FASTR

Future of Automotive Security Technology Research

Automotive Cybersecurity Literature Review

AUTHORS

Marcello Balduccini, Hajer Karoui
Drexel University
{mbalduccini, hk476}@drexel.edu

Dan J. Klinedinst
Carnegie Mellon University
djklinedinst@cert.org

Automotive Cybersecurity Literature Review

Introduction

This report presents the processes and outcomes of the Automotive Cybersecurity Literature Review project, in which we reviewed and summarized the state of high-quality research in automotive cybersecurity. The project identified the major kinds of research conducted in automotive cybersecurity, with the ultimate goal of indicating which technologies are underserved, what type of research is underrepresented, and where FASTR should focus its resources. The review was created using an iterative process that included gathering representative sources, building a concept taxonomy, and classifying the collected sources accordingly. Finally, we analyzed the resulting research categories as to the amount and quality of research that has been published in each of them.

Methodology

The methodology we followed for creating the literature review was based on a multi-step process:

1. Paper Collection

At the core of this step was an online search for sources. We used Google and Google Scholar, and also directly searched the archives of high quality venues such as IEEE, ACM, BlackHat etc. The collection process was centered on a set of search keywords. The initial set was seeded with a handful of general keywords such as "Automotive Security Best Practices", and keywords extracted from "Automotive Security Best Practices" [1]. For each source returned, we analyzed the title and abstract for new key terms (in limited cases, we also analyzed the text of the source), and the process was iterated. The papers referred to by the sources were also often analyzed to extract in a recursive fashion.
The content quality of each source was evaluated. Sources determined to describe high-quality research were collected and used in the following steps of the process.

2. Taxonomy Creation

The next step of the process consisted in building a taxonomy of concepts relevant to automotive cybersecurity research. The taxonomy was built bottom-up, starting from concepts found in the sources we had identified in the previous step. Whenever appropriate, more general concepts were introduced in order to form a broad concept hierarchy.

The ultimate goal of the taxonomy is to allow for a systematic classification of the sources found in our literature review, described in the next section. To this purpose, we reviewed source content and concepts in a strategic way, studying economical yet useful ways of organizing key concepts. Our analysis resulted in the identification of three dimensions: Activity, Component, and Access. We identified key terms and established relationships among them, focusing mostly on class-subclass relationships, and associated them with one of the three dimensions. Figure 2.1 illustrates the hierarchy of the Activity category, which generalizes the major types of research activities found in the sources: Attack, Defense, and Analysis. In turn, each of them is divided into concepts at a more granular level, such as Data Exfiltration under Attack. The Component and Access categories were treated similarly and will be discussed in the full presentation.

