UNIVERSITY OF BIRMINGHAM

School of Computer Science
College of Computer Science FT

MSc. Project

Secure E2EE Chat System Based on Signal Protocol

Submitted in conformity with the requirements
for the degree of MSc. Computer Science
School of Computer Science
University of Birmingham

Ziyan Wang
Student ID: 2014988
Supervisor: Dr Mihai Ordean

September 2020

Declaration

The material contained within this report has not previously been submitted for a degree at the University of Birmingham or any other university. The research reported within this report has been conducted by the author unless indicated otherwise.

Signed .....

Ziyan Wang

MSc. Project
Secure E2EE Chat System

Ziyan Wang

Contents

Table of Abbreviations

- 3DES – Triple DES
- 3G – Third Generation

1 Overview

This paper is a formal analysis of the communication protocols and standards which are used as part of the European Rail Traffic Management System (ERTMS) platform. This report has a particular focus on identifying key components of GSM-R in the context of ERTMS, identifying areas of vulnerability and exposure, and proposing potential solutions for improvement.

1.1 Abstract

The UK Rail Network handled some "1.6 billion journeys ... travelling over 37 billion miles" during 2013-14 (**?**). At present, the UK rail network is reliant on existing infrastructure that dates back to the 1960s (**?**), where signalling is provided through line-side equipment, which relays aspects to the train driver. This, in turn, is interpreted either as a 'Movement Authority' (MA) which gives permission to proceed into the next 'block'* or alternatively an order to stop, should another train occupy the block ahead. One issue with this system is reliability. As the signals are line-side, cable and system failures lead to delays, which impact day-to-day operations.

The current platform for UK rail signalling does not provide an opportunity for necessary growth, as passenger volumes increase, and the need for a human to interpret and react to signals detracts from the potential capacity and speed of a given line. One such example is the West Coast Main Line, where Railtrack, the then-predecessor to Network Rail planned to implement Moving Block signalling, providing line-speeds of up to 140mph. However, due to issues encountered during the project, the existing (unchanged) system was retained, leading to line-speeds being restricted to 125mph. In contrast, in 2015, the Channel Tunnel Rail Link (CTRL/HS1) has line speeds of between 230km/h (approx. 143mph) and 300km/h (approx. 186mph)(**?**) – a considerable increase, due to the use of the TVM and KVB systems, which are cab-based systems, providing signalling and speed information directly to the cab. This, however, has issues with inter-operability where a number of systems are required to operate a train in different countries (**?**).

The solution for these capacity issues, whilst also improving safety and reliability, is ERTMS. This platform, which has four levels of operation, discussed in this report, transforms a line-side signalling system and creates it into a network capable of a 'moving block' system at the highest level. At the core of this system is GSM-R, a rail implementation of the GSM Standard, providing a means for signalling and other line information to flow between the train and the network. This will be reviewed later in this paper. ERTMS also provides a platform for common signalling, allowing rail vehicles to transit between countries seamlessly without the need to switch to a different signalling system, reducing the opportunity for human error.

Whilst ERTMS is largely standardised, it relies on an otherwise open communications channel (GSM) for data-flow. The use of GSM-R within ERTMS adds the provision of a 'safety layer', EuroRadio, and other rail-specific applications. The core focus of this project was to analyse these layers and determine if they provide a secure and trusted medium for communications between ERTMS entities. Through formal analysis of train to trackside communications in ERTMS, potential vulnerabilities were exposed and recommendations made to improve the security of the platform.

1.2 Acknowledgements

The culmination and success of this project would not have been possible without the kind help, wisdom and support of many people, some of whom deserve special mention.

To my Project Supervisor, Tom Chothia, and Joeri de Ruiter for our numerous meetings discussing and mapping extensive specification documents, furthering our understanding of ERTMS and ultimately shaping this project, delivering new concepts to investigate as part of ongoing research.

To my friends, who have listened to the countless ideas to improve security, to make this project unique in many ways, with the hope it will one day make a difference to commuters and rail bodies.

To my family, spending endless hours proof-reading, reading up and following the progression of ERTMS adoption to ensure I did not miss anything during this project. Their patience has been fantastic, and their help is greatly appreciated.

*A 'block', in railway terminology, is a stretch of track on any given line.