Beyond the Dolev-Yao Model:
Realistic Application-Specific Attacker Models for Applications Using Vehicular Communication

Christoph Ponikwar, Hans-Joachim Hof

MuSe - Munich IT Security Research Group
Department of Computer Science and Mathematics
Munich University of Applied Sciences (MUAS), Germany
Email: `christoph.ponikwar@hm.edu,`
`hof@hm.edu`

Smriti Gopinath, Lars Wischhof

Department of Computer Science and Mathematics
Munich University of Applied Sciences (MUAS), Germany
Email: `smriti.gopinath@hm.edu,`
`wischhof@hm.edu`

Abstract—In recent time, the standards for Vehicular Ad-hoc Networks (VANETs) and Intelligent Transportation Systems (ITSs) matured and scientific and industry interest is high especially as autonomous driving gets a lot of media attention. Autonomous driving and other assistance systems for cars make heavy use of VANETs to exchange information.They may provide more comfort, security and safety for drivers. However, it is of crucial importance for the user's trust in these assistance systems that they could not be influenced by malicious users. VANETs are likely attack vectors for such malicious users, hence application-specific security requirements must be considered during the design of applications using VANETs. In literature, many attacks on vehicular communication have been described but attacks on specific vehicular networking applications are often missing. This paper fills in this gap by describing standardized vehicular networking applications, defining and extending previous attacker models, and using the resulting new models to characterize the possible attackers interested in the specific vehicular networking application. The attacker models presented in this paper hopefully provide great benefit for the scientific community and industry as they allow to compare security evaluations of different works, characterize attackers, their intentions and help to plan application-specific security controls for vehicular networking applications.

Keywords–security; attacker model; VANET; V2X; ITS.

I. INTRODUCTION

Vehicular networking applications are a subset of applications used in Intelligent Transportation Systems (ITSs). They typically need security controls, especially, when safety is at stake. For a constructive planning of security controls, it is of benefit to have a model of a typical attacker, a so-called attacker model. Typical attack classes are impersonation, data tampering, sybil attacks, or Denial of Service (DOS) attacks, please refer to [1] for a survey on these attacks. However, these attack classes are very general and their severity differs from application to application. Hence, it is beneficial to have application-specific attacker models for vehicular networking applications. This paper presents vehicular networking applications specific attacker models. These attacker models could be used for security control planning as well as evaluation of security controls. Also, standardized attacker models as in this paper are hopefully a great benefit for the scientific community to compare evaluations of different papers and modeling real world attackers.

This paper is structured as follows: Section II presents related work and shows the gap this paper is closing. Section III gives an overview on vehicular networking applications. Section IV presents a classification of attackers that is used for the application-specific attacker models introduced in Section V. Section VI concludes the paper.

II. RELATED WORK

The field of attack modeling has a long history with some of it rooting in reliability engineering and the vault tree analysis which got adopted and adapted as attack trees [2]–[4] in the realm of secure systems engineering. Because of its detailed and explicit nature the attack tree modeling approach is best suited when goals of an attacker have been elicited and actual mitigation should be developed. The approach taken here categorizes attackers based on different aspects that are derived from their goal, which in return tries to take advantage of a specific vehicular networking application. Others use a game theory based approach to infer intentions, objectives and strategies of attackers [5], we derive these from the vehicular networking application that the attacker tries to exploit.

The often cited Dolev-Yao attacker model [6] models the attacker as an active saboteur. He is omnipotent and can therefore intercept, eavesdrop, or modify all communication of the network. Furthermore, the attacker can pose as a legitimate communication partner and can therefore initiate a communication with every participant in the network. Compromising or breaking cryptographic primitives is not possible for a Dolev-Yao attacker. Networks in an Intelligent Transportation System (ITS) aren't limited to the Internet, instead they consist of Vehicular Ad-hoc Networks (VANET), enabling ad-hoc communication. Cellular technologies, like Long Term Evolution (LTE), can provide connectivity to the Internet. Roadside Units (RSU) or other stationary participants could be connected via traditional electrical or optical wired technologies to other separated networks or the Internet. The Dolev-Yao model is far too imprecise for such a complex networking structure and it only depicts a special type of attacker. This attacker is also unrealistically strong by being omnipotent, which gets increasingly unlikely the more complex and diverse a network becomes. This was previously pointed out in regards to sensor networks [7][8]. Especially, it is pointed out that physical security should not be expected because an attacker can easily get access to those nodes and perform a take over or compromise

cryptographic secrets [7]. In such a way, an outside attacker becomes an inside participating one. To sum it up, the Dolev-Yao model is far too imprecise and unrealistically strong to be of use for security controls planning in realistic vehicular networking scenarios.