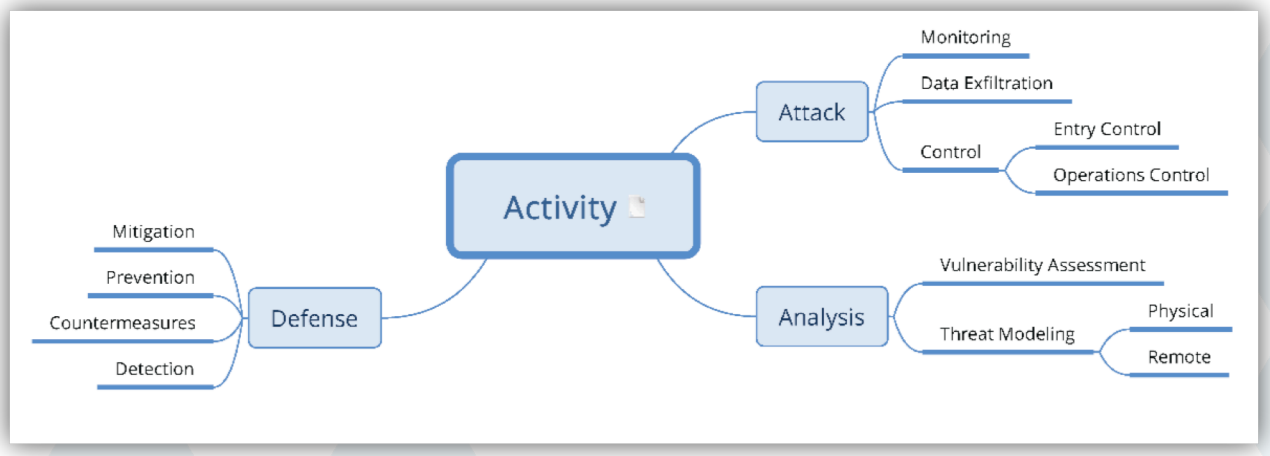

Figure 2.1: Activity Hierarchy

3. Paper Classification

The next step consisted in classifying the papers based on concepts from the taxonomy described in the previous section. The classification occurred along the three dimensions of Activity, Component, and Access discussed in the previous section. As one might expect, the paper-classification and taxonomy-creation steps were highly iterative and mutually guided each other, as the selection of attributes mentioned in each paper was a major key in building and expanding our taxonomy.

The paper-classification process made it possible to describe the content of papers using triples of the form: Activity, Component, and Access. A single paper could describe multiple aspects of the research, in which case multiple triples were used to describe it. This flexible representation could grow beyond triples if further important dimensions were identified. The result of this process was a triple-based paper-classification system, made semantically rich thanks to the hierarchical organization of the concepts used in the triples.

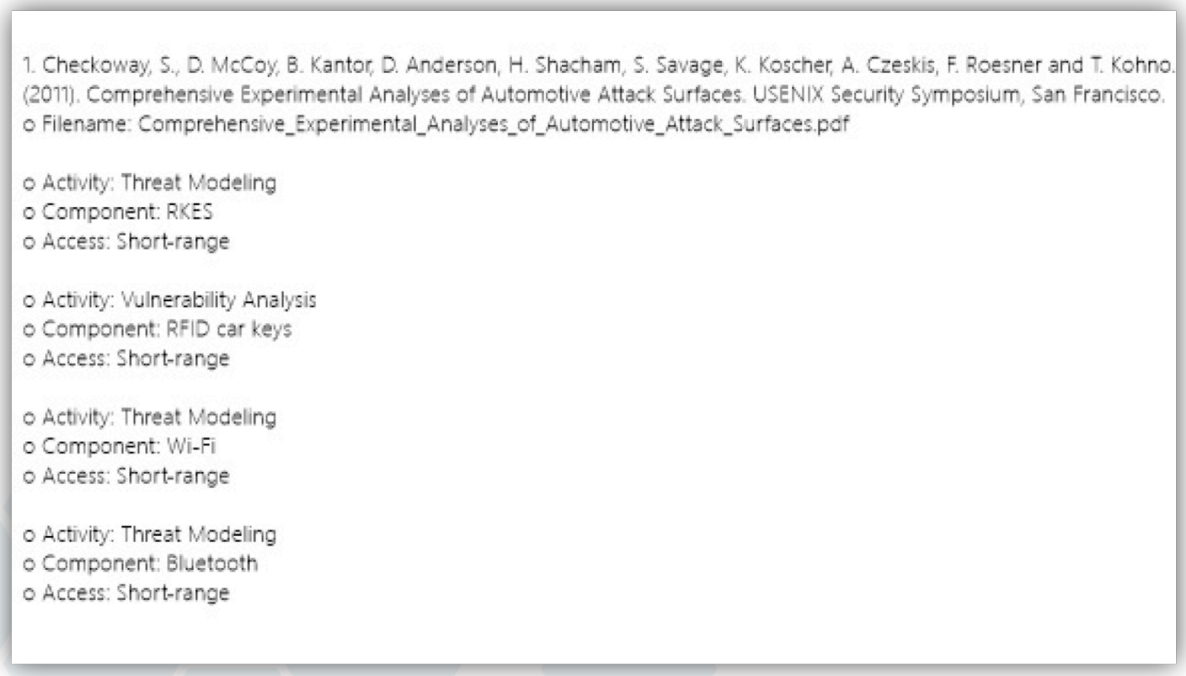

Figure 3.1: Visual Clustering of Sources

Figure 3.1 illustrates the classification of "Comprehensive Experimental Analyses of Automotive Attack Surfaces" [2]. According to our analysis, the paper falls under Threat Modelling and Vulnerability Analysis categories, which, in turn, fall under Analysis in the Activity diagram. The components described in [2] are RKES, RFID car keys, which are subclasses of KeyAccess of the Component hierarchy, and Wi-Fi® and Bluetooth®, both of which fall under Wireless Communications. Because the paper focuses on short-range communications, it was categorized, in the Access dimension, as Remote Access.

