Privacy Implications of Smartphone-Based Connected Vehicle Communications

Greig Paul
Department of Electronic
& Electrical Engineering
University of Strathclyde
Glasgow, UK
Email: greig.paul@strath.ac.uk

Darshana Thomas
Department of Electronic
& Electrical Engineering
University of Strathclyde
Glasgow, UK
Email: darshana.thomas@strath.ac.uk

James Irvine
Department of Electronic
& Electrical Engineering
University of Strathclyde
Glasgow, UK
Email: j.m.irvine@strath.ac.uk

***Abstract*—Considerable work has been carried out into making the vision of connected vehicles a reality, with inter-operable communications to take place between vehicles for the purpose of improving road safety and alerting road users to accidents or sudden braking. The cost of deploying such a solution to large numbers of vehicles is significant, and vehicles have a much longer lifespan than other consumer equipment, leading to other work considering the use of smartphones as possible devices for such connected vehicle networks. In this paper, we consider the security and privacy implications of using smartphone based platforms for connected vehicle applications, both in vehicles, and those carried by pedestrians. We also consider the general risks of relying on consumer smartphones, particularly with regard to the lack of long-term security updates being available. We finally explore the need for privacy to be considered in the design of solutions, in addition to the well-recognised need for security, and explore the trade-off between anonymity and prevention of abuse, in the context of designing future connected vehicle technologies.**

I. Introduction

Considerable research and work has been carried out in the field of connected vehicles [1], particularly with regard to utilising this connectivity to share data between vehicles, thus reducing road-traffic accidents [2] and improving traffic flow [3]. Research has also highlighted concerns with regards to the security of these networks [4]. Despite this, for connected vehicles to benefit as many people as possible, it is necessary to ensure that access to these communications is as close to universal as possible. In [5] and [6], the need for pedestrians to be included in collision-avoidance solutions is considered, and models for the warning of both drivers and pedestrians (via their smartphones) is given.

We expand upon these works, by considering the implications on user privacy when regular smartphones (or platforms derived from these, such as Android Auto [7], intended to introduce Android devices to vehicles) are used. The concept of using Android-based smartphones as communications links for connected vehicles as an interim measure until greater adoption of IEEE 802.11p was proposed in [8]. This approach has clear merit, given that the intended lifespan of a smartphone is significantly shorter than that of a vehicle. This means that, even when connected vehicles become mainstream, there will still be a significant period where many vehicles will not be equipped with this technology, potentially reducing many of the benefits of the technology.

Data transmitted and received by connected vehicles is potentially safety-critical, especially with the advent of autonomous vehicles, and the creation of road trains [9] meaning that driving decisions may be made as a result of input received from other vehicles. The security (namely, the authenticity and reliability) of this data is therefore crucial for both the overall network, and the occupants of the vehicle.

Additionally, a new security challenge is introduced when considering connected vehicle safety applications, namely that of quality of service. The ability for an attacker to even slightly delay the transmission or reception of important signalling data could potentially be as damaging as someone sending false information. Given people are already sufficiently motivated to deliberately cause vehicle collisions for the purpose of claiming insurance money [10], there exists a clear motive for malicious actors to attempt to, for example, delay braking messages, in order to deliberately cause a crash. The ability to interfere with, or delay the transmission of, vehicle-to-vehicle messages, would only aid in carrying out these activities.

II. Smartphone Privacy Considerations

There has been considerable research into the lack of user control over privacy on smartphones in recent years, and indeed work has attempted to rectify these issues, including techniques for privacy-preserving sharing [11], and backwards-compatible optional permissions techniques [12]. Significantly, however, there has been little deployment of user-facing privacy controls on Android handsets. This poses a significant challenge for those attempting to use smartphone handsets for use in connected vehicle environments, where it is possible for other applications to (without the clear consent of the user) choose to gather and centrally store data being transmitted by connected vehicles, as is common in applications today [13]. Indeed, with various methods of ex-filtrating data from an Android-based device [14] capable of bypassing other privacy protection techniques, it is highly likely that any data transmitted through a connected vehicle network could be gathered and transmitted to central aggregation servers, where that data is no longer under the control of the user.

This may have privacy implications for users, particularly given the ease with which sensitive device identifiers (such as IMEI and IMSI numbers) can be accessed and used to uniquely identify an individual handset [13]. If an individual's movements could be correlated together at multiple points, it would be possible for an adversary to potentially build up a record of the movements of other individuals, thus violating their privacy in a large scale.

Additionally, there is considerably fragmentation in the issuance of firmware updates for smartphones. In May 2015, only around 10% of Android devices were running Android Lollipop, the most recent version of Android [15]. This is despite it having been available since November 2014. This is significant, since in a safety-critical application, prompt firmware updates may be needed to address emerging security threats, or to counter-act threats which are seen in the wild. Indeed, over a quarter of Android devices in use as of May 2015 are running on an Android firmware released before June 2012, meaning they lack 3 or more years' worth of security updates. With Android devices typically receiving only a single major version upgrade, prior to their manufacturer ceasing to provide update support (including security updates), there is significant risk to connected vehicles which rely on the security of the individual vehicles concerned. This risk is further exacerbated when one considers the security implications of users not receiving timely and ongoing updates for manufacturer-provided binary drivers, as discussed in [16].

