**Implementing Cyber Security Controls in Road-Based Intelligent Transportation Systems (ITS) in London, UK**

With the prospect of almost 70% of the global population living in urban areas by 2050 (Cabelin et al., 2021), smart city concepts that utilize technology to facilitate more effective and efficient infrastructure are gaining traction (Vitunskaite et al., 2019). Intelligent Transportation Systems (ITS) form part of this vision and intend to manage increasing problems in existing transportation systems. Challenges with the road network are particularly pressing in London with UK motorists reportedly wasting on average 31 hours in traffic per year and London having the second most congested road network in Europe (Baker et al., 2022). Therefore, the successful development and implementation of road-based ITS initiatives, such as Connected and Autonomous Vehicles (CAV) (TfL, 2019) and Surface Intelligent Transport System (Hanley, 2018), must be ensured. To ensure successful adoption of these initiatives, security and privacy requirements must be suitably addressed (Stamou et al., 2021). This will allow the full benefits of ITS to be realised in London, including reducing journey times, reducing emissions and increasing public safety (Chen et al., 2018). To support these aims, this literature review examines the cyber security controls that have been applied to the ITS use case. As a foundation, the review initially explores the vulnerabilities and threats applicable to ITS to understand the requirement for these controls.

**Vulnerabilities**

The increased connectivity and reliance on technology opens transportation systems up to new cyber vulnerabilities (Vitunskaite et al., 2019). This applies both to the technology itself but also the human factor (Chang & Seely, 2018). There are various components that are core to current and planned ITS concepts in London, including infrastructure, connected vehicles, wireless communications and even mobile applications.

* *Infrastructure:* Vivek & Conner (2022) and Ganin et al. (2019) consider the prioritization of infrastructure components based on their overall impact on the system if disrupted. Whilst they both consider betweenness centrality as a key indicator, this proves to be less effective than other methods, including greedy algorithms. The use of legacy infrastructure, such as old sensors (Shoukry et al., 2018), could become a vulnerable entry point for attacks that could move laterally across the ITS network (Park & Choi, 2020).
* *Connected Vehicles*: The varying levels of automation of vehicles can be considered on a scale, from no automationto fully autonomous (Andraško et al., 2021). This factor influences both the attack surface of vehicles and also the impacts that exploiting a vulnerability could have.
* *Wireless communications*: The concept of open networks in ITS creates a large attack surface. Particularly, the use of message broadcasting can be considered a key vulnerability (Cabelin et al., 2021). Some studies favour a decentralized communication model for communication networks (Baker et al., 2022; Abbas et al., 2021), however some studies believe this increases vulnerability and networks should instead be centralized (Hirtan & Dobre, 2018).
* *Mobile applications*: The use of connected mobile applications to manage ITS interaction for users also introduces various vulnerabilities from the world of mobile security.

**Threats**

Cyber threats to ITS can either be active or passive (Husnoo et al., 2021). They threaten the confidentiality, integrity and availability of these systems (Vijayakumar et al., 2022). Several motivations are considered for these attacks, from selfish drivers wanting clearer roads to data theft for political gain (Cabelin et al., 2021). Transportation systems, including ITS, are considered to be critical infrastructure meaning that the impact of disruption on society would be significant, for example the impacts on public safety and ultimately human life (Stamou et al., 2021). This factor could make ITS an attractive target for attacks but also could make them more difficult to defend given the uptime requirements (Sellitto et al., 2021). Attackers may also target priority components of the system to evoke the highest impact. Due to the infancy of the technology, we currently only have a trivial understanding of the cyber threats to real-world ITS and there are still several unknowns (Chen et al., 2018). Ganin et al. (2019) argues that overall resilience in ITS is key to tackling these unknown threats.

**Controls**

***Prevention***

Preventative controls, particularly authentication, are key to protecting communication between ITS components, including from eavesdropping**,** denial of service (DoS) attacks and unauthorized access by external actors (Eiza & Ni, 2017; Wang et al., 2021). Baker et al. (2022) recommends a lightweight authentication solution that utilizes fog computing and private blockchain. Abbas et al. (2021) similarly recommends private blockchain for its benefits, including immutability and transparency. The standard approach to using consensus in blockchain is not appropriate for real-time systems, however Baker et al. (2022) uses a lookup mechanism to reduce computing overhead and Abbas et al. (2021) uses peer approvals. Asghar et al. (2018) addresses the challenge of scalability in certificate revocation lists (CRL) for public key cryptography based solutions through linking them to a particular vehicle. An anonymous batch authentication mechanism is suggested by Vijayakumar et al. (2022) in order to further reduce the processing burden, protect against insider attacks and provide conditional privacy. Ha et al. (2020) goes a step further in suggesting that ITS authentication should be quantum-resistant, undermining the use of thecryptographic methods in the aforementioned studies. The quantum-resistant lattice-based public key solution proposed also protects against insider attacks, is efficient and could open the door to other security mechanisms, including homomorphic encryption.

