The Failure of Trust in Trusted Systems

Angela Mison, Gareth Davies and Peter Eden

University of South Wales, Treforest, UK

Angela.Mison@southwales.ac.uk

Gareth.Davies@southwales.ac.uk

Peter.Eden@southwales.ac.uk

Abstract: Contrary to the early days in which freedom of access and knowledge for all was a fundamental tenet of the burgeoning internet, today, the internet is a hostile environment. This paper represents that practices of trusted autonomous systems and zero trust must reside both organisationally and in any connected device, and that they will be insufficient to secure any hyperconnected system. For example, in the area of Connected and Autonomous Vehicles (CAV), the emphasis of standards associated with cybersecurity is to protect vehicles from an external attack, particularly where it may have an impact on safety. The Internet of Vehicles (IoV) is a subset of the IoT. Security of the IoT has not been standardised and is applied by proprietary organisations. Little consideration has been given to the IoV not being the target of an attack, but a means to an end. Vehicles necessarily communicate with the infrastructure and other vehicles. Additionally, outsourced organisational systems and third-party components within a complex, interconnected, communicating system renders it impossible to define and secure all endpoints. Malware in any part of the hyperconnected systems, provides opportunities for hackers. The security of the systems is only as strong as its weakest link. As an example of an onward attack, a DDOS attack is a debilitating exhaustion of resources attack that disables intended operation of a system. Formation of a botnet from the IoV for use in onward attacks is hypothesised. Such a botnet could have a global reach. Research has indicated that the complete cleansing of a computer-based botnet could take between 5 and 15 years. However, with decentralised command and control and peer to peer communication, the botnet could remain persistent. It is shown that persistent botnet formation software is readily available on the dark market and that specialist software can be commissioned as Crime as a Service. Organised crime groups have already reverse engineered vehicle systems. Mobile attack platform swarms are an attractive proposition to the malefactor, and with the potential for global reach, perhaps the next step on from ransomware. Intermittent disruption from mobile sources is hard to trace and there is an existing pool of 1.2 billion vehicles.

Keywords: IoV, Trusted autonomous systems, zero trust, botnet, DDOS attack platform, cybersecurity

1. Introduction

Contrary to the early days in which freedom of access and knowledge for all was a fundamental tenet of the burgeoning internet, today, the internet is a hostile environment. Hyperconnectivity, resulting from the formation of a system of systems, has introduced major security difficulties, some of which are not covered by trusted autonomous systems or zero trust mechanisms. The example used throughout this paper is that of a vehicle, a device in the Internet of Vehicles (IoV) which itself is a subset of the IoT and also possesses industrial control system attributes (Stouffer, et al. 2015).

Vehicles have intelligent interconnected systems. They are subject to frequent updates by the manufacturer. It is not known, contractually, if third-party components can be updated by their suppliers. Overall, they represent a complex system which has been developed in an evolutionary manner in an attempt to make vehicles safer. It is not necessarily the vehicles that need to be made safer as they are responsible for only 5% of accidents. The systems interconnect and work to mitigate the actions of drivers who are inherently unsafe and directly responsible for 95% of accidents (Office for National Statistics 2021), (Transport Scotland Commdhail Alba 2016), (Rollison, et al. 2018). Each introduction of mitigation increases the complexity and can increase the vulnerability of the overall system.

When considering cyber-attacks and their defence, the emphasis is, inevitably, on defence of the device under consideration and what damage can be done as a result. While system developers think in terms of what a system should do in terms of its requirements specification, hackers think in terms of whether access to one system provides access to another and what those systems can be made to do after access has been gained.

The standards associated with cybersecurity of vehicle systems are designed to protect vehicles from malefactors and to ensure continuing safety (ISO/SAE 2021). Further discussion covers distributed responsibilities and damage scenarios which result in adverse consequences in the context of the vehicle or other road user. The latter is subject to some debate regarding the roles and responsibilities for cybersecurity

and safety. This debate provides a gap through which some considerations may fall. The industry appears to be taking the risk mitigating approach of cyber resiliency engineering (ISO/IEC/IEEE 15288:2015, Systems and software engineering—Systems life cycle processes 2015), (Ross, et al. 2021) for the vehicle itself without considering its potential for weaponisation (Horowitz 2021).

