TRAKS: A Universal Key Management Scheme for ERTMS
Executive Summary

RICHARD J. THOMAS, University of Birmingham, UK
MIHAI ORDEAN, University of Birmingham, UK
TOM CHOTHIA, University of Birmingham, UK
CLIVE ROBERTS, University of Birmingham, UK

This paper presents a new Key Management and Distribution Scheme for use in the European Rail Traffic Management System (ERTMS). Its aim is to simplify key management and improve cross-border operations through hierarchical partitioning. The current scheme used in ERTMS involves the creation and distribution of 3DES keys to train and trackside entities, which are then used as part of the EuroRadio Protocol to provide message authentication. This results in the distribution of tens of thousands of keys using portable media, a prohibitively high burden on management and resourcing. We present a symmetric key solution, TRAKS, which has the benefit of being backwards compatible with the current ERTMS standard and being post-quantum secure. This new scheme reduces the number of cryptographic keys in circulation, and maintains the current security model. We achieve this by dynamically deriving unique keys from a shared secret, i.e. the line secret, which is combined with IDs of trains, and of signalling equipment. In addition to providing better key management, our scheme also adds authentication to the location data provided by EuroBalises.

1 INTRODUCTION

The European Rail Traffic Management System (ERTMS) is a safety-critical ICS which provides a suite of protocols used to deliver a modern train management and signalling platform[1]. This standard is designed with the intention to enable trains to interoperate across borders and optimise the running operation of railways. At present, the system is being rolled out across Europe and also on high-speed lines around the world.

ERTMS is defined as a protocol stack formed of the following three layers: GSM-R [1], EuroRadio and the Application Layer Protocol. The EuroRadio and the Application Layer Protocol form ETCS, the European Train Control System [2]. GSM-R, a rail-specific variant of the GSM protocol, is used for communications between the train and trackside infrastructure such as radio block controllers (RBCs), i.e. the trackside components that manage trains in a geographical area. RBCs are responsible for issuing 'movement authorities', messages which permit a train to move a specific distance at a given speed, and managing safe train movement in a geographic region of approximately 70km. Trains periodically provide location updates and the RBC would respond with an updated movement authority. The EuroRadio protocol layer provides authentication and integrity of the communication using cryptographic MACs. Messages which have a valid MAC (or are from a carefully selected subset of messages that may be sent at a high priority and not requiring a MAC) are passed to the application layer.

EuroBalises are devices placed between the tracks, typically in groups of two or three, which are read by a train passing over them. The train trusts the EuroBalise to provide accurate location (rather than using GPS) and track profile data, which can include speed limits, gradients and tilt profiles. Currently, the balise data is validated using a CRC code, which is publicly known [5], and is only for error detection but does not provide any integrity protection.

The current ERTMS standard [3] states that key provisioning and management should be done based on geographical *domains* (e.g. Great Britain), where each domain has a Key Management Centre (KMC) which is responsible for key generation and management for that domain. Additionally, the KMC also defines procedures to install the keys on train on-board units (OBUs) and RBCs. Throughout the paper we will interchangeably use the terms *train* and *OBU* to refer to trains. The current procedure requires that keys for an OBU or from an RBC are generated by the KMCs following a request from a vendor (e.g. Siemens). After generation, the keys for the requesting OBU or RBC are sent in the clear on portable media devices [4], to be installed."”

This setup is highly inefficient; using portable media devices to move keys greatly increases the risk of compromise, especially due to the fact that keys on the device are stored in cleartext. Additionally, this makes deployment and management of keys difficult (i.e. in order to update a key for an RBC, an engineer needs to physically travel to the RBC's location in order to install the key on the portable media device). Informal discussions with rail systems managers have highlighted that insecure strategies like (i) provisioning all (OBU, RBC) key pairs to each OBU and RBC, or simply (ii) having KMCs extend the life of keys when they are due to expire are used in practice. Cross-border operation is also challenging as keys need to be shared between geographical

[1]http://www.ertms.net

Authors' addresses: Richard J. Thomas, University of Birmingham, Birmingham, UK, R.J.Thomas@cs.bham.ac.uk; Mihai Ordean, University of Birmingham, Birmingham, UK, M.Ordean@cs.bham.ac.uk; Tom Chothia, University of Birmingham, Birmingham, UK, T.P.Chothia@cs.bham.ac.uk; Clive Roberts, University of Birmingham, Birmingham, UK, C.Roberts.20@bham.ac.uk.