In recent years, Google has started to distribute some key components of the Android operating system through its Play Store, offering app-like updates. Examples of this include their own services framework, and the Chromium-based web view. This is beneficial for the security of consumer-oriented applications on devices, by ensuring devices can receive web browser updates, long after their manufacturer has ceased to provide firmware updates. Within the context of networking pedestrians and vehicles through the use of smartphones, however, this would not resolve the problems of security vulnerabilities within the core frameworks of the operating system (which require a new firmware image to update), the Linux kernel in use on phones, and driver and hardware-specific modifications. In particular, kernel-level exploits give rise to the potential for malicious software to gain root access (if a suitable bypass of SELinux is found), raising the prospect of malicious software being able to interfere with the correct operation of a smartphone application. Similarly, vulnerabilities in outdated drivers (for example, the WiFi drivers) may contain weaknesses which could give rise to attacks or denial of service [16].

III. The Importance of Latency

During transmission of critical data from a connected vehicle (or a smartphone or other device acting as part of this network), even a small additional component of client-side latency may reduce the safety benefits of the system. For example, the window of opportunity to avert an accident between an overtaking and oncoming vehicle may be very small depending on the speeds involved, and would be closely linked to the transmission range between vehicles, and the latency experienced by both vehicles handling the messages. In order to achieve the best possible chance of averting such a collision, it is important that communication latency between vehicles is minimised as much as possible. In particular, the round-trip latency is significant, on account of the need for both parties involved in an exchange to communicate, prior to potential for collision being detected.

By using a device which is not dedicated solely to the secure communication of safety-related data to other vehicles, quality of service issues arise. In order for smartphones to be viably used as part of a vehicle-to-vehicle network, it is necessary for there to be assurances as to how quickly a device will respond to a particular stimulus over the network interface. For example, a smartphone running in deep sleep mode in a pedestrian's pocket would need to be able to wake rapidly, in order to process an incoming alert from a vehicle passing in the road nearby. If this message was not processed in time, the user may not be warned of the imminent danger. Nonetheless, users have an expectation that their smartphone will have low power consumption in sleep, and expect it to be responsive to their own usage.

On account of this, and considering the difficulty in producing a suitably secure approach to retrofitting this to existing smartphone handsets, we suggest it is be unwise to attempt to proceed with using smartphones in a connected vehicle environment, unless there were much stronger (and required) assurances of timely security updates, and guaranteed response times to incoming network messages. This is naturally of particular importance when used in a safety-critical application, such as that of warning people of hazards developing around them in real-time. For a cooperative safety system like that of connected vehicles to work correctly, it is obviously important that third parties should not be put at risk, on account of one user's older smartphone taking longer to respond to incoming requests.

IV. Anonymity in Vehicular Communications

A protocol to allow for anonymity in vehicle-to-vehicle communications is presented in [17]. In particular, the focus on allowing for verifiable integrity and authenticity of messages is given, although this technique relies upon a trusted central authority, which is able to establish the identity of every vehicle present, and is required to issue secure tokens to each vehicle.

The question of whether or not full anonymity is desirable in a connected vehicle environment is one which will no-doubt be debated in the future, although we suggest two key factors to be considered are:

- the maximum harm an anonymous actor can do, and the consequences of this action, balancing the need to trace the perpetrator
- users' desire to travel without being pervasively tracked and monitored at all stages of their journey

While clearly drivers do not currently have full anonymity (vehicles are fitted with registration plates to allow for identification and tracing in the event of their drivers breaking the law), the potential for the mass monitoring of users' movements, either by other vehicles, or by road-side infrastructure, is a concern for users of connected vehicles. Indeed, these concerns are already becoming evident as a result of vehicle makers gathering data from currently available internet-connected cars [18]. A survey by the University of Michigan [19] revealed that 30% of respondents are "very concerned" about security breaches and the risks of their movements being tracked, and that a further 37% are "moderately concerned" by this.

It is therefore clear that achieving user acceptance of connected vehicle privacy will be an important factor in increasing adoption of connected vehicle technology, particularly if that technology is opt-in, through the voluntary installation of a piece of software on their smartphone.

By offering users controlled a form of anonymity against pervasive identification by other drivers or actors, privacy can be preserved, albeit at the increased risk of potential attacks, whereby malicious users may invent new identities, in order to flood an area with invalid reports (thereby warning other cars of false risks of collision). This is an ongoing challenge, which is common in decentralised technologies, where there is little barrier-to-entry for new users of a platform [20]. On the other hand, if the risk posed by malicious users cannot be mitigated, greater assurances of the origin of messages on inter-vehicle networks may prove necessary.

