UNIVERSITY OF LIMERICK
OLLSCOIL LUIMNIGH

KBS RESEARCH BULLETIN

April 2021
Issue 92

Connected and Autonomous Vehicles: A Cyber-Risk Classification Framework

Barry Sheehan, Finbarr Murphy, Martin Mullins, Cian Ryan.

Introduction and Background

The multiplicity of enabling technologies embedded within connected and autonomous vehicles (CAVs) promises prevention and mitigation of accidents, reduction in greenhouse gas emissions and more efficient utility of energy and infrastructure. With this, the in-vehicle communication network supports an increasing wealth of electronic control units (ECUs), sensors, actuators and interfaces. A primary goal of driver-less vehicles is the reduction of road fatalities predominately caused by human error. However, it is again humans who pose the greatest threat to CAVs. The creators of the enabling technologies may unwittingly create systems with defects or vulnerabilities[1] that allow malicious hackers the opportunity to exploit these vulnerabilities. CAV cyber-risk is of particular concern to insurers, regulators and policing authorities and an appropriate method to risk assessment is required. As vehicles have become functionalised beyond their traditional purpose as a means of transport, the on-board software requirements have risen exponentially. A modern CAV may have approximately 100 million lines of code directing the effective operation of up to 70 ECUs. To put this into perspective, the Windows Vista operating system has only 40 million lines of code, has 905 known vulnerabilities listed in the National Vulnerability Database (NVD), and was exploited in the widescale WannaCry and NotPeyta ransomware cyber-attacks in 2017. Figure 1 illustrates some fundamental cyber-attack types, vectors (or modes) and surfaces. In the absence of connectivity, hackers require physical access to the vehicle to exploit system vulnerabilities. A successful attack of this kind would be confined to a singular vehicle only. However, with CAVs, the connection mechanisms which supports the communication between vehicles and infrastructure, also enables cyber-attacks to be carried out over wireless networks.

The Cyber-Risk Classification Framework

The absence of historical information on cyber-attacks mean that traditional risk assessment methods are rendered ineffective. This paper proposes a proactive CAV cyber-risk classification

[1] A vulnerability is defined as a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity or availability. Mitigation of the vulnerabilities in this context typically involves coding changes but could also include specification changes or even specification (CVE, 2018).

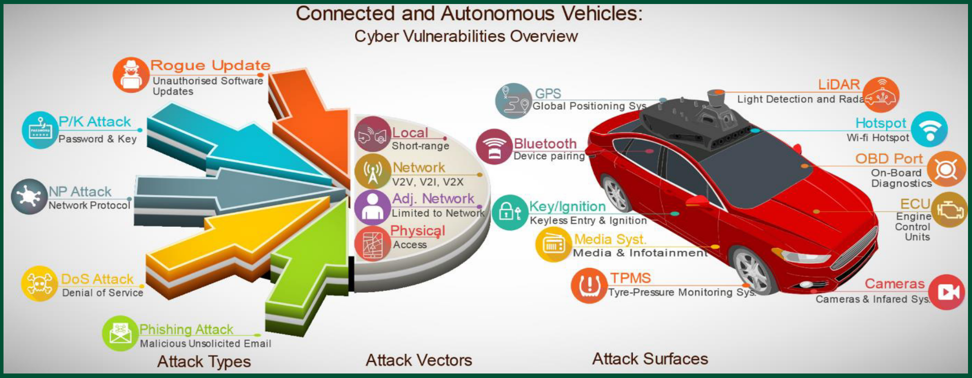


Figure 1: Overview of cyber-attack types, attack vectors (or modes) and CAV attack surfaces

As a leading Irish business school in a public university system, KBS is committed to excellence in teaching and to fostering knowledge and understanding of business and society within a diverse, research active and socially engaged environment.

Research at KBS serves this mission. Our goal is to cultivate excellence in research, underpinned by our core values including commitments to promote learning and discovery as well as social responsibility and ethical behaviour; to protect academic freedom and enhance knowledge; to maintain a future orientation and an international perspective; to promote inclusive and sustainable societies and facilitate the involvement of industry.

