Human-Centred Vehicle Security

James Nicholson
james.nicholson@northumbria.ac.uk
Northumbria University
Newcastle, UK

ABSTRACT

Connected vehicles – cars connected to the internet – are rapidly becoming the norm in the marketplace. Yet, little work has explored user-centred security implications of such devices. Much like other internet-enabled devices, connected vehicles suffer from new security threats while also being vulnerable to persistent existing security threats. However, unlike other widely-adopted Internet of Things gadgets, connected cars could have serious physical ramifications if compromised, including physical injury or even death. This paper explores some likely threats, with the view of promoting more work around human-centred vehicle security.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

human factors, usable security, autonomous vehicles

INTRODUCTION

Self-driving vehicles – or *autonomous* vehicles – are one of the most hyped and innovated products of the past few years. Promises include better traffic management [13], safer transport [2], and even longer-lasting mobility, e.g. for older users [6].

CHI'19 Workshop on "Looking into the Future: Weaving the Threads of Vehicle Automation", May 2019, Glasgow, UK

Research has focused on sensor technology [2], which of course is pivotal for the concept to function. Some work has also focused on the technical security of the technology (e.g. [1, 17]), which once again is extremely important for autonomous vehicles to gain legislative approval and user acceptance. We must also consider that connected vehicles – those connected to the internet – are becoming more prevalent and these may face some similar issues to autonomous vehicles.

However, little work has focused on the human-centred security issues that could affect these vehicles. After all, they share many similarities to desktop, mobile, and Internet of Things (IoT) devices, where we have observed and experienced clear evidence that bad security practices – or *security hygiene* – endanger the safety of data (e.g. [16]). It is also important to note that while some threats may reflect those of other established technologies, the consequences for autonomous vehicles may be more severe – resulting in possible injury or death.

HUMAN-CENTRED SECURITY ISSUES

The fact that humans bypass computer security measures is by no means a new observation. Decades of research has demonstrated how users continue to create poor passwords [12], fall for fake emails [14], and fail to update their software despite multitudes of research in this area, and the efforts put in place by government and organisations in educating users [4]. Of course, in many situations the procedures or systems are not fit for purpose, despite being technically secure. Below I cover some key usable security problems that have plagued computer systems in the past, and that are likely to translate to autonomous vehicles.

Software Updates

Connected and autonomous vehicles will need to be patched in order to prevent attackers from exploiting software vulnerabilities. Computer users notoriously avoid updating their software for a variety of reasons, including ignorance, inconvenience, and fear [4, 10, 15]. In some contexts, such as internet routers or some IoT devices, firmware or software may never be updated.

While the update cycle for connected and autonomous vehicles may be less regular than those for other systems (assuming a higher quality control), users will likely still be required (perhaps by law [7]) to authorise the installation of such updates. In addition to the avoidance reasons cited above, drivers may be even less motivated to update their machines due to (i) needing the vehicle again in an unplanned manner and/or (ii) fear of the update 'bricking' their machine and thus being unable to travel (e.g. to work).

This avoidance behaviour may be exacerbated even more by the fact that vehicles should only be updated when not in use and when parked in a trusted location – i.e. in a driveway or outside the house. Out of sight, out of mind. It is unlikely that vehicles will be updated when inactive in transitional locations – e.g. parked at work or in a shopping centre.

User Authentication

User authentication will be vital for smart and autonomous vehicles – after all thieves should not be able to bypass the authentication mechanisms any easier than the current methods (i.e. physical keys). In fact, wireless keys – a recent innovation – have been shown to be less secure than traditional keys by being vulnerable to Signal Amplification Relay Attacks [8].

The introduction of wireless keys suggest a movement away from traditional keys. However, new methods must take into consideration known human behaviours. For example, recent trends appear to suggest that smartphones may serve as the authentication hub. While maintaining a token is desirable (we do not want users forgetting their secret codes and being unable to travel!), drivers' security hygiene should be considered – specifically smartphone owners' usage of weak passcodes, reusing passcodes, or even not bothering with passcodes at all [5]. We also have to take into consideration users' negative attitudes towards two-factor authentication in part due to the reliance on extra hardware [3].

Authentication mechanisms specific to vehicles should also be considered, with the caveat that even more time pressures and distractions apply when compared with traditional settings.

Social Engineering

Social engineering continues to be an effective attack vector for traditional computer communications (e.g. [11]). This trend – attackers targeting users rather than attempting to bypass technological measures – will most likely translate to connected and autonomous vehicles. A probable scenario would be deceiving drivers to open compromised messages that can hijack the vehicle – after all users in a driving context are more likely to be distracted, and the UI of the vehicle screens may not lend itself to effective cue identification (e.g. [9]). Social engineering tactics designed to deceive users into granting an attacker physical access to the vehicle itself should be considered, for example attacks that rely on distracting users while in authentication range.

CONCLUSIONS

In this paper, I have presented some likely human-centred security threats that could target connected and autonomous vehicles. While the threats themselves are prevalent in our existing devices, these are likely to be amplified by the context of connected and autonomous vehicles.

REFERENCES

[1] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine* 53, 6 (2015), 126–132.

[2] James M Anderson, Kalra Nidhi, Karlyn D Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A Oluwatola. 2014. *Autonomous vehicle technology: A guide for policymakers*. Rand Corporation.

[3] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L Jean Camp. 2018. A qualitative study on usability and acceptability of Yubico security key. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. ACM, 28–39.

[4] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. 2015. A study of usersâĂŹ experiences and beliefs about software update messages. *Computers in Human Behavior* 51 (2015), 504–519.

[5] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4806–4817.

[6] Corey D Harper, Chris T Hendrickson, Sonia Mangones, and Constantine Samaras. 2016. Estimating potential increases in travel with autonomous vehicles for the non-driving, elderly and people with travel-restrictive medical conditions. *Transportation research part C: emerging technologies* 72 (2016), 1–9.

[7] Michael Inners and Andrew L Kun. 2017. Beyond liability: Legal issues of human-machine interaction for automated vehicles. In *Proceedings of the 9th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. ACM, 245–253.

[8] Hyera Jeong and Jaewoo So. 2018. Channel correlation-based relay attack avoidance in vehicle keyless-entry systems. *Electronics Letters* 54, 6 (2018), 395–397.

[9] James Nicholson, Lynne Coventry, and Pam Briggs. 2017. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 285–298.

[10] James Nicholson, Lynne Coventry, and Pam Briggs. 2018. Introducing the cybersurvival task: assessing and addressing staff beliefs about effective cyber protection. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 443–457.

[11] Wombat Security. 2019. *2019 State of the Phish Report*. Technical Report. Wombat Security.

[12] Chao Shen, Tianwen Yu, Haodi Xu, Gengshan Yang, and Xiaohong Guan. 2016. User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security* 61 (2016), 130–141.

[13] Alireza Talebpour and Hani S Mahmassani. 2016. Influence of connected and autonomous vehicles on traffic flow stability and throughput. *Transportation Research Part C: Emerging Technologies* 71 (2016), 143–163.

[14] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. 2017. Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1421–1434.

[15] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of software updates: The process of updating software. In *Proceedings of the 2016 chi conference on human factors in computing systems*. ACM, 3215–3226.

[16] Ryan West, Christopher Mayhorn, Jefferson Hardee, and Jeremy Mendel. 2009. The weakest link: A psychological perspective on why users make poor security decisions. In *Social and Human elements of information security: Emerging Trends and countermeasures*. IGI Global, 43–60.

[17] Eray Yağdereli, Cemal Gemci, and A Ziya Aktaş. 2015. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation* 12, 4 (2015), 369–381.