Whilst Hirtan & Dobre (2018) suggest the use of symmetric key encryption to support authentication, the majority of papers recommend the use of asymmetric encryption which has the added bonus of providing assurance of the integrity of the messages using digital signatures (Vijayakumar et al., 2022). The literature also explores options that partially use encryption and solutions that replace it altogether. Sfar et al. (2019) leverages game theory in a complementary manner with encryption to limit the computational processing required. Wang et al. (2018) replaces this need altogether, instead using physical controls to defend against attacks. Both are admittedly highly theoretical approaches and could be challenging to implement in a real world ITS. Another option to reduce the strain of cryptographic processing on devices is to offload them to edge devices (Choudhary & Dorle, 2021).

***Privacy***

Data privacy is fundamental to ensuring users trust and adopt ITS services (Husnoo et al., 2021). The vast data generated by ITS systems, including personal data such as location, are not just of interest to malicious actors. Local authorities may use it for investigating accidents and private companies may us it to identify market patterns and opportunities (Andraško et al., 2021). With private industry already heavily involved in the development of ITS in London, these controls are particularly important (Vitunskaite et al., 2019).

Schmittner et al. (2019) suggests ensuring privacy by design to ensure relevant regulations, such as the General Data Protection Regulation (GDPR), are adhered to from the outset. Andraško et al. (2021) promotes the use of data minimization and anonymization in line with existing EU legislation, which is still applicable to the UK. Vijayakumar et al. (2022) uses anonymity in a batch authentication mechanism to protect both user identity and location when using value add services for vehicular ad-hoc network (VANET) vehicles. Husnoo et al. (2021) argues that data anonymization can lead to data loss and does not prevent against data re-identification, so the concept of differential privacy is offered. In support of this, differential privacy is used as a basis for a geo-indistinguishability scheme to protect the location of users (Shi et al., 2019) and even to allow for open sharing of transportation datasets (Asghar et al., 2017). Another theoretical offering in the literature was the use of game theory to balance the risks and rewards of sharing data (Sfar et al., 2019). In a less theoretical approach to user privacy, Hirtan & Dobre (2018) recommend empowering users to define security policies. This approach is scalable, can build trust, and can ultimately encourage users to share more data (Gosman et al., 2018). However, the underlying technology should be abstracted away from the user (Schmittner et al., 2019) and there should be user education to underpin this mechanism (Valentini et al., 2020).

***Detection***

Intrusion detection systems (IDS) are key to protecting ITS through continuous monitoring and real-time response to threats (Eiza & Ni, 2017). The solutions offered in the literature differ in terms of the underlying technology, the attack scope and the hosting location. Due to the various unknowns in ITS, the most popular IDS approach is to use the vast amounts of data to implement anomaly detection, either via a statistical model in Valentini et al. (2020) or most commonly using machine learning techniques (Park & Choi, 2020; Cabelin et al., 2021). Bangui & Buhnova (2021) proposes utilizing deep learning algorithms, such as federated learning, to make the model more lightweight in line with device requirements but ultimately these are unsupervised which can create challenges in critical systems. Vivek & Conner (2022) also recommends an unsupervised machine learning algorithm but this aims at detecting general disruptions in ITS networks as opposed to just cyber-attacks. Chen et al. (2018) offers an information relative approach to reduce overhead and improve accuracy through focusing on the most important data.

Some solutions specifically address a particular attack, for example DoS (Valentini et al., 2020) and false data injection (Cabelin et al., 2021). Others offer a holistic approach to IDS as part of a wider security architecture for ITS. Finally, the majority of the recommended solutions are host-based to ensure availability, however there are also collaborative approaches to IDS available and even the possibility of offloading some of the processing to unmanned aerial vehicles (Bangui & Buhnova, 2021). The variety of IDS solutions proclaimed as successful in the literature may be due to the use of datasets that are of limited relevance and size. The privacy of datasets used for training IDS algorithms is also important and can be preserved by utilizing federated learning (Baker et al., 2022).