Analysis has been carried out on the potential targets and classes of hacks that might occur, but these are vehicle centric (Ghosh, 2016), With technological advances, other potential attacks have been identified (Guardknox 2021), but again these are vehicle centric. Hackers and criminals gain entry then consider monetisation opportunities (Rajput 2018).

2. Why onward attacks are feasible

Log4j (Mitre Corp e; 2021) has highlighted that zero day vulnerabilities will always represent a weakness in large interconnected systems and prove the maxim that testing shows the presence of errors, never their absence. This vulnerability demonstrated that not all historically developed systems were/are capable of being identified and updated without extensive delay. The view taken here is that the initial failing of cybersecurity may well occur in the manufacturer's system or other permitted communicating system which has been infiltrated by malware and that as a trusted source of coding and updating for its marque or application, has transmitted relevant malware to a vehicle. The vehicle itself has not been subject to attack although this may be done through firmware vulnerabilities (Regenscheid 2018) or Supply Chain vulnerabilities (Boyens, et al. 2021).

From the perspective of a hacker, it is simple to determine that vehicle systems and the context in which they operate are ill-defined, hence the existence of vehicle to everything (V2X) communications' implication that there is an onward attack route and manufacturers may be relying on the filtering security of the receiving system for communications from a vehicle. Spreading throughout the vehicle population outside specific marque and model is hypothetically possible via universally permissible vehicle to vehicle (V2V) communication.

Consider the Internet of Vehicles (IoV) simply as computers on wheels, connected to the internet via V2X. This could enable an almost undetectable source from which to launch an attack as, being mobile, it is likely that any attack would be intermittent, the hardest form of fault to find. It is not necessary to interfere with the vehicles' actual operations, but vehicles could be made to run interference against other external computer operations. The vehicle would still conform to the relevant cybersecurity standards (ISO/SAE 2021) as the vehicle itself is not under attack. Many attacks are possible, as has been demonstrated in the IoT. Lack of consideration of the IoV being a subset of the IoT may have led to complacency as to targets (Heubl 2019), (Matthews 2018) and motivation of malefactors .

3. Legal liability for onward attacks

Using the argument of the IoV as a subset of the IoT, there is potential legal liability for vehicle manufacturers as the US Federal Trade Commission (FTC) report concerning a hack into IoT devices argued that responsibility for security of a device is the responsibility of the manufacturer of the device rather than the owner/user which runs counter to the (ISO/SAE 2021) concept of distributed responsibility. The FTC filed a complaint alleging that an IoT device vendor:

failed to take reasonable steps to protect their [product] from widely known and reasonably foreseeable risks of unauthorized access (US Federal Trade Commission, 2017)

In the settlement of the case (US Federal Trade Commission, 2019) the FTC included the statement:

the settlement includes protections for consumers who currently own devices covered by the order. [The manufacturer] must automatically push fixes to devices set up to receive them and must provide clear step-by-step instructions to all consumers explaining how to patch their devices themselves.

The FTC rulings mark a distinct difference from vehicle manufacturers considering updates to vehicle systems in which there is an attempt to shift liability for non-performance, to the owner/user of the vehicle. There is industry evidence that users (owners/drivers) will prioritise updates for a useful application over a security update. An example was given of response rates to a safety system update versus an automatic parking app

offering. The take up of the parking app was much greater than the safety update, which was deferred. The argument of safety and security -v- convenience, particularly if that safety and security is not directed at the owner/user of a vehicle but to some potential remote and unknown third party, prioritises convenience – a selfish perspective (the-autonomous.com and Infineon 2020). Such procrastination is a *widely known and foreseeable risk* as defined by the FTC and should represent a major concern for manufacturers.

