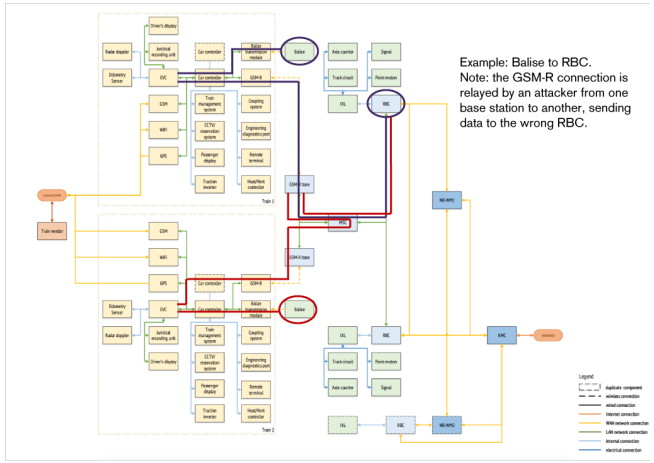
Cyber Security in the Rail Sector – An Integrated Approach

Richard J. THOMAS, Mihai ORDEAN and Tom CHOTHIA
University of Birmingham, Birmingham, UK

The Challenge

Cyber security threat modelling is a critical challenge throughout the rail undertaking

- **Security is usually an afterthought**, where safety and functionality comes first
- **Vague and updated specifications** often lead to threats which impact safety
- **The assumptions made about security are often outdated**, impacting system integrity
- **The requirements of the EU NIS Directive and TS 50701** requires the undertaking to understand cyber security risk to assets and infrastructures
- Asset owners and operators should be able to **reason about the security and safety of their systems** using similar decision-making processes
- **Using legacy systems with known vulnerabilities** threatens the safety and security of the railway
- **How do we find these assets and quantify the threat?**



Example: Balise to RBC. Note: the GSM-R connection is relayed by an attacker from one base station to another, sending data to the wrong RBC.

```
Adversary a1:
[Balise]->[Balise transmission module]->[EVC]:0.32736
[Balise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00016
[Balise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]->[MSC]->
    ->[GSM-R base]->[GSM-R]->[EVC]:0.32747
[SecureBalise]->[Balise transmission module]->[EVC]:0.06591
[SecureBalise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00006
[SecureBalise]->[Balise transmission module]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->
    ->[RBC]->[MSC]->[GSM-R base]->[GSM-R]->[EVC]:0.06597

Adversary a2:
[Workstation1]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]:0.13456
[Workstation1]->[Train vendor]->[Internet Gateway]->[GSM]->[Car BUS]:0.03275
[Workstation2]->[Train vendor]->[Internet Gateway]->[WiFi]->[Car BUS]:0.0313
[Workstation2]->[Train vendor]->[Internet Gateway]->[GSM]->[Car BUS]:0.00762

Adversary a3:
[GPS]->[DAS Display]:0.97222
[GPS]->[Car BUS]->[Passenger display]: 0.9452
[GPS]->[Car BUS]->[EVC]->[GSM-R]->[GSM-R base]->[MSC]->[RBC]:0.00085
```

Acknowledgements: Funding for this paper was provided by the UK's Centre for Protection of National Infrastructure (CPNI) and the Engineering and Physical Sciences Research Council (EPSRC) via the SCEPTICS: A SystematiC Evaluation Process for Threats to Industrial Control Systems project

The SCEPTICS Modelling Tool

The SCEPTICS Modelling Tool applies our **novel** modelling framework to enable asset owners and designers to identify cyber security threats and risks, and prioritise remediation.

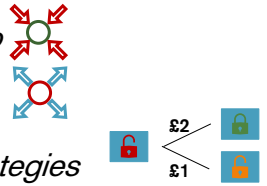
- Leverages the **CVSS Framework** to enable rail engineers to reason about the cyber security of assets and systems
- Enables critical and vulnerable assets to be identified, based on convergence of data, or where there is a high likelihood of an exploit being successful
- Allows asset owners and designers to define cyber security strategies to reduce exposure and risk
- Supports investment-decision making by identifying where the best investments in cyber security can be achieved.

Technical Detail

- Visio-based tool which can reason across architectures (granular to generic)
- Uses Probabilistic-OR and graph-based search techniques to find all paths to and from two points and determine the likelihood of success across the attack path
- Tracks changes of data types (e.g., location into a movement authority) to categorise the severity of the successful attack

Types of Analysis

- *All Roads Lead to*
- *Patient-Zero*
- *Testing New Strategies*



Impact in Practice

We tested the SCEPTICS tool and framework using a model of ERTMS and a reference on-board architecture. The security profiles and outputs were validated by rail sector stakeholders.

Results

The diagram on the left shows two paths found by the tool – the blue one is a genuine balise sending valid data to the train, while the red one shows false balise data being sent to the RBC, potentially leading to an errant Movement Authority being sent.

We also tested what a *secure balise* (one that is authenticated) achieves *(Adversary 1)*, as well as the risks arising from a compromised supply chain partner (*Adversary 2*) and the effect of spoofed GPS (*Adversary 3*) on a train and RBC.

References

Checkoway, S. et al. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. Proceedings of the 20th USENIX Conference on Security (USA, 2011), 6.

Evans, R. et al. 2016. SCEPTICS: A Systematic Evaluation Process for Threats to Industrial Control Systems. (2016).

Hawthorn, A. 2017. A Proven Approach to Requirements Engineering – The Why, What and How of REVEAL.

Download a long-version of the paper and tool at **research.rjthomas.io/wcrr2022-sceptics**