Artifacts

Our literature review produced three main artifacts: a database of sources described by triples (61 triples), a concept taxonomy (57 concepts), and a hierarchical, visual clustering of the sources along the three attributes. The artifacts are useful for identifying the state of research in automotive cybersecurity. The use of a taxonomy enables the grouping of the sources according to different dimensions and facilitates the identification of areas in automotive cybersecurity that lack research. Having a hierarchical organization, opposed to a flat organization, yields the ability to group the sources based on increasing levels of abstraction, which, in turn, helps with information visualization.

The hierarchical clustering of the high-quality research, depicted in Figure 4.1, allowed for a practically useful visual grouping of the sources and simplified the task of identifying areas where research is more active versus those where it is less active. A separate clustering was created for each dimension of the classification. Each clustering was obtained by augmenting the concept taxonomy for that dimension by additional nodes, each representing a source. The level of a source node in the hierarchy was determined based on the classification of the source along that dimension. For example, a paper related to the Bluetooth component would result in a source node in the Component hierarchy being added as a child of concept node Bluetooth.

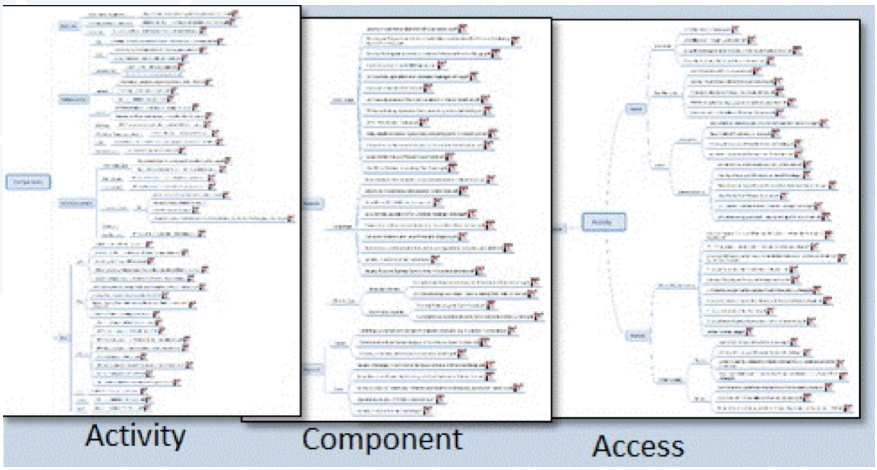

Figure 4.1: Hierarchical clustering of high-quality research

Analysis

Our first avenue of analysis was to examine how the existing research broke down into different categories in the taxonomy. This was strictly an observational approach. We did not attempt to assign any sort of ideal distribution against which we could compare our observations.

The Component and Access hierarchies broke down approximately as we would expect. The Components being researched generally fall into one of two categories: radio frequency (RF) interfaces or the CAN bus. RF interfaces are a prime candidate for attack vectors, as they allow access to the vehicle's internal network without physical access to the vehicle. The CAN bus is a common, often mandatory, network bus in consumer vehicles. These systems are easy to access and widely adopted, so it is unsurprising to find most of the work focused on them. There is less work on network buses other than CAN, such as LIN, FlexRay, and proprietary buses such as GMLAN. There is also relatively little research on cellular interfaces, possibly due to the technical and legal challenges of testing cellular devices and protocols.

The Access hierarchy divides into Remote and Local in proportions that are not equal but are not surprising with this small sample size. In vehicles, Remote and Local indicate actual physical proximity and access. However, they are analogous to remote, network-based attack vectors in traditional computers and local attack vectors (e.g., privilege escalation), respectively. Further, the Remote category is somewhat analogous to a vulnerability and its associated exploitation on traditional computers, while the Local category is analogous to the payload that is executed after exploitation. That is, to gain access to a vehicle (without physical interaction), a researcher has to find a Remote vulnerability and a way to exploit it. The researcher must then perform Local actions to demonstrate that the exploitation was successful and to illustrate the risk of the original vulnerability. In that sense, the ability to send CAN messages to certain ECUs is the vehicular equivalent of a security researcher being able to run "calc.exe" with a Windows exploit.