Also, in (the-autonomous.com and Infineon 2020) it was suggested that some parts of the system might not need as much defensive preplanning as others. There is a fundamental flaw in this argument. The primary concerns are that the overarching system itself is not defined, and the longevity of a vehicle. It has been suggested that the lifetime of a car is approximately 20 – 30 years and that vehicle identification numbers (VIN) used for official registration, and manufacturing numbers are reserved for up to 60 years before reuse (National Archives 2021).

4. The need for Fortified Cyber Defence – endpoint protection

The IoT is categorised as a set of devices that have embedded systems that connect to the internet to extend their functionality and to allow firmware to be updated and managed remotely. In a sense it is a class of pervasive computing which includes sensors, communication devices and control mechanisms that can collect data, communicate with users and be remotely controlled (Voas, Laplante and Applebaum 2018). IoT security is considered in (Fagan, et al. 2021)

However notionally complex, a vehicle is a mobile IoT device, which by its very nature is connected to the road transport system infrastructure, other vehicles and the inimical V2X. Vulnerabilities arise from the manufacturer's hyperconnectivity, through the supply chain, Cloud, any app, or any system to which it may be permissibly connected. The lack of current definition means that there is no possibility of enumerating and defending the potentially infinite number of endpoints available for the initial attack. Vehicle access points are a subset of endpoints, whether defined, within the manufacturer's and road transport system's hyperconnected system of which the vehicle is a part. It is not possible to secure and defend something which has no context or system boundaries (Burkacky, et al. 2020).

Discussions of the motivation of malefactors are mainly directed at hacking vehicles, and the reason given for any malware enabling DDOS attacks within the vehicle is given as lack of authentication (SAE International, 2017). As stated previously, within existing standards, opportunity, and liability for attacks in which vehicles are formed into a botnet for onward attacks, e.g. DDOS attack platforms, are not considered.

Drawing from Secure Beyond Breach (Reiber, 2020) and (Burkacky, et al. 2020), the first line of cyber defence is a firewall which, does not present a challenge to the skilled hacker. What is required is hierarchical fortified cyber defence (Dewar 2014). While multifactor authentication may be possible, each level of fortified defence places an additional economic burden on the hacker. The malefactor is having to breach each effective firewall. Unfortunately, each breach permits an assessment, reconnaissance of the internals, the discovery of the networks and systems, enabling the decision regarding the usefulness for offensive e.g. payload delivery, or defensive purposes e.g. kill processes, obfuscation.

5. The need for zero trust – Microsegmentation and API security

Currently, no one programs or builds a vehicle and its systems from scratch. Various parts of the systems and componentry are outsourced. Effectively, it has become a standard supply chain. The componentry is tested, validated, and certified as conforming to specification. The manufacturer has to take that on trust. It is well known that in vehicles comprising millions of lines of code, and third-party components, there will be errors, no matter how carefully and proficiently put together. The manufacturer is dependent on suppliers and their quality systems. Certainly, there are few outright failures, but opportunities for hackers can arise.

Microsegmentation involves the definition of virtual networks according to necessary communication. Any internal virtual network is a microcosm of the complex system. Prevention of incursion by an interloper does not entail consideration of benign or malignant intentions. The environment and operating parameters must be considered in as comprehensive a way as possible (Rose, Mitchell and Connelly 2020). The cybersecurity issues concerning vehicle manufacturers are the identification of interconnections which must be permitted, and the impossibility of defining the potentially infinite endpoints, some of which have been revealed to be in

the componentry (JSOF 2020). The system is not closed with defined entry and exit points. There are concerted efforts to prevent unauthorised access to systems, but having gained access, it can be assumed that hackers have the necessary authority to make external communications via undefined V2X or V2V.