A realistic attack scenario is the exploitation of low level software or hardware vulnerabilities in the network stacks of wireless transceivers. The existence and importance of these vulnerabilities has been discussed in various publications, [9]–[12]. This scenario marks the lower bound of attack scenarios that are discussed in this paper. While still being relevant specifically to wireless communication, cellular or ad-hoc, it is also not specific to only one vehicular networking application and the root cause of vulnerable soft- and hardware proliferates through all the layers of current systems and is not specific to wireless communications. Therefore, this is not in focus for this publication. Instead, the main contribution is the combination and extension of previous attacker models by [6][7][13] and the detailed description of realistic attacker models via the extended model. Most of the previous works [14]–[18], are missing realistic attacker models. Some like [15]–[17] use categories of attacks, like impersonation, data tampering, sybil, or DOS attacks and describe each attacker based on its category. [18] is really close to defining realistic attacker models by defining categories of attackers, like driver, road side or infrastructure.

Realistic attacker models are needed to better understand who might be the attacker of a system, for better comparison and ultimately needed to make risk based decisions about whether to implement security controls and how to guard against a specific realistic attacker.

III. Vehicular Networking Applications

A general classification of vehicular networking applications uses two classes: *safety applications* and *non-safety applications*. For realistic attacker models, a more fine-grain categorization is needed. The classes used in this paper are described in the following. Please refer to [1] for a detailed description of the vehicular networking applications.

A. Cooperative Sensing (Safety)

Cooperative Sensing applications use V2X communication for situation awareness, e.g., to reduce risks of accidents while driving.

Road Hazard Signalling (RHS): When a vehicle picks up a standardized condition [19], an application broadcasts these conditions to other recipients using a Decentralized Environmental Notification Messages (DENM) [20]. Conditions include emergency vehicle approaching, slow vehicle, stationary vehicle, emergency electronic brake lights, wrong way driving, adverse weather condition, hazardous location, traffic condition, roadwork, and human presence on the road.

Cooperative Collision Avoidance (CCA): When a vehicle senses a possible collision with an approaching vehicle based on Cooperative Awareness Messages (CAM) [21] received from nearby vehicles, the driver gets a warning. Two distinct collision warning applications has been specified: Intersection Collision Risk Warning (ICRW) (a warning is triggered if a collision is likely to happen at an intersection) and Longitudinal Collision Risk Warning (LCRW) (a warning is displayed to the driver if a front or rear end collision is likely)[22].

B. Cooperative Maneuvering

Applications apply V2X communication for driving automation functions in the levels 3 to 5 as defined in SAE J3016 [23].

Cooperative Adaptive Cruise Control (CACC): To optimize resource usage by forming a convoy or platooning and reducing speed alteration via an extended horizon where minor changes can be leveled out.

Cooperative Merging Assistance (CMA): To avoid collisions vehicles and roadside units (RSU) cooperate and negotiate merging maneuvers.

Cooperative Automated Overtake (CAO): For takeover maneuvers either in a fully autonomous self-driving or a driver assistance scenario, cooperation among vehicles to improve safety is needed.

C. In-Vehicle Internet Access

Internet-based applications are offered to passengers and in distraction reduced versions even to the driver.

D. Mobility Monitoring and Configuration

The status of a vehicle can be remotely queried and modified. This application includes control of auxiliary heating systems as well as software and firmware updates. Usually, the accessed vehicle is in a parked position during the interactions of this application.

IV. Attacker Model

There are already different characteristics for attackers known in literature, some described in the following paragraphs and extended if needed.