Cabelin et al. (2021) uses a data-centric IDS model that includes the concept of trust. Several other solutions focused on trust as being core to ensuring the protection of ITS from malicious communications. Shoukry et al. (2018) recommends a physics-based model that can be used to determine reliable sources of data and propagate trust from a central root. Wang et al. (2021) offers a hierarchal approach to trust that uses blockchain for trust storage and verification. These trust models put significant reliance on reputation and quality parameters should also be used to create a more reliable measure of trustworthiness (Gosman et al., 2018).

***Regulation***

Attempts to regulate cooperative ITS in the EU have been rejected as they were seen as prescriptive and constrictive of innovation which is vital to the development of ITS (Ducuing, 2021). However, the infancy of this technology is not a reason to disregard security standards (Vitunskaite et al., 2019). Any standards and regulations should instead be flexible in their enforcement to allow for controlled innovation. Whilst specialized ITS regulations are in development, the Network and Information Systems (NIS) Directive mandates security provisions for essential services, such as transportation systems, and there are specific guidelines available for securing CAVs (Andraško et al., 2021). High level standards for smart city solutions have been released in the UK, however the security focus is limited and they are not yet enforced. In order to ensure security by design, the UK government must introduce a holistic framework based on flexible security principles for all ITS stakeholders to adhere to.

Some studies regarding holistic approaches to ITS security architecture are predominantly in their preliminary phase and being actively researched in order to support such initiatives (Schmittner et al., 2019; Chen et al., 2018). In addition, Choudhary & Dorle (2021) aims to provide actionable guidance to industry regarding choosing the most suitable security solutions from the various algorithms and models available. Further to the creation and enforcement of standards, Stamou et al. (2021) offers a security assurance framework tailored to ITS with a focus on usability and scalability for real-world use. Sellitto et al. (2021) considers how to overcome challenges with testing large-scale critical systems with the use of cost effective digital twins using an ITS case study. In this way, standards and assurance models can bring the foundation required to tie together some of the disparate security solutions discussed in this paper.

**Conclusion**

ITS has many applications that are being actively explored in London and there are both known and unknown cyber risks that need to be addressed in order for the benefits to be realised. Existing research shows that ITS are being met with automated cyber security controls that incorporate cutting edge technologies, such as artificial intelligence and blockchain. The literature also shows an attempt to get ahead of security challenges through developing controls for future technologies, such as quantum computing. Whilst not all literature considers them, catering for the constraints of ITS devices is key to developing successful controls. Existing research shows coverage of the majority of key functions provided by cyber security controls, however there is limited coverage of response and recovery (NIST, 2018). In addition, most research is focused on CAV so controls for other vulnerable components of the system should be further explored.

References

Abbas, K., Tawalbeh, L., Rafiq, A., Muthanna, A., Elgendy, I., & Abd El-Latif, A., (2021) Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. *Security and Communication Networks* 2021:1–13.

Andraško, J., Hamuľák, O., Mesarčík, M., Kerikmäe, T. & Kajander, A. (2021) Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union. *Sustainability* 13(19): 10610.

Asghar, H., Tyler, P. & Kaafar, M. (2017) Differentially Private Release of Public Transport Data: The Opal Use Case. *Computer Research Repository.*

Asghar, M., Doss, R. & Pan, L. (2018) ‘A Scalable and Efficient PKI Based Authentication Protocol for VANETs’, 2018 28th International Telecommunication Networks and Applications Conference. IEEE.1–3.

Baker, T., Asim, M., Samwini, H., Shamim, N., Alani, M. & Buyya, R. (2022) A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems. *Computer Networks* 203: 108676.

Bangui, H. & Buhnova, B. (2021) Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey. *Procedia Computer Science* 184: 877–886.

Cabelin, J., Alpano, P., and Pedrasa, J. (2021) ‘SVM-based Detection of False Data Injection in Intelligent Transportation System’, 2021 International Conference on Information Networking (ICOIN). IEEE. 279–284.

Chang, K. & Seely, B. (2018) ‘The challenging nexus of technology and security in transportation management center operations’, Proceedings of the Fifth Cybersecurity Symposium. New York, NY, USA: ACM. 1–9.

Chen, Q., Sowan, A. & Xu, S. (2018) ‘A safety and security architecture for reducing accidents in intelligent transportation systems’, Proceedings of the International Conference on Computer-Aided Design. New York, NY, USA: ACM.1–7.

Choudhary, S. & Dorle, S. (2021) ‘Empirical investigation of VANET-based security models from a statistical perspective’, 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA). IEEE.1–8.