Security at the API, authentication, can be achieved by having operational contours which define acceptable parameter lists, both for functional entry and exit, and which on exit are checked as input with the receiving API. This is still insufficient. There is an argument for random factors to be added to the parameter list which are difficult for a hacker to guess or calculate, but a proposed solution is the introduction of immutable systems with extended parameter list to include pattern of life factors. The implication of this is lack of access to system componentry by third parties, and removal of any on board learning facility, as any change would involve failure to match the pattern of life characteristics. The pattern of life factors could be based on timings, latency, frequency, length of the parameter list, etc. It would render the extended parameter list impossible to guess, and the rate of system updates would limit the temporal window available to hackers.

It is essential to understand that anything done in the cybersecurity and authentication field is at best a deterrent to an incursion, not a guarantee of impenetrability. Its purpose has the benefit of buying time for the defender, during which time, it is hoped that an attack, or precursor, will be detected/noticed/mitigated, and the attacker deterred from onward action. In a real time system, in a vehicle, which has limited onboard resource, incursion may not be recognised until the vehicle fails or its telematics data indicate to the manufacturer that there is a problem. Any active malware may present as a drain on resources. Detection of a problem in the system does not indicate the location of the problem, merely its consequence.

6. Botnets/Thingbots

A botnet is a logical collection of connected devices in which command and control of devices can be exercised by an unauthorised third party. A thingbot, though a term not in very common usage, refers to a botnet of compromised IoT devices. (IBM X-Force® Research, 2017). A botnet is designed to carry out the tasks ordered by the botmaster. By enabling communication from a vehicle, it is possible to use the fleet as a platform for a DDOS attack or any other attack.

With the number of vehicles on the road, the degree of frequent communications between V2X and V2V, and the price of botnets being dependent on their quality and number of infected devices, the arrival of the suggested attack platform is late in coming. This tardiness may be reflective of the protections applied and the complexity of the architecture, given that there is other low hanging fruit in the IoT environment. It may already be present, in the fleet, and if so, its persistence is detrimental.

Botnets are common in criminal usage. There are many botnets for lease in the Dark Market. They are used to commit crimes using someone else's computing or other resources and, depending on how they are encoded, can make it difficult to trace back to the perpetrator. The malware to construct a botnet, including demonstration videos of the malware in action can be found on youtube.com. There are sites in the dark web such as AlphaBay, reputedly closed in 2017 (Dark Web Link, 2019), which approximate to eBay for criminals, where it is possible to purchase the malware of choice for any particular exploit, or to commission same.

A thingbot of compromised vehicles can themselves form the basis of an onward attack, in this instance DDOS is the exemplar. There is a reasonably standard process for creating and growing botnets. Increasingly, Peer to Peer (P2P) protocols are used (Park, Ratzin and van der Schaar, 2011). P2P is a networking mechanism that requires no central server. Multiple links are available between all members of the network. A P2P system would compare version numbers of the botnet and update to the newest version between connected peers leading to the botnet being in a constant state of renewal. The result is resilient and pervasive.

7. Botnet establishment example: dark_nexus

Bitdefender have authored a white paper (Bitdefender, 2020) concerning a new IoT botnet, dark_nexus, influenced by Qbot and Mirai with original core modules. dark_nexus comes from a known malware author and seller, greek.Helios and has been subject to approximately 30 updates in 3 months, dating from December 2019 and March 2020, enhancing its capabilities and robustness.

Although greek.Helios does not appear to offer full Crime as a Service openly, dark_nexus is available for lease on a Dark Market equivalent to eBay from \$20 upwards starting from 2500 seconds (Dark Web Link, 2019). One of the uses of dark_nexus has been DDOS attacks. To date most botnet victims would appear to be in the Far East, Eastern Europe, and Brazil, but with IoT, spread can be global as represented in the Akamai quarterly report (Akamai, 2020), (Akamai a, 2020), (Arghire, 2020).

Hash values for each known version are available, on GitHub as Indicators of Compromise. The rate of versioning would seem to indicate that while older versions may be detected automatically, other detection mechanisms must be used in addition.