Insider Attacker vs. Outsider Attacker [7][13]: An outsider attacker is restricted because he does not participate in regular communication. An insider attacker on the other hand is a regular participant in the communication. A participant could become an insider attacker e.g., when hacked or infected with malware.

Active Attacker vs. Passive Attacker [7][13]: A passive attacker only eavesdrops on communication. An active attacker on the other hand acts in the network, e.g., by creating and inserting messages, by replaying messages, or by modifying existing messages.

Static Attacker vs. Dynamic Attacker [7]: An attacker adapting his behavior based on the behavior of network environment or attack target is called a dynamic attacker. Static attackers on the other hand do not adapt to changes whatsoever. An example of a static attack is the most basic form of malware which doesn't utilize a command and control infrastructure and is build only for a specific purpose, like sending spam. An example of a dynamic attack is an attacker of an Advanced Persistent Threat campaign, which adapts to security measures or changes his goal based on the detected environment around it.

Cooperative Attacker [7] **vs. Individual Attacker**: Attackers colluding to reach a common goal (e.g., destabilization of the network) are called cooperative attackers. An attacker limited to its own abilities is called an individual attacker.

Local Attacker vs. Extended Attacker [13] **extension: Global Attacker** [7]: How much influence an attacker has is an important criteria for the scope and impact a given attack can develop. Limited by his physical abilities, a local attacker can only influence participants in his ad-hoc communication

vicinity. An attacker controlling multiple network segments has the ability to execute more sophisticated attacks that need a greater area of influence. This so-called global attacker has the ability to access every message of the network. But based on the diversity and complexity of ITS network architecture, this type of attacker is limited to the infrastructure providers or to attackers that can influence or execute control over this communication infrastructure.

Malicious Attacker vs. Rational Attacker [7][13] **extension: Opportunistic Attacker**: An indiscriminate attacker who does not care about losses, resource usage, or consequences and targets functionality of participants or the network is called malicious attacker. A rational attacker tries to reach a certain goal by the cheapest means possible and is focused on his benefit or profit. An attacker who only executes an attack when an opportune circumstance occurs is called an opportunistic attacker.

Table I shows the profile matrix based on the attacker characteristics described above that is used in the rest of this paper to describe application-specific attackers.

TABLE I. GENERAL ATTACKER PROFILE MATRIX

Attacker Properties			
Membership:	insider		outsider
Method:	active		passive
Adaptability:	dynamic		static
Organization:	cooperative		individual
Scope:	global	extended	local
Motivation:	malicious	rational	opportunistic

Based on this profile matrix, specific attackers can be modeled. The worst possible attacker is shown in Table II. The worst possible attacker is the most powerful attacker one can think of. As described in Section II for the Dolev-Yao model, such a powerful attacker is quite unlikely to appear in most realistic scenarios (however, there is one valid scenario listed below).

TABLE II. WORST ATTACKER PROFILE MATRIX

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	dynamic		~~static~~
Organization:	cooperative		~~individual~~
Scope:	global	~~extended~~	~~local~~
Motivation:	malicious	~~rational~~	~~opportunistic~~

Table III shows the weakest possible attacker of the application specific attacker model.

TABLE III. WEAKEST ATTACKER PROFILE MATRIX

Attacker Properties			
Membership:	~~insider~~		outsider
Method:	~~active~~		passive
Adaptability:	~~dynamic~~		static
Organization:	~~cooperative~~		individual
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	~~rational~~	opportunistic

The worst attacker and weakest attacker are both ends of the application specific attacker model presented in this paper.

However, in most vehicular networking applications a realistic attacker model lies between the worst attacker and the weakest attacker. The following section presents the realistic attacker models applicable for each vehicular networking application presented in Section III.

V. APPLICATION SPECIFIC ATTACKER MODELS

For each vehicular networking application (see Section III.), different specific attacker profiles are described in this section.

A. Cooperative Sensing (Safety)

Attackers interfering with safety functions are always inadvertently or intentionally risking to cause damage to themselves or other humans besides causing financial damage. It is important to keep this in mind especially when judging about the motivation of a certain attacker.

