Poster Abstract: Cyber-Physical Security for Smart Cars – Taxonomy of Vulnerabilities, Threats, and Attacks

Abdulmalik Humayed and Bo Luo
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS 66045, USA
{ahumayed,bluo}@ku.edu

ABSTRACT

As the passenger vehicles evolve to be "smart", electronic components, including communication and intelligent software, are continuously introduced to new models and concept vehicles. The new paradigm introduces new features and benefits, but also brings new security concerns.

Smart cars are considered cyber-physical systems (CPS) because of their integration of cyber- and physical- components. In recent years, various threats, vulnerabilities, and attacks have been discovered from different models of smart cars. In the worst-case scenario, external attackers may remotely obtain full control of the vehicle by exploiting an existing vulnerability. In this poster, we examine smart car security from a CPS' perspective, and derive a taxonomy of threats, vulnerabilities, and attacks. We demonstrate a systematic model of smart car security by distinguishing between cyber, cyber-physical, and physical (C-CP-P) components and their interactions. We present our reflections on how the systematic model and taxonomy could be utilized to help the development of effective control mechanisms.

1. INTRODUCTION

Today's smart cars are composed of a significant presence of cyber and intelligent components, such as: intelligent driver assistance, vehicle-to-vehicle (V2V) communication, automated driving, etc. Smart cars are considered a type of CPS, in which components could be categorized as *cyber*, *cyber-physical* and *physical*. In particular, components that directly link with the physical world are physical, including *sensors* that monitor the behavior of a physical component, and *actuators* that control the physical world. Cyber and cyber-physical components are those with communication and computation capabilities realized by software or hardware. The ones with a *direct* interaction with physical components are considered cyber-physical, whereas the others are cyber.

These CPS components are tightly coupled, and many components are commercial-off-the-shelf (COTS) or implemented by third parties. In addition, new technologies with wireless capabilities and physical impacts are also deployed. Manufacturers integrate those components aiming to provide safer and more comfortable driving experiences. However, this interaction result in security issues.

ICCPS '15, Apr 14-16, 2015, Seattle, WA, USA
ACM 978-1-4503-3455-6/15/04
http://dx.doi.org/10.1145/2735960.2735992.

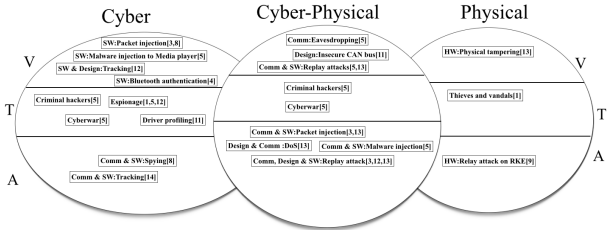

Figure 1: Summary of vulnerabilities (V), threats (T) and controls (C).

With the complex cyber-physical interactions among the heterogeneous components, security becomes difficult to assess, and new security issues arise. In practice, an in-depth understanding of the vulnerabilities, threats and attacks is essential to the development of intrusion detection and defense mechanisms. Thus we propose a security taxonomy for smart cars' vulnerabilities, threats, and attacks from a CPS perspective. It not only systematizes existing knowledge and provides insightful perspectives for smart car security, but also identifies open areas that need more attention, and highlights unsolved challenges.

2. TAXONOMY OF CPS SECURITY FOR SMART CARS

We follow the standard security terminology [5]: (1) *vulnerabilities* are "security weaknesses that might be exploited to cause undesired consequences"; (2) *threats* are sets of "circumstances that potentially cause loss or harm"; and (3) *attacks* are "the exploitation of vulnerabilities by threats".

We show a summary from the CPS perspective in Figure 1. Note that references are in the poster, not in this abstract.

2.1 Vulnerabilities

Causes of Vulnerabilities. *Assumed isolation.* Cars' components are assumed to be isolated, and are not technically ready to be connected to the outside world. Communication capabilities are often added to provide certain functions, without carefully examining the potential security breaches.

Heterogeneity. The heterogeneity of the cars' components

Vulnerability	Type	Cause
TPMS easy interception	CP	H
GPS traceability	C	H
Bluetooth authentication flaw	C	Con
Insecure CAN bus	CP	I, Con
Replay vulnerabilities	CP	I
Communication software flaws	C	Con
Media player exploitations	C	H
Physically unprotected components	P	I

Table 1: Summary of vulnerabilities. C: Cyber, CP: Cyber-Physical, P: Physical; I: Isolation assumption, C: Connectivity, H: Heterogeneity

and the integration of COTS components often introduce security vulnerabilities. The internal details of the integrated components are unknown, and thus their behaviors may be unexpected to the manufacturer.