Thus far, dark_nexus propagates by brute forcing Telnet protocol, an economically profitable time and effort method for breaching susceptible systems. The botnet has been customised for 12 architectures and its delivery is dynamically configured for the victim system. Inter alia it introduces code enabling SOCKS5 proxy (Leech, et al., 1996) which operates at Layer 5 (Session) over TCP/IP that enables tunnelling and supports IPv6. dark_nexus botnets operate using asymmetric encryption for communications between the device and the C2 server.

dark_nexus incorporates a risk assessment process that identifies other processes which may represent a threat to its existence. It maintains a whitelist of processes and their IDs and terminates processes that cross a threshold value of risk it has calculated. It is thought to do this in order to ensure monopoly control over its botnets, thereby ensuring price stability and control for its author and users.

The development of such software may be a skilled artform, and take much time, but there is no reason to suspect that the economic return on investment by the malware author will not repay any investment of time spent researching the possibilities.

8. Supply chain introduced vulnerability: Ripple20

To emphasise the potential problems associated with the use of third-party components, and supply chain similarities, the example given is that of Ripple20. This extends the concept beyond the IoV and into the national critical infrastructure.

Ripple20 (JSOF, 2020) presents nineteen zero day vulnerabilities in a widely embedded TRECK TCP/IP stack. There have been historical upgrades to the stack, but with the number and age of systems in use, not all the affected stacks will have been patched or upgraded, and differing configurations and collaborations add to the complexity of the issue.

The vulnerabilities identified enable attackers to bypass NAT and firewalls. They permit the undetected control of devices without user interaction. Any communication packets that may result are similar to or are actual valid packets. Resultant traffic may thus appear legitimate. JSOF has demonstrated exploitation of these vulnerabilities on different devices as a proof-of-concept. (JSOF, 2020)

Fifteen of the vulnerabilities have ratings scores ranging between 3.1 and 8.2. Four of the most serious vulnerabilities have a CVSS score >9 and are indicated below:

- CVE-2020-11896 enables remote code execution related to IPv4 tunnelling (Mitre Corp a, 2020).
- CVW-2020-11897 The Treck TCP/IP stack before 5.0.1.35 has an Out-of-Bounds Write via multiple malformed IPv6 packets (Mitre Corp b, 2020)
- CVE-2020-11898 The Treck TCP/IP stack before 6.0.1.66 improperly handles an IPv4/ICMPv4 Length Parameter Inconsistency, which might allow remote attackers to trigger an information leak (Mitre Corp c, 2020)
- CVE-2020-11901 The Treck TCP/IP stack before 6.0.1.66 allows Remote Code execution via a single invalid DNS response (Mitre Corp d, 2020)

A more detailed indication of the vulnerabilities is given in (JSOF, 2020) from which it can be deduced that these vulnerabilities may represent a critical threat to vehicles, resulting in their use as attack platforms, both onward and internally. Some useful mitigation advice is given.

Design reliance on a specific embedded system may render upgrades infeasible, particularly where legacy systems may be involved. There are reports indicating that a full system update can take 5 – 15 years across affected devices before the total population is treated. Many of the systems affected by Ripple20 do not directly contain TRECK TCP/IP stacks, and may not even be connected to the internet, but any resultant infection may have been imported through, or amplified by, the supply chain. (JSOF, 2020).

For an embedded system which is highly defective, widely distributed, highly vulnerable and has been in existence for in excess of twenty years, it is very unlikely that all devices, quoted as in the billions, will or can be updated, which leaves the IoT and the national critical infrastructure with a persistent and potentially pervasive problem, whereby an unknown population of raw devices will not or cannot get the necessary firmware update.

9. Maintenance ramifications and recovery from attack

Although no one can state with any certainty the types and numbers of attacks that may become possible during a possible 60 year lifetime, it is certain that with technological developments some, at least, will become foreseeable. Timeliness of security updates becomes a critical maintenance issue as it may not be possible to update during vehicle operation without disabling the vehicle or leaving the embedded systems and neural networks in consequential unknown states. The problem is exacerbated by differentiated timing of updates leaving an apparent single class of vehicles in a mixed, unknown system state which could lead to incompatibility and inconsistency. A leaf could be taken from the hackers and updates effected through use of a botnet, a copy of the new immutable system, determined by version number, being made to an additional hard drive for update at a convenient time.

