On Threat Analysis and Risk Estimation of Automotive Ransomware*

Full Paper

Nils Weiss University of Applied Sciences Regensburg Regensburg, Germany Nils2.Weiss@othr.de Markus Schroetter University of Applied Sciences Regensburg Regensburg, Germany Markus1.Schroetter@st.othr.de Rudolf Hackenberg University of Applied Sciences Regensburg Regensburg, Germany Rudolf.Hackenberg@othr.de

ABSTRACT

This paper combines a theoretical model for the risk estimation of a ransomware attack on vehicles with our experiences during an implementation of a real world ransomware as proof of concept. Our gained knowledge on ransomware attacks targeting a real car is transferred into a general model for risk estimation. It provides a generic guideline for the risk estimation and allows for identifying possible weaknesses in a vehicle's design concerning the threat of automotive ransomware. Through our abstracted approach, this model is applicable on every modern car. An example to prove this model is provided as well.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability;

KEYWORDS

Ransomware, Automotive Software, Security

ACM Reference format:

Nils Weiss, Markus Schroetter, and Rudolf Hackenberg. 2019. On Threat Analysis and Risk Estimation of Automotive Ransomware. In *Proceedings of ACM Computer Science in Cars Symposium, Munich, Germany, September* 2019 (ACM-CSCS'19), 9 pages. https://doi.org/10.475/123_4

1 INTRODUCTION

As almost everything in our modern society, vehicles are becoming more digital and connected. They are equipped with increasing numbers of small computers (Electronic Control Units (ECUs)) to improve safety and comfort. This development is an opportunity to improve everybody's life, but can lead to critical threats in terms of security. Security researchers already showed that automotive

*Produces the permission block, and copyright information

Unpublished working draft. Not for distribution

for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republisl

tee. Request permissions from permissions@acm

55

56

⁵⁸ 2019-08-29 11:27 page 1 (pp. 1-9) Submission ID: 123-A12-B3

attacks are possible and may have fatal consequences if they are used for malicious purposes[12].

Looking at the recent trends in traditional computer attacks, ransomware comes to mind. This type of malware has become quite popular among attackers and even has been in the news due to the devastating impact it can have. The popularity of this type of malware and the changes in the automotive industry raise the question of whether there can be a similar attack on vehicles.

The main incentive for creating an automotive ransomware is the possible profitability. Contrary to classical malware on computers, an automotive attack will require substantially more resources to create. To compensate this effort, an automotive ransomware attack has to scale well. This can be done by increasing the number of infections and the amount to pay for each. Here lies the potential of the automotive industry as a ransomware target.

Statistics of the International Organization of Motor Vehicle Manufacturers show that the automotive industry is growing constantly[13] and the average vehicle is continuously shifting towards a modern vehicle[14]. This means that the number of potential targets is increasing. Considering the average cost of a car, the demanded ransom can be significantly higher than the average amount of a traditional ransomware attack.

2 RELATED WORK

The field of automotive security has been researched for several years now. Most of this research focuses on ways to manipulate vehicles and automotive attack vectors in general. In 2010 a team of researchers analyzed and demonstrated how to control various functionality of a vehicle through an attack[5]. These findings give a basis for different manipulations to be potentially utilized by an automotive ransomware attack. Miller and Valasek did an extensive evaluation on vehicle attack surfaces[7] showing many different possible entrypoints which could also be utilized. In 2015, Miller and Valasek demonstrated a remote attack of an unaltered passenger vehicle[11]. The same attack could have been modified into a large-scale state-of-the-art ransomware attack.

The idea of an automotive ransomware has been discussed by ESCRYPT in 2018[6]. Marko Wolf et al. introduced an attack scheme with focus on a Command and Control (C&C) server based ransomware, discussed the possibilities of distribution and created an extensive security concept for building ransomware-proof vehicles. This paper takes a more general approach on automotive ransomware, introduces a model for risk estimation and focuses on

115

116

59

60

to post on servers or to redistribute to lists, requires prior specific permission and/or a

ACM-CSCS 19, September 2019, Munich, German

ACM ISBN 123-4567-24-567/08/06...\$15.00

⁵⁷ https://doi.org/10.475/123_4

an in-depth threat analysis. Furthermore, this paper discusses the proof of concept implementation on a real vehicle.

