CSEP564 : Computer Security : Reading 1

Karuna Sagar Krishna

October 2, 2024

Paper Title

Comprehensive Experimental Analyses of Automotive Attack Surfaces

Paper Authors

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno

Problem

The paper aims to provide a comprehensive security analysis of modern automobiles. Previous literature has narrowly focused on physical threats on the computing units of automobile. These physical threats are downplayed since physical access is needed implying harm can be done without attacking the computing units. The authors argue that computing units in an automobile can be compromised remotely. The authors are also trying to convince the automobile industry that these threats are serious and practical attacks are possible.

Approach

The authors have approached the problem like how a software developer would approach security for software products. The paper starts to define the threat model by describing the various computing units, how they are connected and their inputs/outputs. Using this knowledge, we can identify the various possible threats. The paper shows that there is an internal and external attack surface i.e. internal attack surface enables attacker to leverage vulnerabilities to move across the system and attack other units while external attack surface refers to attacker trying to find gain entry into the system. The paper considers the capabilities of the adversary; specifically, technical and operational capabilities. Technical capabilities refer to the knowledge and tools required to find vulnerabilities that can be exploited. Operational capabilities refer to the adversary's capabilities to mount the attack by delivering malicious inputs which can be categorized as indirect physical, short range wireless and long range wireless attack channels. In order to convince the automobile industry to take these threats seriously, the authors demonstrate real attacks for each operational capability category. To counter the far-fetched argument, the authors describe what it took for them to identify the vulnerabilities, how much did it cost them in terms of time/effort/money, to what extent the attack could cause harm and if these attacks can be detected by its users. Further, the authors point out practical motivation for attacks and the harm that could be caused. The authors go on to suggest various mitigations.

Conclusions

The authors have demonstrated via concrete attacks that modern automobiles have various security and privacy threats which can be exploited remotely. They have established the motivation and cost of mounting attacks. The paper has also shown that once exploited the attacker could be stealth and exfiltrate data and control the automobile. The authors have laid out recommendations for future automobile security and identified the major challenges.

New Ideas

The most interesting idea in this paper is that automobiles are computing systems too. I think most of the population doesn't fully realize this and more importantly neither does the automobile industry. The authors urge automobile industry to learn from security evolution in PC industry.

Another interesting idea is that the paper is pragmatic by not only showing the vulnerabilities and attack surface on a real car, but also how it ties to post compromise control, how the attacker can remain undetected and also the motivation of such an attacker.

Improvements

The paper could have formally drawn a threat model diagram to visually represent the computing units, how they are connected and what data is exchanged between them. As a software developer, I have prior experience with such diagram (Microsoft Threat Modelling Tool). There are many details that such a diagram can surface which might be interesting to an attacker. Since security is as good as the weakest link, such a diagram could be useful to identify the weakest link.

The paper could have also used the STRIDE categories to classify threats, adding to the comprehensive goals of the paper.

The paper could have suggested other security practices found in software industry that could be adopted. For example, security training for car dealership employees and car system developers, penetration and fuzz testing, security certification for cars, security audits and eventing to detect abnormal activities.

New Directions

Though the paper targets modern automobiles, the contents was only focused on cars. A new direction to explore would be mass transport systems (buses, trains, airplanes and ships). I believe the risk on mass transportation systems are higher because they carry more people and such vehicles can cause more damage (think along the lines of 9/11 attack, hijacking, impacting supply chain for various industries).

Within the car industry, self driving cars are emerging and so is the right time to explore security and privacy threats before they become ubiquitous. The paper briefly mentions emerging wireless channels and standards (DSRC, CICAS-V). Future papers could perform security analysis of these standards so that security is ingrained in the standard and design rather than being added during implementation or as an addon.