If it cannot be demonstrated that manufacturers have developed their systems with due care and consideration of regulations, standards, safety, security, and reasonably foreseeable events, they are likely to fall foul of their insurers and open themselves to class actions. Of particular relevance to manufacturers will be the semantics of the verbs in the standards. The standard SAE J3216 (SAE International, 2020) seeks to provide a common semantics for the industry so that to promote a common understanding. Where a recommended standard's requirement has not been filled, it will be for the courts to decide the reasonableness of that non-performance.

10. Conclusion

Although this paper addresses the potential for onward attacks in the IoV, that potential exists in all IoT systems. With promotion of evermore interconnectedness, the time may have come to consider the way the internet is seen and used. Considered definition of contexts in which the IoV and critical national infrastructure work would enable microsegmentation, the definition of end points, and the ring fencing of operational platforms. Ring fenced, the endpoints are not infinite, but defined by the purpose.

There is a reliance on cyber defence regarding an attack against the vehicle itself, but little consideration to its use as an attack platform. One of the purposes of security by design is to consider what a system can be made to do, not what it was designed to do. Even in this, the perspective tends to the internal. There is never a guarantee in the face of a determined attacker, or against cross infection from a permissible or trusted source.

Security standards lag the development and sale of IoT devices. Existing devices may be infected and persistently so. Both owners and manufacturers may be unaware of the types of infection indicated above. Enthusiasts may exacerbate problems through modifications to their vehicles.

There are techniques which mitigate against such onward attacks but, due to persistence, the opportunities for such may continue in a residual population leading to re-establishment of the botnet. Peer to peer communication is enabled via Vehicle to Vehicle (V2V) communication, essential for collision avoidance and situation awareness, thus it is not amenable to a simple solution. It is not certain at this time how a fleet could be tested and cleansed without simultaneous update of all vehicle systems in existence. Mobility adds to the problems as even if mandated updates are undertaken in one country, crossing a border in a vehicle could reinfect the fleet.

Ripple20 has demonstrated that the supply chain represents a vulnerability to vehicles. Stringent security by design methods should be in place in the manufacture or development of any systems to be deployed in a vehicle and any resulting system approved for release subjected to a security audit. This will not be proof of an inviolate system but should be capable of identification of many vulnerabilities. It is possible that this could be enforced by SLAs and a sharing of potential liability in contractual clauses.

Any resolution needs to consider the Internet of Vehicles, a subset of the IoT, as a botnet, or launch platform for onward attacks. Security by design is a current paradigm. In that process, extended by (Reiber, 2020) there needs to be consideration of what can be done as a launch platform, how to prevent the installation of necessary malware, and how to limit V2X communications. The resolution developed should be generically applicable to all endpoints and capable of scaling to the projected 2.3 Billion vehicles on the road.

Systems evolve, bringing with them their history, and often combining operational and monetisation platforms as a post hoc activity. For vehicles, the monetisation platform profits support the original manufacturing company, and has a knock on effect within third party's asset and fleet management. Perhaps the underlying problem of cybersecurity within the IoT has resulted from growth of surveillance capitalism which has led to platform monetisation and data as a commodity.