Our research finds a focus in the four academic departments of the School as well as in active research clusters and broad thematic descriptors. The current research clusters are:

- Accountability (ARC)
- Efficiency & Productivity Analysis
- Emerging Risk Assessment & Underwriting
- Human Rights & Development Practice
- Consumers in Society
- Psychological Science in Business
- Privatisation & PPP
- Quality of Work

Research seminars are also regularly organised by the themes of Work, Knowledge & Employment and Public Policy, Enterprise, Governance & Sustainability.

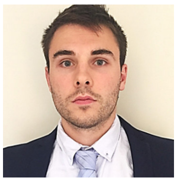
See http://www.ul.ie/business/research for more information.

Authors

Barry Sheehan, Department of Accounting & Finance, Kemmy Business School, University of Limerick, Limerick

Finbarr Murphy, Department of Accounting & Finance, Kemmy Business School, University of Limerick, Limerick

Martin Mullins, Department of Accounting & Finance, Kemmy Business School, University of Limerick, Limerick



Cian Ryan, Department of Accounting & Finance, Kemmy Business School, University of Limerick, Limerick

UNIVERSITY OF LIMERICK
OLLSCOIL LUIMNIGH
Kemmy Business School

model which overcomes this issue by incorporating known software vulnerabilities contained within the US National Vulnerability Database (NVD) into model building and testing phases. This method uses a Bayesian Network (BN) model, premised on the variables and causal relationships derived from the Common Vulnerability Scoring Scheme (CVSS), to represent the probabilistic structure and parameterisation of CAV cyber-risk. The resulting BN model, illustrated in Figure 2, is validated with an out-of-sample test demonstrating nearly 100 % prediction accuracy of the quantitative risk score and qualitative risk level. The model is then applied to the use-case of GPS systems of a CAV with and without cryptographic authentication. In the use case, we demonstrate how the model can be used to predict the effect of risk reduction measures. This model can be used by insurers, vehicle manufacturers and suppliers to classify the risk of CAVs using known system vulnerabilities. It can also be used to forecast future vulnerabilities using scenario analysis. To our knowledge, this is the first application of a probabilistic risk assessment of CAVs cyber systems using a significant data set.

Methodology

A Bayesian Network (BN) model is proposed which utilizes the large collection of known software vulnerabilities stored in the NVD and the standardised CVSS scoring mechanisms to classify cyber-risk for CAV systems. The model is constructed using NVD data in the following steps. First, the graphical structure of the network is learned (i.e., determining the causal relationships). Next, the parameters are learned (i.e., the strength of the causal relationships via the conditional probability tables are determined). An out-of-sample validation test is then performed to examine the model accuracy. Finally, the model is then applied to a proposed CAV GPS system case study.

Relevance of Research Findings to Industry

The motor insurance industry are key stakeholders to the success of CAVs. Insurers are innovation enablers; they can bear the financial risk that underlies all state-of-the-art emerging technologies, particularly in early stages of development. Figure 3 illustrates how autonomous systems may be improving as more autonomous miles are driven. With CAVs, however, technology faults or malicious exploitation by hackers not only present the threat of potentially catastrophic financial loss, but also major commercial reputational damage. Future autonomous vehicles linked to one manufacturer may be susceptible to catastrophic insurance loss since hacking a single vehicle may compromise an entire fleet. The volume and complexity of the sub-systems which comprise a CAV denote the difficulty ahead for insurers to forecast future claims with some degree of accuracy. Motor insurers will be required to adjust their actuarial pricing and underwriting systems as accident liability transfers from the human driver to the CAV technology. It has been projected that the adjustment to autonomous vehicles will generate at least $81 billion in new insurance revenues in the US between 2020 and 2025, with cyber-risk and product liability presenting the greatest opportunity generating $12 billion and $2.5 billion respectively in 2025.

With 250 million connected cars predicted by 2020, the potential for major product recall or liability claims triggered by cyber-attacks or software defects increases. For example, the Jeep Cherokee cyber-attack conducted by researchers initiated the recall of 1.4 million vehicles and at a cost of €761m to the manufacturer, Chrysler. This possibility of highly significant correlation of CAV cyber-attacks could prove a major obstacle for motor insurers in terms of risk-taking capacity and reserving. Therefore, only larger insurers, reinsurers and, indeed, marketplaces such as Lloyd's of London may have the capacity to underwrite CAV cyber insurance in the future. The probabilistic model developed in this research provides insurers with a cyber-risk classification tool, promoting proactive risk assessment as the motor insurance industry shifts to a technology-induced liability regime. The model may be used by insurers to classify the cyber-risk of the CAVs sub-systems and, hence, set underwriting criteria based on the aggregated risk level.