University of Birmingham 2017.

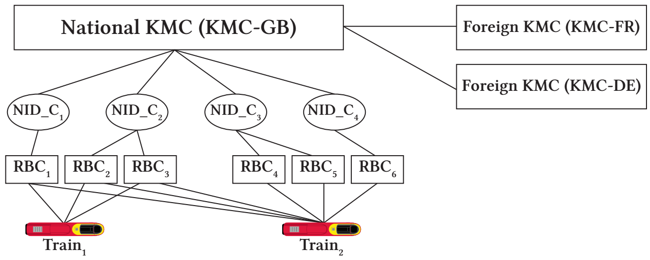

Fig. 1. TRAKS Key Hierarchy for ERTMS. TRAKS is composed of four layers: (1) the national infrastructure for the 'home domain', which is responsible for liaising with foreign KMCs. (2) Geographic regions within a country, known as NID_C. (3) RBCs, responsible for command and control messages to trains. (4) Trains, which operate across one or more NID_C regions.

ERTMS Keys	Current	TRAKS
NID_C Secret	×	$knid\_c$
RBC Derivation Key	×	$km_{rid,null}$
Train Key	$K_{MAC_{rid,oid}}$	$km_{rid,oid}$
Balise Secret	×	km
Balise NID_C Area Key	×	$km_{\texttt{NID\_C},null}$
Balise MAC Key	×	$km_{\texttt{NID\_C},bgid}$

Fig. 2. Proposed TRAKS Key Management Hierarchy. We introduce the new notation used throughout this paper as: a train with OBU ID 3, communicating with an RBC with ID 5 would have the key $km_{rid5,oid3}$. Balise MAC Keys are bound by the NID_C they are located in and their unique balise group ID, $bgid$.

domains that are managed by different KMCs. Under the current scheme, additional burden is placed on the foreign KMC operators (KMC owners who are outside of the 'home domain' that the train is registered). Whenever a new OBU is to operate in their domain, they are required to establish the appropriate keys to hand to the 'home' KMC, but they also have to send an engineer to each of their RBCs to install the necessary keys. In the case of a progressive national deployment, this burden is high.

2 BENEFITS OF TRAKS

Using TRAKS (Train and RBC Authenticated Key Scheme), it is possible to reduce the complexity of key management across a domain, but also improve cross-border operation by reducing the number of key management activities required.
The key benefits delivered by TRAKS are:

Reduced number of keys in circulation. Currently, a unique KMAC pair exists between a train and RBC. This means that for any new train introduced to a network, an engineer must also install the appropriate KMAC key onto every RBC required. Under TRAKS, the RBC is provisioned once and may derive the appropriate km key based on the ETCS ID of a given train. New trains are still provisioned with a unique $km_{rid,oid}$ key.

Full backwards-compatibility against SUBSET-038. One key consideration for TRAKS was to enable infrastructure managers to progressively implement the scheme. Keys issued under TRAKS may be used immediately, while the underlying infrastructure (e.g. RBCs) are upgraded to support key derivation. We expand on this point in our paper.

Quantum-secure foundations. SUBSET-038 keys use 3DES, an algorithm that is being phased out, where key management operations under SUBSET-137 will be online, using RSA Public Key Cryptography. In a post-quantum world, RSA and Diffie-Hellman, two commonly used algorithms will not be secure. TRAKS does not use public key cryptography, instead using pseudo-random functions, which are believed to be post-quantum secure, and allows alternative algorithms to be used in its key derivation process.

