Lewle Sebastian Seneviratne

University of Essex

Research Methods and Professional Practice

Unit 4:

Implementing Cyber Security tools and/or techniques in local road and railway transportation system in Denmark

LITERATURE REVIEW

Introduction

Nowadays, transportation infrastructure continues to expand from isolated nodes to large, interconnected networks enabling “Intelligent & Digitalised Public Transport”. Consequently, cybersecurity is a critical concern, as merging cyber threats will impact the operations of the transport service and the whole economy and potentially the health and safety of citizens (European Union Agency for Network and Information Security, 2015; Ministry of Transport, 2019a).

Firstly, the literature review focuses on technologies deployed in Denmark and covers current technologies and the technologies known to be considered for future deployment in road and railway transportation infrastructure. A review of Danish authorities' existing reports compiles current transportation system deployment with increased dependence on digital solutions (Ministry of Transport, 2019b) and the efficiency of transport services based on time-critical, complex IT systems directly depends on cybersecurity (Mecheva & Kakanakov, 2020; Pizzi, 2020).

Existing reports have focused on threat assessment and implementing effective cybersecurity policies and practices in public transportation management (European Union Agency for Network and Information Security, 2015; Center for Cyber Security, 2021a; Center for Cyber Security, 2021b). In order to investigate effective cyber security techniques and tools, the literature review takes a technical approach and evaluates the current state of technologies used in public transit and their vulnerabilities by reviewing known vulnerabilities discussed in a variety of technical venues and presents the estimated costs of attacks on transit technology when the information is available in the literature.

Background

The transportation subsystem is under the authority of the Ministry of Transport, which is responsible for the sector in general and comprises railway, aviation, roads, and maritime ports. Figure 1 represents the current organisational structure of the Ministry of Transport, Denmark.

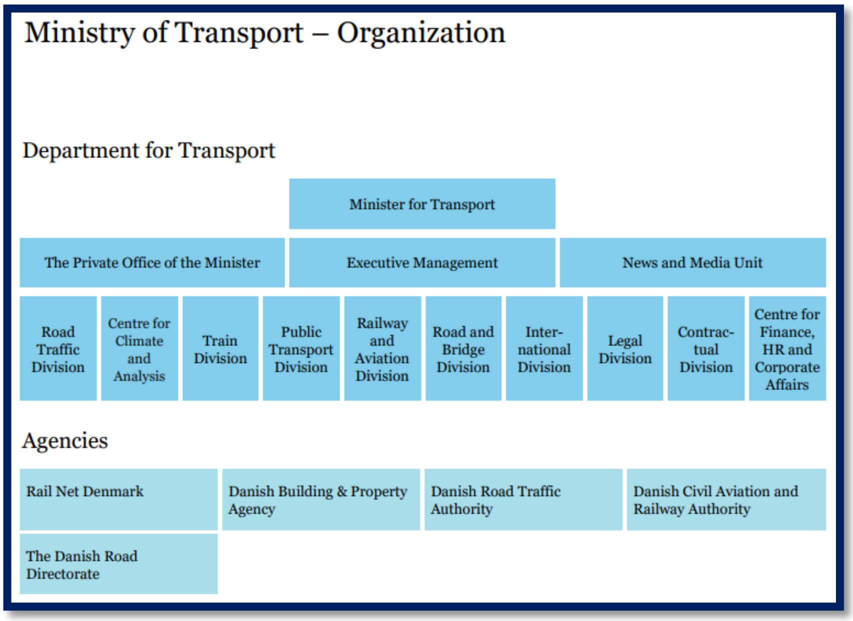
Ministry of Transport – Organization
Department for Transport
Minister for Transport
The Private Office of the Minister
Executive Management
News and Media Unit
Road Traffic Division
Centre for Climate and Analysis
Train Division
Public Transport Division
Railway and Aviation Division
Road and Bridge Division
Inter-national Division
Legal Division
Contrac-tual Division
Centre for Finance, HR and Corporate Affairs
Agencies
Rail Net Denmark
Danish Building & Property Agency
Danish Road Traffic Authority
Danish Civil Aviation and Railway Authority
The Danish Road Directorate

