Chapter 78
Exploring Cyber Security Vulnerabilities in the Age of IoT

Shruti Kohli
University of Birmingham, UK

ABSTRACT

The modernization of rail control systems has resulted in an increasing reliance on digital technology and increased the potential for security breaches and cyber-attacks. Higher-level European Train Control System(ETCS) systems in particular depend on communications technologies to enable greater automation of railway operations, and this has made the protecting the integrity of infrastructure, rolling stock, staff and passengers against cyber-attacks ever more crucial. The growth in Internet of Things (IoT) technology has also increased the potential risks in this area, bringing with it the potential for huge numbers of low-cost sensing devices from smaller manufacturers to be installed and used dynamically in large infrastructure systems; systems that previously relied on closed networks and known asset identifiers for protection against cyber-attacks. This chapter demonstrates that how existing data resources that are readily available to the railways could be rapidly combined and mapped to physical assets. This work contributes for developing secure reusable scalable framework for enhancing cyber security of rail assets

INTRODUCTION

The Internet of Things (IoT) has evolved rapidly over the last 5 years, bringing with it the promise of low-power, connected devices that are able to monitor themselves and their surroundings. While much of the marketing hype around the IoT has been about consumer devices (connected fridges etc.), much of the standards development has been driven by industrial applications, in particular the need to find low-cost solutions for the monitoring of geographically dispersed infrastructure networks, such as roads, railways, or pipelines. Underpinning the IoT is the integration of a number of existing sensor, actuator and communication technologies; RFID-based identification, wired and wireless sensors, actuator networks (powered values etc.), enhanced communication protocols (4G mobile data etc.), and distributed intelligence for smart objects are just the tip of the iceberg. In industrial contexts, the IoT falls into the category of a Cyber-Physical System. Cyber Physical Systems (CPS) can be defined as system of col-

DOI: 10.4018/978-1-5225-5634-3.ch078

laborating computational elements controlling physical entities, (Pu,2011). A CPS integrates the 3Cs: Computation, Communication and Control, and enables the interaction between the physical world and the cyber world. CPS can provide real-time sensing, dynamic control, information feedback, and other services (Dong *et al*., 2011). The use of IoT technologies as a component of wider CPS has huge potential for impact in many domains. Some representative applications are personalized healthcare, intelligent transportation systems, sustainable environment, and disaster management etc..,(Gupta et al., 2013). They also share significant quality of service requirements,including the need for near real-time performance, continuous availability, high security and privacy of individual's personal data(Pu et al., 2011). Further examples of industrial applications of the IoTinclude cyber-transportation systems (CTS), machine-to-machine (M2M) communications, (Wan et al., 2011).

By increasing the degree of connectivity of everyday devices, the IoT will drive a significant increase in the complexity of many infrastructure-based systems, not least due to the increase in the number of data endpoints the system as a whole will expose to potential threats (Ma et al., 2011). The authenticity and integrity of data being produced via the IoT is therefore a source of great interest within industrial domains, where asset data is the basis of many (potentially costly) real-time decision making processes. This is reflected in the scope of research projects currently investigating IoT topics, whereensuring the cyber security of resultant systems is a real concern, (Suoet al, 2011).

In summary, the IoT offers the rail industry huge potential benefits in terms of ease of monitoring its geographically dispersed infrastructure, vehicles, and operating status (including climatic effects, tresspass etc.); however, it also brings increased risk of cyber-attacks through increasing numbers of devices and data endpoints, communicating over public telecoms networks, and coming from a large number of non-traditional supply chains,(Ma et al. 2011). In this chapter author discusses one potential mechanism for mitigating those risks, through the use of ontology-driven asset monitoring frameworks, tuned to detect cyber-attacks.

NEED OF CYBER SECURITY IN IoT ENABLED SYSTEMS

Cyber security is concerned with the security of cyberspace, a domain that encompasses all forms of networked, digital activities; alongside any actions conducted through digital networks. Traditionally, CPS have been formed around closed networks, and their cyber security has been based on that principle. As the IoT components of these systems expand, the system themselves open up to wider internet, and as a result need to be developed that can fulfil the new requirements around reliability, security and privacy, (Chen et. al.,2012).

Cyber-attacks on CPS have been increasingly in the news in recent years, due to the safety implications of a successful attack against a software system that controls physical infrastructure.One of the most well-known cyber-attack incidents involving a class of CPS known as Supervisory Control and Data Acquisition (SCADA) networks is the attack on Maroochy Shire Council's sewage control system for Queensland, Australia,(Abrams et al.,2008). The attack took place in January 2000, almost immediately after the control system for the sewage plant was installed by a contractor company, the plant experienced a series of problems. It was observed that the pumps were not running when needed, alarms were not being reported, and there was a loss of communications between the control center and the pumping stations, (Rudner et al.,2013). At the beginning, the sewage system operators thought there was a leak in the pipes. At no point did they think that it was an attack. It was only after months of logging that they