3 RANSOMWARE

117

118

119 120 121

122 123

124

125

126

127

128

129

130

132

133

134 135 136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

Taking the different types of ransomware explained in Symantec's tech report[15] and also considering doxware[17], one of them seems the most reasonable for automotive attacks. Both crypto ransomware and doxware rely on important or sensitive data, which a usual vehicle does not contain a lot of. Systems like hands-free calling or the camera for driver drowsiness detection could be used to collect sensitive information. Nonetheless, the worst for a car owner to happen is the car being unusable or being a danger to his health. Therefore, this paper focuses on automotive locker ransomware. All further descriptions about ransomware components refer to this type.

Ransomware components 3.1

This section gives an overview on the components for an ideal automotive ransomware. Basis for this list is the systematic segmentation of the traditional ransomware called "WannaCry"[2][9][4] into components. The identified ransomware components have then been put into the automotive context and extended by many automotive-specific components.

Each ransomware component can be influenced by multiple rating metrics. Rating metrics are introduced in section 4. The dependencies between ransomware components and rating metrics allow the creation of a risk model to evaluate the likelihood of an automotive ransomware attack and possible prevention strategies. Every component has an *Importance* property. The importance indicates the necessity of this component for a ransomware implementation. It was categorized by how effective the ransomware will still be if it is not implemented. If a component's importance is very high, it is unlikely to generate any profit through a ransomware attack, when this component isn't implemented. In contrast, for a component rated low, it is imaginable to create a fully functional implementation of a ransomware. Still, the implementation of a component with low importance will increase the possible profit of a ransomware attack.

Initial Infection 160 Definition Initial entry-point into the car. 161 162 Description It grants access to the car's inner network and permanently takes over an internal system. 163 164 Importance Very High 165 Influenced by • Attack Surface Attackability 166 Topology 167 • Protocol Vulnerability 168 • Operating System 169 • Hardware Properties 170 • Update Mechanism 171

174

| Definition | A mechanism to spread the infection onto new targets |
|----------------------|--|
| | from an infected target. |
| Description | An automotive ransomware can distribute itself through |
| _ | an outside entity (e.g. repair shop testers [16]) or by using |
| | an infected vehicles' communication capabilities and self- |
| ~ | replicating across vehicles. |
| ffect | Mass infections are possible. |
| nportance | High |
| ifluenced by | Attack Surface Attackability |
| | Topology |
| | Protocol Vulnerability |
| 1.0 | . CX |
| nternal Sprea | |
| Definition | A functionality to infect further internal components of an automotive network. |
| Description | Once inside the car's network, a possibility to spread |
| | across many ECUs. This gives access to safety-critical |
| | functions and actuators only specific ECUs have. Internal Spread can be a component to escalate privileges inside a |
| • • | virtualized ECU. Additionally, in case an ECU is replaced, |
| $\sim 1 \mathcal{Y}$ | it could be infected again. |
| ffect | Increases the impact and difficulty to remove. |
| nportance | Medium |
| ifluenced by | |
| ijiuenceu by | TopologyProtocol Vulnerability |
| XY | Operating System |
| | Hardware Properties |
| 2 | Update Mechanism |
| | |
|)ynamic Att a | |
| Definition | An advanced functionality for automated infection modi- fication. |
| Description | Altering an ECUs firmware requires processor architec- |
| 1 | ture specific exploits. They may vary between different |
| | firmware versions or different feature configurations of |
| | the same car model. A dynamic attack component can |
| | update the attack mechanisms of a ransomware based on target identification. |
| ffect | Increases the number of potential targets. |
| | |
| nportance | Low |
| ıfluenced by | Operating System |
| | Hardware Properties Number of Vulnerable Vehicles |
| | Number of Vulnerable Vehicles |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