A perpetrator is stuck in traffic, he then decides to push a button that forces his vehicle to send out false road hazard warnings to influence other vehicles. In an ideal situation for the attacker, the victim vehicles fall for his false claims. He might pose as an emergency vehicle, send out false wrong way driving warnings, roadwork, or human presence on the road to clear a lane, to speed past other vehicles. He is an active dynamic insider acting as an individual, with local reach, see table IV. As stated previously, fiddling with safety functions is borderline malicious activity. The speeding attacker might still try to be rational about the reliance of the successful deceiving of other traffic participants as they might simply ignore his false claims or he might overlook real hazards.

TABLE IV. SPEEDSTER PROFILE MATRIX

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	dynamic		~~static~~
Organization:	~~cooperative~~		individual
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	rational	~~opportunistic~~

Another group taking advantage of this safety application may be a single or group of environmentalists or annoyed residents. Their goal might be to reduce the speed of vehicles, no matter what the rest of the community decided on to be acceptable. There are two basic technical approaches these attacker can pursue either they try to jam valid RSUs (Denial of Service), see Table V, or they try to compromise or mimic a valid RSU, see TableVI.

TABLE V. OUTSIDER TRAFFIC CALMING PROFILE MATRIX

Attacker Properties			
Membership:	~~insider~~		outsider
Method:	active		~~passive~~
Adaptability:	~~dynamic~~		static
Organization:	~~cooperative~~		individual
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	~~rational~~	opportunistic

When being able to communicate to other vehicles other attacks are possible, like trying to get the vehicles to alter their route, because of hazard warnings like weather conditions or

TABLE VI. INSIDER TRAFFIC CALMING PROFILE MATRIX

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	~~dynamic~~		static
Organization:	~~cooperative~~		individual
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	~~rational~~	opportunistic

fake traffic conditions. But a single RSU or a fake one has only a limited area of influence.

A small step up for the attacker who is compromising RSUs, see Table VI, to slow vehicles down, would be if he does not stop after controlling one RSU. He would try to get control over a larger area to have a bigger influence on victim vehicles, see Table VII. By doing so he poses a greater risk to safety in that area by exercising his power over an area and colluding RSUs, to make the false or modified warnings look authentic.

TABLE VII. SOPHISTICATED TRAFFIC MANIPULATION PROFILE MATRIX

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	dynamic		~~static~~
Organization:	cooperative		~~individual~~
Scope:	~~global~~	extended	~~local~~
Motivation:	~~malicious~~	rational	~~opportunistic~~

To prevent duplicate information, the following attack model omits the table, because the attacker resembles the worst case attacker as pictured in Table II. The attacker could be a foreign power either state sponsored or independent but the goal of this group would be to put on a stranglehold on safety related functions to unleash massive chaos by using infrastructure to flood victims with false hazard, collision warning and creating non existent vulnerable road users in front of vehicle, to get the safety systems to collapse and shutdown. During such an attack the goal of the attacker would be to create human casualties or at least create huge financial losses and impediment. The whole purpose of such a malicious attack is to weaken the position of an opponent and to strengthen their own, this could be also achieved by holding the infrastructure ransom and threatening to vandalize the infrastructure. To have such a large scale effect the attacker needs to compromise the infrastructure by ether common vulnerabilities or by compromising the provider of it.

The last three attacker types in this section dedicated are derived from the weakest attacker, see Table III. The goal of these attackers is to acquire knowledge about nearby vehicles. This goal is similar to the snooping individual who uses the manufacturer build in monitoring as described in Table XIII. The difference between these three type of attackers is their scope, whether they have only local, extended or global reception. A local influence might be easy to establish, only one receiver is needed. For extended visibility, more receivers are required, but for global reach the RSU to attacker receiver ratio must be one-to-one. This would be easy to achieve for an worst case attacker as he does not only want to have control over some infrastructure but wants to have control over all

available ones.