References

- Akamai a, 2020. *Your Guide to DDOS Attacks*. [Online] Available at: <https://www.akamai.com/uk/en/resources/ddos-attacks.jsp> [Accessed 23 June 2020].
- Akamai, 2020. *Q4 STATE OF THE INTERNET SECURITY SPOTLIGHT*. [Online] Available at: <https://www.akamai.com/uk/en/multimedia/documents/social/q4-state-of-the-internet-security-spotlight-iot-rise-of-300-gbp-ddos-attacks.pdf> [Accessed 23 June 2020].
- Arghire, I., 2020. *Security Week: Akamai, Amazon Mitigate Massive DDoS Attacks*. [Online] Available at: <https://www.securityweek.com/akamai-amazon-mitigate-massive-ddos-attacks> [Accessed 23 June 2020].
- Bitdefender, 2020. *New dark_nexus IoT botnet puts others to shame*. [Online] Available at: <https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf> [Accessed 20 June 2020].
- Boyens, J. et al., 2021. *Draft (2nd) NIST Special Publication 800-161 Revision 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf> [Accessed 20 December 2021].
- Burkacky, O. et al., 2020. *Cybersecurity in automotive: mastering the Challenge*. [Online] Available at: <https://www.mckinsey.com/~media/mckinsey/industries/automotive%20and%20assembly/our%20insights/cybersecurity%20in%20automotive%20mastering%20the%20challenge/cybersecurity-in-automotive-mastering-the-challenge.pdf> [Accessed 20 December 2021].
- Dark Web Link, 2019. *AlphaBay Dark Web Link*. [Online] Available at: <https://darkweblink.com/alphabay/> [Accessed 24 June 2020].
- Dewar, R., 2014. *The Triptych of Cyber Security: A Classification of Active Cyber Defence*. Talinn, NATO OCD COE Publications.
- Fagan, M. et al., 2021. *NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf> [Accessed 20 December 2021].
- Ghosh, S., 2016. *Automotive Cybersecurity: From perceived threat to stark reality*, Warrendale: SAE International.
- Guardknox, 2021. *Vehicle Hacking is here to stay*. [Online] Available at: <https://www.guardknox.com/vehicle-hacking-connected-vehicles/> [Accessed 20 December 2021].
- Heubl, B., 2019. *How to hack an IoT device*. [Online] Available at: <https://eandt.theiet.org/content/articles/2019/06/how-to-hack-an-iot-device/> [Accessed 20 December 2021].
- Horowitz, M., 2021. *Cybercrime predictions for 2022: Deepfakes, cryptocurrencies and misinformation*. [Online] Available at: <https://www.weforum.org/agenda/2021/11/2022-cybercrime-predictions-checkpoint/> [Accessed 20 December 2021].
- IBM X-Force® Research, 2016. *The inside story on botnets*. [Online] Available at: <https://www.ibm.com/downloads/cas/V3YJYVZX> [Accessed 23 June 2020].
- IBM X-Force® Research, 2017. *The weaponisation of IoT Devices: The rise of the thingbot*. [Online] Available at: <https://www.ibm.com/downloads/cas/6MLEALKV> [Accessed 20 June 2020].
- IEEE, 2015. *ISO/IEC/IEEE 15288:2015, Systems and software engineering—Systems life cycle processes*. [Online] Available at: <https://ieeexplore.ieee.org/document/7106435> [Accessed 20 December 2021].
- Islam, M., Nguyen, G., Pan, R. & Rajan, H., 2019. *A comprehensive Study on Deep Learning Bug Characteristics*. s.l., ACM, pp. 510-520.
- Islam, M., Pan, R., Nguyen, G. & H, R., 2020. *Repairing Deep Neural Network:: Fix Patterns and Challenges*. Seoul, ACM.