Figure 1: Ministry of Transport – Organization (Ministry of Transport, 2022)

Today, Danish transportation systems have improved their operational and financial processes and services with the deployment of modern computing machines and technologies, such as mobile applications, automatic passenger counters (APC), autonomous vehicle location, connected vehicles (CVs), autonomous vehicles (AVs), and other devices in the field (Ministry of Transport, 2019b). The achieved advantages include improved fleet management, increased ridership and rider satisfaction through bus tracking and other mobile apps, more easily accessible fare payments, and more (Ministry of Transport, Building, and Housing, 2017; Brakewood et al., 2015). These achievements highlight the continued growth in transportation technologies, which have significantly developed from individual nodes to large, interconnected networks of devices in recent years.

In 2018, Danish public transport provider DSB's ticket systems and website were hit by a distributed denial-of-service attack - a DDoS attack, and for hours, travellers could not buy tickets - neither via DSB's app, their website, nor at ticket machines (Valeur, 2018). The cyber-attacks thus showed that the technological threat can become an expensive affair for the Danish transportation system and its vendors and that hackers can hit government institutions that are absolutely vital for maintaining a well-functioning society.

In 2016 ransomware attack against the San Francisco Municipal Transportation Agency in the United States disrupted the agency’s ticketing systems, allowing passengers to ride for free for three days (Brewster, 2018).

Even well-known cyber-attacks keep evolving, and it is crucial to learn how to mitigate these effectively as the transportation sector is a particularly attractive target for adversaries seeking to have a broad impact area, such as extorting money from private companies and public authorities, disrupting operations in the transport sector and potentially undermining client trust.

Reference List

Brakewood, C., Macfarlane, G. & Watkins, K. (2015). The impact of real-time information on bus ridership in New York City. *Transportation Research Part C: Emerging Technologies* 53. DOI: 10.1016/j.trc.2015.01.021.

Brewster, T. (Nov 28, 2016) Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System -- UPDATED. *Forbes*. Available from: https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/?sh=1bd0a1470614 [Accessed 2 April 2022].

Center for Cyber Security (2021a) *The cyber threat against land and air transport*. Available from: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-for-land--and-air-transportation.pdf [Accessed 2 April 2022].

Center for Cyber Security (2021b) *The cyber threat against the Danish aviation sector*. Available from: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-for-aviation.pdf [Accessed 2 April 2022].

European Union Agency for Network and Information Security (2015) *Cyber Security and Resilience of Intelligent Public Transport - Good practices and recommendations*. Available from: https://www.enisa.europa.eu/publications/good-practices-recommendations [Accessed 2 April 2022].

Mecheva, T. & Kakanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems. *Computers* 9(4). DOI: https://doi.org/10.3390/computers9040083.

Ministry of Transport, Building, and Housing (2017) *Reorganisation of the s-bane for driverless operation*. Available from: https://www.trm.dk/media/5oidavkw/final-report.pdf [Accessed 2 April 2022].

Ministry of Transport (2019a) Ny strategi for cyber- og informationssikkerhed. Available from: https://www.trm.dk/nyheder/2019/ny-strategi-for-cyber-og-informationssikkerhed [Accessed 2 April 2022].

Ministry of Transport (2019b) *Strategi for cyber- og informationssikkerhed 2019-2021 i transportsektoren*. Available from: https://www.trm.dk/publikationer/2019/strategi-for-cyber-og-informationssikkerhed-2019-2021-i-transportsektoren [Accessed 2 April 2022].

Ministry of Transport (2022) *Organisationplan for Transportministeriet*. Available from: https://www.trm.dk/media/oqxlpvvw/ministry-of-transport-organization-januar-2022.pdf [Accessed 2 April 2022].

Pizzi, G. (2020) Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment. *Transportation Research Procedia 45*: 250-257 . DOI: 10.1016/j.trpro.2020.03.014

Valeur, J. (May 14, 2018) Sådan blev DSB's billetsystemer lagt ned: DDoS-angreb er internettets brostenskast. *Politiken*. Available from: https://politiken.dk/viden/Tech/art6510622/DDoS-angreb-er-internettets-brostenskast [Accessed 2 April 2022].