More connectivity. The new cyber communication capabilities and intelligent features, although intended for improving safety and entertainment, make cars vulnerable to remote attacks. Furthermore, manufacturers tend to prefer remote diagnostics, partly for more convenience and lower cost.

Categorization of Vulnerabilities. The type of a vulnerability is determined by its location: a vulnerability in the Bluetooth is considered cyber, while a TPMS protocol vulnerability is considered cyber-physical. In Table 1, we summarize the vulnerabilities with their *types* and *causes*.
Cyber Vulnerabilities: insecure ECU may allow malwares to be injected, while vulnerabilities are also detected in the Bluetooth authentication mechanism [4].

Cyber-Physical Vulnerabilities: the legacy CAN protocol is insecure by design, it lacks encryption, authentication, and access control, e.g., TPMS messages are easily intercepted.

Physical Vulnerabilities: tampering with physical components may cause cyber or cyber-physical impact, e.g. applying heat to temperature sensors to spoof the thermometer.

2.2 Threats

We analyze threats from five perspectives: *source*, *target*, *motive*, *attack vector*, and *potential consequences*. This provides a systematic description of the threats such that procedures like threat modeling and risk assessment can utilize. We give four examples of typical threats to smart cars.

Criminal hacking (motive). A hacker (source) may target internal ECUs (target) through the vehicles' communication interfaces (vector), and cause collision or inability to control (consequences).

Cyberwar (motive). A hostile nation or terrorists (source) may target national transportation infrastructure and their commuters (target), through fully compromised cars (vector), to cause large-scale collisions and potential critical injuries (consequence).

Espionage (motive). Intelligence agencies (source) may target individuals (target), through exploiting vulnerabilities in traceable GPS components (vector), to obtain the targets' private location information (consequence).

Driver profiling (motive). Companies (source) may seek to obtain drivers' driving habits (target) through analyzing stored information in ECUs (vector), which is a privacy and confidentiality violation (consequence).

2.3 Attacks

A successful attack requires an attacker to get access to the internal network, either physically, through the OBD-II, USB ports, or the media player, or wirelessly, through the Bluetooth or cellular links [1]. A plethora of attack opportunities are open once an attack gains access.

We have surveyed smart cars' attacks in the literature, and categorized them into cyber, cyber-physical, and physical based on the damages' location. Attacks that do not reach sensors/actuators are considered purely cyber, while attacks that directly impact physical components are physical. We present an analysis of the attacks in the poster, while a few examples are provided below.

Cyber Attacks. Attackers could eavesdrop the unencrypted communication from the tire pressure monitoring system (TPMS), and identify vehicles from a unique ID [4].

Cyber-Physical Attacks. Replay attacks could be launched to retransmit (previously captured) legitimate commands and result in undesired consequences [3].

Physical Attacks. Attackers may relay the physical-layer communications between the car and its key fob to allow them to enter and start the car [2].

3. CONCLUSIONS AND REFLECTIONS

In the poster, we present a taxonomy of smart car vulnerabilities, threats and known attacks. We identified the sources of the vulnerabilities and the threat models. Analysis of existing attacks also showed that they fall into the models. Therefore, an effective way of developing control mechanisms to improve smart car security is to eliminate such vulnerabilities. For instance, re-design the protocols or standards to include strong encryption and authentication; eliminate unnecessary and insecure connectivity; introduce IDS and fail-safe mechanisms from the physical-side (or have them isolated from other cyber components).

4. ACKNOWLEDGEMENTS

Bo Luo is supported in part by NSF CNS-1422206 and University of Kansas GRF-2301876. Abdulmalik Humayed is supported in part by Jazan University.

5. REFERENCES

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011.

[2] A. Francillon, B. Danev, S. Capkun, S. Capkun, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *NDSS*, 2011.

[3] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive can networks — practical examples and selected short-term countermeasures. In *SAFECOMP*, 2008.

[4] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC*, pages 11–13, 2010.

[5] C. P. Pfleeger and S. L. Pfleeger. *Security in Computing (4th Edition)*. Prentice Hall PTR, 2006.