- ISO/SAE, 2021. *ISO/SAE 21434:2021 (en): Road vehicles Cybersecurity engineering*. [Online] Available at: <https://www.iso.org/obp/ui/#iso:std:iso-sae:21434:ed-1:v1:en> [Accessed 20 December 2021].
- JSOF, 2020. *Ripple20*. [Online] Available at: <https://www.jsf-tech.com/ripple20/> [Accessed 20 June 2020].
- Leech, M. et al., 1996. *SOCKS Protocol Version 5*. [Online] Available at: <https://www.ietf.org/rfc/rfc1928.txt> [Accessed 4 July 2020].
- Matthews, K., 2018. *Evolution of IoT hacking*. [Online] Available at: <https://www.iotforall.com/evolution-iot-hacking> [Accessed 20 December 2021].
- Mitre Corp a, 2020. *CVE-2020-11896*. [Online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11896> [Accessed 20 June 2020].
- Mitre Corp b, 2020. *CVE-2020-11897*. [Online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11897> [Accessed 20 June 2020].
- Mitre Corp c, 2020. *CVE-2020-11898*. [Online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11898> [Accessed 20 June 2020].
- Mitre Corp d, 2020. *CVE-2020-11901*. [Online] Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11901> [Accessed 20 June 2020].
- Mitre Corp e, 2021. *Search Result log4j*. [Online] Available at: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=log4j> [Accessed 20 December 2021].
- National Archives, 2021. *Part 565 - Vehicle Identification Number (VIN) Requirements*. [Online] Available at: <https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-565> [Accessed 2021 December 2021].
- Office for National Statistics, 2021. *Reported road accidents, vehicles and casualties tables for Great Britain*. [Online] Available at: <https://www.gov.uk/government/statistical-data-sets/reported-road-accidents-vehicles-and-casualties-tables-for-great-britain#contents> [Accessed 20 December 2021].
- Park, H., Ratzin, R. & van der Schaar, M., 2011. *Peer to Peer Networks - Protocols, cooperation and Competition*. [Online] Available at: https://www.vanderschaar-lab.com/papers/chapter_P2P_hpark.pdf [Accessed 20 December 2021].
- Rajput, B., 2018. Understanding Modus Operandi of the Cyber Economic Crime from People-Process-Technology Frameworks Perspective. *Journal of Emerging Technologies and Innovative Research*, March.5(3).
- Regenscheid, A., 2018. *NIST Special Publications 800-193: Platform Firmware Resiliency Guidelines*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf> [Accessed 20 December 2021].
- Rollison, J., Regev, S., Moutari, S. & Feeney, A., 2018. What are the factors that contribute to road accidents? An assessment of Law Enforcement views, ordinary drivers' opinions, and road accident records. *Accident Analysis and Prevention*, Volume 115, pp. 11-24.
- Rose, S., Mitchell, S. & Connelly, S., 2020. *NIST Special Publication 800-207 Zero Trust Architecture*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf> [Accessed 2021 December 2021].
- Ross, R. et al., 2021. *Developing Cyber-Resilient Systems: A systems Security Engineering Approach*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf> [Accessed 20 December 2021].
- SAE International, 2017. *CERTIFICATES AND SIGNATURES: How to Ensure Authentication in the IoT*. [Online] Available at: <https://saemobilus.sae.org/content/TBMG-26489/> [Accessed 24 June 2020].
- SAE International, 2020. *SAE J3216 Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles*, Warrendale: SAE International.
- Stouffer, K. et al., 2015. *NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security*. [Online] Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf> [Accessed 20 December 2021].
- the-autonomous.com and Infineon, 2020. *Virtual Meeting Chapter Event Safety and Security*, s.l.: s.n.
- Transport Scotland Commdhail Alba, 2016. *Article 2 Contributory factors to reported road accidents*. [Online] Available at: <https://www.transport.gov.scot/publication/reported-road-casualties-scotland-2016/article-2-contributory-factors-to-reported-road-accidents/> [Accessed 29 December 2021].
- US Federal Trade Commission, 2017. *FTC sues D-Link over router and camera security flaws*. [Online] Available at: <https://www.consumer.ftc.gov/blog/2017/01/ftc-sues-d-link-over-router-and-camera-security-flaws> [Accessed 20 June 2020].
- US Federal Trade Commission, 2019. *D-Link settlement: Internet of Things depends on secure software development*. [Online] Available at: <https://www.ftc.gov/news-events/blogs/business-blog/2019/07/d-link-settlement-internet-things-depends-secure-software> [Accessed 20 June 2020].
- Voas, J. K. R., Laplante, P. & Applebaum, S., 2018. *White Paper (Draft) : Internet of Things (IoT) Trust Concerns*. [Online] Available at: <https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf> [Accessed 20 December 2021].