Ducuing, C. (2021) Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. *Computer Law & Security Review* 40: 105514.

Ganin, A., Mersky, A., Jin, A., Kitsak, M., Keisler, J. & Linkov, I. (2019) Resilience in Intelligent Transportation Systems (ITS) *Transportation Research Part C: Emerging Technologies* 100: 318–329.

Gosman, C., Cornea, T., Dobre, C., Pop, F. & Castiglione, A. (2018) Controlling and filtering users data in Intelligent Transportation System. *Future Generation Computer Systems* 78: 807–816.

Ha, S., Lee, H., Won, D. & Lee, Y. (2020) ‘Quantum-resistant Lattice-based Authentication for V2X Communication in C-ITS’, 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM). IEEE. 1–8.

Hanley, P. (2018) United Kingdom-London: Data services 2018/S 248-573371. Available from: <https://ted.europa.eu/udl?uri=TED:NOTICE:573371-2018:TEXT:EN:HTML&src=0> [Accessed 5 March 2022].

Eiza, M. & Ni, Q. (2017) Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Vehicular Technology Magazine* 12(2): 45–51.

Hirtan, L. & Dobre, C. (2018) ‘Blockchain Privacy-Preservation in Intelligent Transportation Systems’, 2018 IEEE International Conference on Computational Science and Engineering (CSE). IEEE. 177–184.

Husnoo, M., Anwar, A., Chakrabortty, R., Doss, R. & Ryan, M. (2021) Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey. *IEEE Access* 9:153276–153304.

NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [Accessed 14 March 2022].

Park, S. & Choi, J. (2020) Malware Detection in Self-Driving Vehicles Using Machine Learning Algorithms. *Journal of Advanced Transportation* 2020: 1–9.

Valentini, E., Meneguette, R. & Alsuhaim, A. (2020) ‘An Attacks Detection Mechanism for Intelligent Transport System’, 2020 IEEE International Conference on Big Data (Big Data). IEEE. 2453–2461.

Sfar, A., Challal, Y., Moyal, P. & Natalizio, E. (2019) A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation. *IEEE Transactions on Intelligent Transportation Systems* 20(12): 4405–4414.

Schmittner, C., Chlup, S., Bonitz, A., Latzenhofer, M., Hofer, M., Kloibhofer, C., Raab, T., Spahovic, E. & Doms, T. (2019) ‘Preliminary Considerations for a Cooperative Intelligent Transport System Cybersecurity Reference Architecture’, 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE). IEEE.1–6.

Sellitto, G., Masi, M., Pavleska, T. & Aranha, H. (2021) A Cyber Security Digital Twin for Critical Infrastructure Protection: The Intelligent Transport System Use Case. 230–244.

Shi, D., Ding, J., Errapotu, S., Yue, H., Xu, W., Zhou, X. & Pan, M. (2019) Deep Q-Network-Based Route Scheduling for TNC Vehicles With Passengers’ Location Differential Privacy. *IEEE Internet of Things Journal* 6(5): 7681–7692.

Shoukry, Y., Mishra, S., Luo, Z. & Diggavi, S. (2018) ‘Sybil Attack Resilient Traffic Networks: A Physics-Based Trust Propagation Approach’, 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). IEEE. 43–54.

Stamou, A., Pantazopoulos, P., Haddad, S. & Amditis, A. (2021) ‘Enabling Efficient Common Criteria Security Evaluation for Connected Vehicles’, 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE: 234–240.

TfL (2019) Connected and Autonomous Vehicles: Transport for London, 2019. Available from: <https://content.tfl.gov.uk/connected-and-autonomous-vehicle-statement.pdf> [Accessed 5 March 2022].

Vijayakumar, P., Azees, M., Kozlov, S. & Rodrigues, J. (2022) An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs. *IEEE Transactions on Intelligent Transportation Systems* 23(2): 1630–1638.

Vitunskaite, M., He, Y., Brandstetter, T. & Janicke, H. (2019) Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security* 83: 313–331.

Vivek, S. & Conner, H. (2022) Urban road network vulnerability and resilience to large-scale attacks. *Safety Science* 147: 105575.

Wang, K., Yuan, L., Miyazaki, T., Chen, Y. & Zhang, Y. (2018) Jamming and Eavesdropping Defense in Green Cyber–Physical Transportation Systems Using a Stackelberg Game. *IEEE Transactions on Industrial Informatics* 14(9): 4232–4242.

Wang, X., Garg, S., Lin, H., Kaddoum, G., Hu, J. & Hassan, M. (2021) Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*: 1–10.