B. Cooperative Sensing (Information/Non-Safety)

In comparison to the safety relevant applications mentioned before, informational cooperative sensing application do not have an immediate life threatening aspect. The application for exchanging dynamic mapping information is particularly interesting as it might be used to improve the driver's experience, but could be misused to annoy the driver or even to literally navigate him into dangerous situations. One attacker who is trying to annoy drivers or shop owners sets up a fake RSU to send out false information about points of interest. This might reach from false opening hours to false location information. This can be considered as trolling, wasting someone's time and resources and annoying people to no end, as presented in Table VIII. He is rather static, a individual opportunistic attacker with only a local scope.

TABLE VIII. TROLLING VIA FALSE INFORMATION PROFILE MATRIX

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	~~dynamic~~		static
Organization:	~~cooperative~~		individual
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	~~rational~~	opportunistic

The second type of attacker are criminals, see Table IX, that use technology to make their activities easier. In case of mapping information, they could try to trick the driver via the navigation system to take another route, to send the driver to an abundant place to either rob or kidnap him. It may be enough to setup some fake RSUs or compromise a few, software wise or physically, to mislead or manipulate the victims systems. A single criminal or a group of them may feed dynamic false information into the systems near their victim and may even deploy multiple RSUs to have a higher chance of misleading the driver. When considering criminals as attackers, the differentiation whether their motivation is malicious or rational depends on where the perpetrators want to reuse their scheme, like a business, or if they are outright hitmen. But whether the latter one would invest in the technology and know-how to ease his job of executing a paid for assassination is questionable. Nonetheless intentional criminal activity would be considered malicious.

TABLE IX. FALSE INFORMATION AS CRIMINAL ACTIVITY SUPPORT

Attacker Properties			
Membership:	insider		~~outsider~~
Method:	active		~~passive~~
Adaptability:	dynamic		~~static~~
Organization:	cooperative		~~individual~~
Scope:	~~global~~	extended	~~local~~
Motivation:	malicious	~~rational~~	~~opportunistic~~

C. Cooperative Maneuvering

When considering cooperative maneuvering, one distinguishes if a non-cooperative fallback is available or not. If a non-cooperative fallback is available, the attacker might be just like the trolling one mentioned in Table VIII as no real

harm is possible because a safe downgrade to non cooperative assistance is available. If no fallback is available, there is a safety issue. CACC should have a non cooperative companion ACC. For the cooperative automated overtake application especially in an autonomous driving environment, the safety implications are obvious. An attacker sending false awareness information is only different from the worst case attacker (see Table II) in regards to his reach as he is locally limited and to the organizational aspect as he is an individual, see Table X.

TABLE X. Intentionally false CAM attacker profile matrix

Attacker Properties			
Membership:	insider	~~outsider~~	
Method:	active	~~passive~~	
Adaptability:	dynamic	~~static~~	
Organization:	~~cooperative~~	individual	
Scope:	~~global~~	~~extended~~	local
Motivation:	malicious	~~rational~~	~~opportunistic~~

D. In-Vehicle Internet Access

A malware author who uses the Internet connectivity as an initial attack vector to infect software components in a vehicle is summarized in Table XI. This type of an active attack depends heavily on the design of the vehicular internet access capabilities. If the vehicle itself does not have Internet enabled or capable components and merely provides an access point for other smart devices to get access, than the attack surface is reduced. Still, an outside attacker could try to attack the access point software or more generally common software components among vehicles of the same manufacturer or across the industry, that is reachable via the Internet. The ability of an attacker to adapt his malware or the ability of it getting new orders via an command and control infrastructure makes him an dynamic opponent. As an individual attacker who uses the Internet as the initial access vector to his victims, his capabilities are also limited by the ability to directly connect to a victim or whether the victim has to make the initial connection. In this case, he would resort to common scenarios like water hole, or phishing attacks, where the victim connects to an Internet resource who serves an exploit kit targeted at software vulnerabilities. Nevertheless the attackers scope is limited in the sense of the initial attack vector to a local one, further more he is going to act in a rational way, as he wants to make a profit of off his work.