Analyzing the Activity hierarchy was more interesting. The research to date seems to be weighted toward offensive research (exploitation) and vulnerability analysis. We hypothesize this is because the industry required proof that security vulnerabilities in vehicles were real and exploitable before effort was expended to start developing defenses. Defensive research may also be more likely to be proprietary, as it is often carried out by commercial entities seeking to monetize the results. This is not unlike the pattern of the information security community in general over the past several decades. After vulnerabilities and their impacts began to be demonstrated, more research was done into how to mitigate them, and the industry created technologies such as firewalls, anti-virus software, and more stringent operating-system controls. Although some of the research into vulnerability mitigations is proprietary, it is common to see defensive tools and research at academic conferences such as IEEE Security and Privacy and USENIX Security.

One area where we saw little evidence of public research was the use of more formal methods for verifying security properties of a vehicle or subsystem. In safety-critical software development, it is common to use methods such as model checking or fault-tree analysis to verify code. It is possible these could be used successfully to check security properties, as well. Many subsystems of a vehicle have a finite, albeit large, state space, which is a property that lends itself to symbolic, concrete, or concolic testing.

Our second avenue of analysis was to examine which technologies the research covered. Most of the research targets existing vehicles and systems. Vulnerability analysis and exploitation are based on production-model vehicles, legacy network protocols such as CAN, and current models of onboard computers (ECUs, TCUs, IVIs, etc.) There has been some work on sensors for automated driver assistance systems (ADAS) that are becoming common, such as blind-spot monitoring, adaptive cruise control, and collision avoidance.

Defensive research also focuses on securing the technologies currently in use (the CAN bus and older cellular technologies, for example). Due to the cost of reengineering systems and the long development lifecycle of new vehicles, many defensive approaches consist of adding security to existing systems. Examples include authenticating internal network traffic and adding technologies such as intrusion detection or anomaly detection to the CAN bus.

Overall, little public work has been done on future technologies such as vehicle-to-vehicle and vehicle-to-infrastructure, autonomy and machine learning, and intelligent transportation systems (ITS). It is possible that this type of research is being done in proprietary settings or by people who are not ready to publish their results. However, there is a concern that comprehensive security research on new technologies may lag the market push to deploy them in products. These critical, but potentially underserved, research areas are where we believe FASTR can make the biggest contribution to the state of the practice.

We believe these findings show a need to focus more on the security of emerging and future technologies. Emerging technologies and defensive technologies both seem to be underrepresented in the published literature. While this may continue to be true due to intellectual property issues, we believe it is important to encourage these types of research.

Future Work

By combining the database and the concept taxonomy, we plan to build an ontology that will allow us to ask high-level queries over the multi-dimensional organization of the sources. The ontology will allow the user to get a cross-section of the literature customized according to the user's need. For example, if a user is interested in finding sources related to remote access by means of wireless communications, this will be accomplished by a query on the ontology. Such a query will obviously retrieve sources classified as "Access: Remote" and "Component: Wireless Communications." Thanks to the inference capabilities of ontological reasoning, however, the query will also return additional matches (e.g., sources classified under descendants of wireless communications, such as Wi-Fi, Bluetooth, and cellular).

References

1. Brown, D. A., G. Cooper, I. Gilvarry, D. Grawrock, A. Rajan, A. Tatourian, R. Venugopalan, C. Vishik, D. Wheeler, and M. Zhao (2015). Automotive Security Best Practices.

2. Checkoway, S., D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium, San Francisco.

3. "CONTROL OF EMISSIONS FROM NEW AND IN-USE HIGHWAY VEHICLES AND ENGINES", 40 CFR §86

4. Heitmeyer, C. (2005) Developing safety-critical systems: the role of formal methods and tools. SCS '05 Proceedings of the 10th Australian workshop on safety critical systems and software.

FASTR—Future of Automotive Security Technology Research—is a neutral nonprofit automotive security research consortium working to deliver the actionable applied and theoretical R&D needed now to drive systematic coordination of cybersecurity across the entire supply chain and ensure trust in the connected and autonomous vehicle of the future. For more information, email info@fastr.org

JOIN US!

WWW.FASTR.ORG