022, Tallinn, Estonia)

Aalto University