TABLE XI. Vehicular malware initial attack vector

Attacker Properties			
Membership:	~~insider~~	outsider	
Method:	active	~~passive~~	
Adaptability:	dynamic	~~static~~	
Organization:	~~cooperative~~	individual	
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	rational	~~opportunistic~~

E. Mobility Monitoring and Configuration

There are cases where an owner or an agent of the owner (modder, tuner) could be seen as an attacker from the perspective of a vehicle manufacturer. In this case, the owner or his agent tries to manipulate the vehicle, e.g., to decrease the mileage count of a car. It is obvious that the owner or his agent can access all available communication, hence he is an insider attacker. He also has the ability to modify the hardware of software and react to security controls in place. For example, extraction of cryptographic keys from firmware images is a well-known approach in the car hacking and chip tuning community. Hence, the attacker is an adaptive attacker. Attacks usually affect only one vehicle. A special case is an attack on an online service portal of the manufacturer. If all vehicles of this manufacturer can be modified remotely, the attack could have an extended scope, but the initial vulnerability is still local to the service portal. The owner of a vehicle is a rational attacker as he is resource sensitive. If the use of a vehicle hack has less value than the money needed to execute the hack, the owner likely will not execute the attack. See Table XII for a summary.

TABLE XII. Modder/Tuner profile matrix

Attacker Properties			
Membership:	insider	~~outsider~~	
Method:	active	~~passive~~	
Adaptability:	dynamic	~~static~~	
Organization:	~~cooperative~~	individual	
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	rational	~~opportunistic~~

Another attacker is a control freak attacker. His goal is snooping on his or her spouse, child, or anybody else using the vehicle. As the owner of the vehicle, the active insider individual attacker can use the location tracking or monitoring ability for the legitimate purpose (e.g., finding his vehicle or creating an automatic driver's logbook) but also use it to spy on persons he lends the vehicle to. He does not need to change his behavior as tracking devices are already build into most vehicles. He is very opportunistic as he uses the abilities of the existing monitoring system. Only his own vehicle is affected. The properties of the control freak attacker are summarized in Table XIII.

TABLE XIII. Control Freak profile matrix

Attacker Properties			
Membership:	insider	~~outsider~~	
Method:	active	~~passive~~	
Adaptability:	~~dynamic~~	static	
Organization:	~~cooperative~~	individual	
Scope:	~~global~~	~~extended~~	local
Motivation:	~~malicious~~	~~rational~~	opportunistic

An extension of the control freak attacker is an attacker attacking a centralized location information system of a manufacturer. If such a centralized system (e.g., a service portal) exists and the user can query it for the position of his vehicle (e.g., to find a parked car), it could be an attractive target. The attacker is an outside attacker but he must be highly motivated, persistent, and dynamic. When attacking the system, the possession or control of multiple vehicles might be advantageous but the attacker is still considered to be individual and locally limited to the attacked system, that stores the location information. The attacker is not interested to create outages or service interruption as he is interested in the functioning system and especially in the data it gathers,

therefor he can be considered being rational. See Table XIV for a summary of this attacker.

TABLE XIV. MASS SURVEILLANCE PROFILE MATRIX

Attacker Properties		
Membership:	~~insider~~	outsider
Method:	active	~~passive~~
Adaptability:	dynamic	~~static~~
Organization:	~~cooperative~~	individual
Scope:	~~global~~ ~~extended~~	local
Motivation:	~~malicious~~ rational	~~opportunistic~~

The last two attacker models are still fit into the V2X communication and application paradigm, although they are centered around the existence of systems run by the manufacturer and misusing or exploiting weaknesses in them, which are reachable via the Internet.

VI. CONCLUSION AND FUTURE WORK

This paper presented a survey on current vehicular networking applications, including Cooperative Sensing (Safety), Cooperative Sensing (Information/Non-Safety), Cooperative Maneuvering, In-Vehicle Internet Access, and Mobility Monitoring and Configuration. Novel attacker models are presented that focus on realistic application-specific attacks instead of general attacks on vehicular networks.