229

230

231

On Threat Analysis and Risk Estimation of Automotive Ransomware

ACM-CSCS'19, September 2019, Munich, Germany

| Description Deferminitor Deferminitor Deferminitor Deferminitor Deferminitor Deferminitor Deferminitor Deferminitor Deferminitor <li< th=""><th>233</th><th>Download Fau</th><th>notionality</th><th>Lloon Intonacti</th><th></th></li<> | 233 | Download Fau | notionality | Lloon Intonacti | |
|--|-----|-------------------------------|--|------------------|---|
| an indecion perciption This composent information also be concerning the section also of origination and download the scattal matchine, composent in framewate, or perconnection is also to origination and advection and concerning the section and prove software. Effect perciption This composent information also the section and prove software. Information in hand with the Dynamic Allack composent. Fifter Information information the Dynamic Allack composent. Fifter Definition A mechanism to lock the ransomware tensore tage mechanism. Definition Definition A mechanism to lock the ransomware tensore tage mechanism. Definition Description Insorder for the ransomware to be effective it mast be consometion withe effectin anally week to the | 234 | Download Functionality | | User Interaction | |
| Process of a architecture and the heterogeneity of EU process of architectures, and avoid and avoid and a selection and avoid and a selection and a select | 235 | Definition | | | |
| and of modes of pression and particulations, and accord moleans may meet all of software prepared modes of prison and accords of the statul matrices or prison and accords of the statul matrices or prison accords of the prison matrix ac | | Description | Due to a car's architecture and the beterogeneity of FCU | Description | ≜ |
| all of storage for cutom attack scripts and caplois. The malware cubile stripted down to the bare index in malware with the Dynamic Attack component.input attack malware cubile scripted down with the Dynamic Attack component.input attack malware cubile scripted down with the Dynamic Attack component.If glear in malware index in malware index in malware index in malware index in malware index index in the data comection. This for it regulare is a polongy interaction. This for it regulare is a polong.The interaction. This for it regulare is a polong.Presister in polong. interaction. This for it regulare interaction. This for it regulare is a polong. is a polong.A thank Surface Attack a thin interaction. This for it regulare is a polong.Provide View Philip is a polong.Presister in polong. interaction. This for it regulare is a polong.Provide View Philip is a polong.Provide View Philip is a polong.Presister in polong. in polong.In order for the ransonware removal possibilition. it is a polong.Provide View Philip is a polong.Provide View Philip is a polong.Presister in polong.In order for the ransonware removal possibilition cons. The observe with the polong. is a polong.Provide | | Description | | | 6 |
| I_{1} I_{2} < | | | | | |
| Importance Very High Importance Very High Importance Provide extendable functionality with minimum storage requirements. Influenced by • Topology Influenced by • Attack Surface Attackability • Protocol Vulnerability • Very High Importance Importance Very High Importance Importance Very High Importance Importance Very High Importance Hardware Properties • Operating System Importance Importance Prophatilow • Operating System • Attack Surface Attackability • Attack Surface Attackability • Protocol Vulnerability Importance Prophatimon Prophatilow | | | malware could be stripped down to the bare minimum | Effect | |
| in hand with the Dynamic Attack component.ExampleThe inflationward system can be used for interaction. In put can be used for interaction with a C&C server. <t< td=""><td>241</td><td></td><td></td><td>Importance</td><td>Very High</td></t<> | 241 | | | Importance | Very High |
| Fifter Provides extendable functionality with minimum storage requirements. Influenced by • Topology Influenced by • Attack Strafface Attackability • Topology • Protocol Vulnerability • Protocol Vulnerability • Doperating System • Definition A mechanism to lock the ransonware removal possibilities Payment process, money exchange mechanism. Definition A mechanism to lock the ransonware removal possibilities Payment process, money exchange mechanism. Description In order for the ransonware to be effective it must the hard to remove. All debine (CMO) or reparts System Payment process, woney exchange mechanism. Effect Increases the costs for removal. Influenced by • Engliphe Protocol Vulnerability • Operating System • Attack Surface Attackability Protocol Vulnerability • Operating System • Attack Surface Catackability Protocol Vulnerability • Operating System • Attack Surface Catackability Protocol Vulnerability • Update Mechanism • Update Mechanism Description Relatious ACC: serverts • Undewing for engliphe existing controls. Influenced by • Eradware Properties • Update Mechanism Operating • Operating System | 242 | | | - | , , |
| interaction influenced by • Topology influenced by • Attack Surface Attackability • Operating System influenced by • Attack Surface Attackability • Operating System • Dopology • Portocol Vulnerability • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Definition h order for the ransomware to be effective it must be inso to be attackers identities and the ECU Original Equipment Maunfacturer (OEA) or or erior stops con rest the ECU Immware to removal. Importance • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System • Operating System | 243 | Effect | | Example | |