Applicability to EuroBalises. Currently, EuroBalises provide no authenticity or integrity validation of their payloads beyond a CRC at the end of the telegram. This allows an attacker to mimic a valid balise, potentially placing a train in an unsafe position. Applying TRAKS as a framework, we can provide such guarantees to EuroBalises, allowing them to be a trusted component in the secure architecture of ERTMS.

3 TECHNICAL OVERVIEW

In this section, we provide a technical overview of TRAKS as a scheme. Further detail is given in our paper.

Under TRAKS, the hierarchy changes to that in Figure 1, where we leverage NID_C, a variable presented by EuroBalises to the train to indicate the line, region or country a train is operating in. From this, we can allocate one or more RBCs to a given NID_C, provisioning them with $km_{rid,null}$ keys which allow them to derive the kmkeys for any train in their region. Trains are approved by the infrastructure managers to operate in a given NID_C, where they have their $km_{rid,oid}$ keys provisioned.

For a given NID_C, its key, $knid\_c$ is established as follows:

$$knid\_c_i \leftarrow \mathrm{SGen}(1^{\lambda})$$

where $\mathrm{SGen}(1^{\lambda})$ is a pseudo-random number generator (PRNG) with the security parameter λ. Unlike the offline ERTMS scheme, however, this secret is never given directly to OBUs or RBCs. It is instead used together with IDs to generate the message authentication keys. This approach greatly enhances the usability of the scheme by reducing the overall management overhead (i.e. secret key material storage, distribution and disposal). In the following, we will detail how we use this secret to generate the authentication keys for each ERTMS entity.

Key Derivation is achieved through the use of a pseudo-random function (PRF) by applying the RBC ID to $knid\_c$ which produces the RBC key, $km_{rid,null}$. $km_{rid,oid}$ is derived by the RBC by applying the train ID, oid to $km_{rid,null}$ through the same PRF. We recommend the use of HMAC-SHA-256 as a PRF, which is believed to be post-quantum secure, however, any proven post-quantum secure PRF may be used.

4 PROVEN SECURITY

As part of the development of TRAKS, we have proven that the security of TRAKS key generation is at least as secure the current scheme, while providing all additional benefits with respect to key management. We provide a proof of this security in our paper.

5 CONCLUSION

In this summary, we have presented a new key management solution which we propose for use in ERTMS. Using proven cryptographic techniques, we achieve an interoperable, backwards-compatible solution that can be used in ERTMS. It reduces management overheads for national Infrastructure Managers, and delivers post-quantum security. This scheme has further applications beyond EuroRadio, including EuroBalises to ensure security through safety. By applying a partitioned system principle to ERTMS, we have been able to develop a key distribution scheme which maintains the same level of security in the system, whilst delivering significant benefits for the future.

REFERENCES

[1] GSM-R Functional Group. 2014. *EIRENE System Requirements Specification, version 15.4.0.* Technical Report. European Union Agency for Railways. http://www.era.europa.eu/Document-Register/Documents/P0028D004.3r0.5-15.4.0.pdf
[2] UIC. 2015. UIC ERTMS Projects - UIC. (2015). http://www.uic.org/spip.php?article383
[3] UNISIG. 2015. *SUBSET-037 - EuroRadio FIS, version 3.2.0.* Technical Report. European Union Agency for Railways. http://www.era.europa.eu/Document-Register/Documents/SUBSET-037%20v320.pdf
[4] UNISIG. 2015. *SUBSET-114 - KMC-ETCS Entity Off-line KM FIS, version 1.1.0.* Technical Report. European Union Agency for Railways. http://www.era.europa.eu/Document-Register/Documents/Set-2-Index079-SUBSET-114%20v100.pdf
[5] UNISIG. 2016. *SUBSET-036 - FFFIS for Eurobalise, version 3.1.0.* Technical Report. European Union Agency for Railways. http://www.era.europa.eu/Document-Register/Documents/SUBSET-036%20v310.pdf