TABLE XV. ATTACKER MODEL OVERVIEW

Attacker Properties		
1	Speedster	IV
2	Outsider Traffic Calming	V
3	Insider Traffic Calming	VI
4	Sophisticated Traffic Manipulation	VII
5	Massive Financial Damages and Human Casualties	II
6-8	Information Gathering with three different scopes	III
9	Trolling via false information	VIII
10	False information as criminal activity support	IX
11	Intentionally false CAM attacker	X
12	Vehicular malware initial attack vector	XI
13	Modder/Tuner	XII
14	Control Freak	XIII
15	Mass Surveillance	XIV

Our contribution describes 15 realistic attacker profiles in its main Section V, an summary is given in table XV. These attacker models allow for a more focused planning of security controls for vehicular networks, as well as a better comparability of security evaluations using these attacker models.

Using this attacker modeling approach for evaluation and providing in-depth examples on how to benefit from it in particular vehicular communication applications is reserved for future work.

REFERENCES

[1] C. Ponikwar and H.-J. Hof, "Overview on security approaches in intelligent transportation systems," SECURWARE 2015 : The Ninth International Conference on Emerging Security Information, Systems and Technologies, 2015, pp. 160–165.

[2] C. Salter, O. S. Saydjari, B. Schneier, and J. Wallner, "Toward a secure system engineering methodolgy," in Proceedings of the 1998 workshop on New security paradigms. ACM, 1998, pp. 2–10.

[3] B. Schneier, "Attack trees," Dr. Dobbs journal, vol. 24, no. 12, 1999, pp. 21–29.

[4] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," DTIC Document, Tech. Rep., 2001.

[5] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 1, 2005, pp. 78–118.

[6] D. Dolev and A. C. Yao, "On the security of public key protocols," Information Theory, IEEE Transactions on, vol. 29, no. 2, 1983, pp. 198–208.

[7] H.-J. Hof, "Sichere dienste-suche in sensornetzen," Ph.D. dissertation, Institut fr Telematik an der Universität Karlsruhe (TH), 2007.

[8] H.-J. Hof and M. Zitterbart, "Scan: A secure service directory for service-centric wireless sensor networks," Computer Communications, 2005, pp. 1517–1522.

[9] C. Mulliner, N. Golde, and J.-P. Seifert, "Sms of death: From analyzing to attacking mobile phones on a large scale." in USENIX Security Symposium, 2011.

[10] C. Mulliner, "On the impact of the cellular modem on the security of mobile phones," Ph.D. dissertation, Technische Universitt Berlin, Fakultt IV - Elektrotechnik und Informatik, 2012.

[11] R.-P. Weinmann, "Baseband attacks: Remote exploitation of memory corruptions in cellular protocol stacks." in WOOT, 2012, pp. 12–21.

[12] ——, "Baseband exploitation in 2013: Hexagon challenges," in Pacsec 2013, 2013.

[13] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, 2007, pp. 39–68.

[14] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," Communications Magazine, IEEE, vol. 53, no. 6, 2015, pp. 126–132.

[15] V. Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey," International Journal on AdHoc Networking Systems, vol. 4, no. 2, Apr. 2014, pp. 1–20.

[16] N. Nikaein, S. K. Datta, I. Marecar, and C. Bonnet, "Application distribution model and related security attacks in vanet," in 2012 International Conference on Graphic and Image Processing, 2012, pp. 876 808–876 808.

[17] I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-l. B. A. Manan, "Classes of attacks in vanet," in Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International. IEEE, 2011, pp. 1–5.

[18] T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, "Modeling roadside attacker behavior in vanets," in GLOBECOM Workshops, 2008 IEEE. IEEE, 2008, pp. 1–10.

[19] European Telecommunications Standards Institute, "ETSI TS 101 539-1 V1.1.1 (2013-08): Intelligent Transport Systems (ITS); V2x Applications;Part 1: Road Hazard Signalling (RHS) application requirements specification," Aug. 2013.

[20] ——, "ETSI TS 102 637-3 V1.1.1 (2010-09): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," Sep. 2010.

[21] ——, "ETSI TS 102 637-2 V1.2.1 (2011-03): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Mar. 2011.

[22] ——, "ETSI TS 101 539-3 V1.1.1 (2013-11): Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification," Nov. 2013.

[23] SAE International - On-Road Automated Vehicle Standards Committee, "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," Jan. 2014.