V. Conclusion

Inter-connected vehicles remain a popular ongoing research project, with many proposals having been made to accelerate development and deployment through the use of consumer smartphones as the network-connected nodes for vehicles and pedestrians. We highlighted a number of concerns with this approach, particularly around the security and privacy of user data, and the risks of pervasive surveillance of data gathered by smartphones, both by the operators and providers of such software, and by other applications on smartphones. We also highlighted the potential risks of using general-purpose smartphones in time-critical operations concerning the safety of individuals, as well as the trade-off between anonymity of users, and the ability to detect malicious users having created new identities to generate false messages on an inter-vehicle network.

Acknowledgment

This work was partly funded by EPSRC Doctoral Training Grant EP/K503174/1.

References

[1] E. Uhlemann, "Introducing connected vehicles [connected vehicles]," *Vehicular Technology Magazine, IEEE*, vol. 10, no. 1, pp. 23–31, March 2015.

[2] M. Ashrafi, S. Yousefi, H. Karimi, S. Hosseini, H. Rostami, and H. Ataeian, "Highway chain collision avoidance using inter-vehicular communications," in *Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on*, Oct 2013, pp. 135–140.

[3] Q. Jin, G. Wu, K. Boriboonsomsin, and M. Barth, "Improving traffic operations using real-time optimal lane selection with connected vehicle technology," in *Intelligent Vehicles Symposium Proceedings, 2014 IEEE*, June 2014, pp. 70–75.

[4] K. Han, S. Divya Potluri, and K. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," in *Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on*, April 2013, pp. 160–169.

[5] T. Hwang, J. Jeong, and E. Lee, "Sana: Safety-aware navigation app for pedestrian protection in vehicular networks," in *Information and Communication Technology Convergence (ICTC), 2014 International Conference on*, Oct 2014, pp. 947–953.

[6] X. Wu, R. Miucic, S. Yang, S. Al-Stouhi, J. Misener, S. Bai, and W. hoi Chan, "Cars talk to phones: A dsrc based vehicle-pedestrian safety system," in *Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th*, Sept 2014, pp. 1–7.

[7] (2014, June) Android Auto. Google Inc. Retrieved 18 May 2015. [Online]. Available: http://www.android.com/auto/

[8] K.-C. Su, H.-M. Wu, W.-L. Chang, and Y.-H. Chou, "Vehicle-to-vehicle communication system through wi-fi network using android smartphone," in *Connected Vehicles and Expo (ICCVE), 2012 International Conference on*, Dec 2012, pp. 191–196.

[9] E. Coelingh and S. Solyom, "All aboard the robotic road train," *Spectrum, IEEE*, vol. 49, no. 11, pp. 34–39, November 2012.

[10] V. Ward, "Woman killed in gangs car crash to earn insurance cash," *The Telegraph*, February 2013.

[11] E. De Cristofaro, A. Durussel, and I. Aad, "Reclaiming privacy for smartphone applications," in *Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on*, March 2011, pp. 84–92.

[12] G. Paul and J. Irvine, "Achieving optional Android permissions without operating system modifications," in *81st Vehicular Technology Conference (VTC2015 Spring)*. IEEE, May 2015.

[13] A. Short and F. Li, "Android smartphone third party advertising library data leak analysis," in *Mobile Ad Hoc and Sensor Systems (MASS), 2014 IEEE 11th International Conference on*, Oct 2014, pp. 749–754.

[14] J.-F. Lalande and S. Wendzel, "Hiding privacy leaks in android applications using low-attention raising covert channels," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Sept 2013, pp. 701–710.

[15] (2015, May) Dashboards - Android developers. Google Inc. Retrieved 18 May 2015. [Online]. Available: https://developer.android.com/about/dashboards/index.html

[16] X. Zhou, Y. Lee, N. Zhang, M. Naveed, and X. Wang, "The peril of fragmentation: Security hazards in android device driver customizations," in *Security and Privacy (SP), 2014 IEEE Symposium on*, May 2014, pp. 409–423.

[17] N. Rabadi and S. Mahmud, "Drivers' anonymity with a short message length for vehicle-to-vehicle communications network," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*, Jan 2008, pp. 132–133.

[18] (2013, March) Web-connected cars bring privacy concerns. Washington Post. Retrieved 18 May 2015. [Online]. Available: http://www.washingtonpost.com/business/technology/web-connected-cars-bring-privacy-concerns/2013/03/05/d935d990-80ea-11e2-a350-49866afab584_story.html

[19] B. DeGroat. (2014, April) Connected vehicles: Concerns about security, privacy. University of Michigan. Retrieved 18 May 2015. [Online]. Available: http://ns.umich.edu/new/releases/22114-connected-vehicles-concerns-about-security-privacy

[20] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the sybil attack," *University of Massachusetts Amherst, Amherst, MA*, 2006.