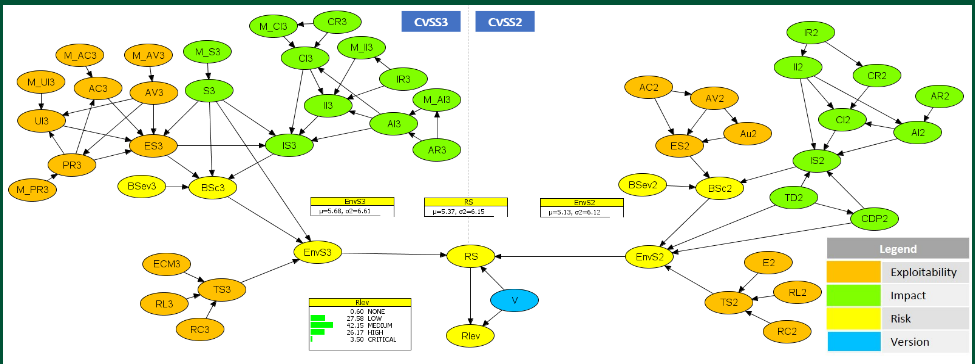
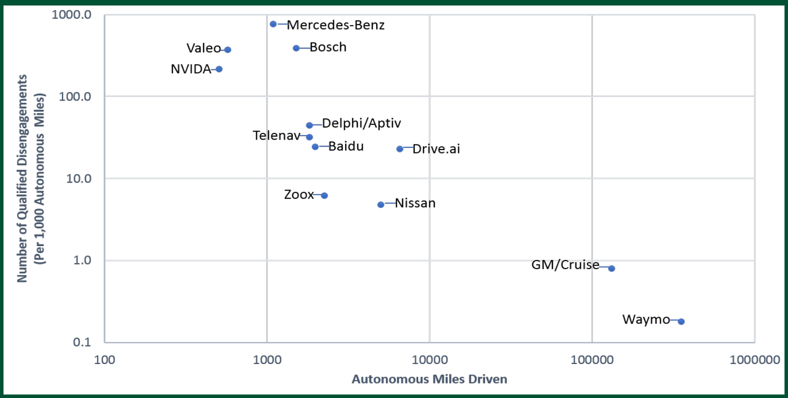


Figure 2: Graphical structure and parameterization of the Bayesian network (BN) CAV cyber-risk classification model. For more detail, see Sheehan et al. (2019)[1].

Figure 3: Number of interventions per 1,000 autonomous miles (log scale) by total driverless miles driven (log-scale) in California between 1st December 2016 (or earlier depending on initial issuance of testing permit) and 30th November 2017 (end of reporting period). Data source: California DMV (2018)



The underlying paper was published in Transportation Research Part A: Policy and Practice, Volume 124, 2019, Pages 523-536, a full copy can be obtained at:
https://doi.org/10.1016/j.tra.2018.06.033

Authors: Barry Sheehan, Finbarr Murphy, Martin Mullins, Cian Ryan.

For further information and comments, please contact:
Dr Deirdre O'Loughlin
Assistant Dean, Research
Kemmy Business School
University of Limerick, Ireland
T: +353 61 213375
E: Deirdre.OLoughlin@ul.ie

Forthcoming Research Bulletin

Title: Are we there yet? Understanding the implementation of re-municipalization decisions and their duration, Public Management Review

Authors: Daniel Albalate, Germà Bel & Eoin Reeves

About the KBS Research Bulletin

The purpose of the KBS Research Bulletin series is to make our research more readily accessible to a wide range of interested stakeholders, and so to allow our work to have a useful impact on the society in which we operate. We regard this as an important part of our stakeholder engagement. The dissemination of these bulletins aligns with both the UL focus on excellence and impact in research, and on the KBS strategic goals of cultivating excellence in research while contributing to our community of stakeholders in a responsible and sustainable manner.

UNIVERSITY OF LIMERICK
OLLSCOIL LUIMNIGH
Kemmy Business School