| Importance Low Protocol Yuhnerability Spology Protocol Yuhnerability Spology Protocol Yuhnerability Spolagy Protocol Yuhnerability | 244 | Ljjeci | , 0 | Influenced by | |
| Anderseed by Attack Surface Attackability Spology Spology | 245 | Importance | • | influenceu o y | 1 65 |
| Attack Surface Attackability Popology Protocol Vulnerability Operating System Update Mechanism Persistence Mechanism Description In order for the ransomware removal possibilities Description In order for the ransomware to be effective it must be tool to a specific car. Also the amount of the ransom vare to be effective it must be achieved by using a cryptocurrency that allows attended to the ransom vare. Importance Effect Increases the costs for removal. Inportance Figlet Inportance Figlet Preventing the victim to pay the ransom. Description Description Influenced by Operating System Update Mechanism Inportance Figlet Provide Victim Properties Update Mechanism Proportance Figlet Provide Victim Properties Update Mechanism Propology Protocol Vulnerability Update Mechanism Propology Proportance Proportance Proportance Proportance Proportance Propology Proportance Propology Proportance Proventing the victim to pay the ransom. Description < | 246 | - | | | |
| Protocol Vulnerability Operating System Definition A mechanism to lock the ransomware removal possibilities. Description A containing the payment must not expose the attackers' identifies and manual of the transom has to be considered. The components User Interaction and Communication may be used for implementing the payment process. Description In order for the ransomware to be effective it must be interest to remove all be effective it must be into the transom has to be considered. The components User Interaction and Communication may be used for implementing the payment process. Description In order for the ransomware to be effective it must be into the transom the to the ransom ware to be effective it must be into the transom the tot the components that address attaching a vehicle specific identifier as a payment process. Influenced by internewer High Inportance Influenced by internewer that be CUI forware to remove the internew that address attaching a vehicle specific identifier as a payment process. Influenced by internewer the CUI forware to remove the internewer the internew that the the CUI forware to remove the internewer the payment internewer that address internewer that address internewer the payment internewer the payment internewer the payment internewer the payment internewer that address internewer the payment internewe | | Influenced by | | | |
| 9 • Operating System Definition Payment process, money exchange mechanism. 9 Persistence Hechanism • Update Mechanism Description In exchange mechanism. 9 Persistence Advancementation A mechanism to look the ransomware removal possibilities. Description In order for the ransomware to be effective it must be hard to remove. All debug, re-flashing, update and restore mechanism may be disabled. In this case, not very effective it must be the for the formoware. Importance Very High 9 Effect Increases the costs for removal. Influenced by • Attack Surface Statability 9 Importance High • Operating System • Attack Surface Statability 9 Definition Behaviour forcing the victim to pay the ransom. • Vehicle Attractiveness 9 Definition Relaviour forcing the victim to pay the ransom. • Attack Surface Statability 9 Definition Behaviour forcing the victim to pay the ransom. • Vehicle Attractiveness 9 Definition Behaviour forcing the victim to pay. • Vehicle Attractiveness 9 Protono Protosol Winershilty • Interaver Properties endities of or were exchange with a C&C server. 9 Definition Behaviour forcing the victim to pay the ransom. Definition 9 Definition Behaviour forcing the victim t | | | 1 07 | Payment | |
| Persistence V=traism Definition A mechanism to lock the ransomware removal possibilities. Description In order for the ransomware to be effective it must be its association, and Communication may be used for implementing the payment process. Persistence V=traism In order for the ransomware to be effective it must be its association, and communication may be used for implementing the payment process. Importance Importance Importance This may be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching any be achieved by using a cryptocurrency that allows attaching a vehicle specific identifier as a payment must be the payment must be that payment must be the payment must | | | • | Definition | Payment process, money exchange mechanism. |
| Persistence Mechanism and must be test to a specific car. Also the amount of the ransom has to be considered. The components User Interaction and Communication may be used for implementing the payment process. Description In order for the ransomware to be effective it must be hard to remove. All debug, reflashing, update and restore mechanism may be disabled. In this case, not even the ECUS Original Equipment Manufacturer (OEM) or repair shops can reset the ECU firmware to remove the ransomware. Importance Importance Importance Importance Importance Importance Importance Very High Malicious Cherription Description Operating System • Attack Surface Attackability • Attack Surface Attackability Malicious Cherription Behaviour forcing the victim to pay the ransom. Description A data link for the communication with a C&C server. Description Behaviour forcing the victim to pay the ransom. Description A data link for the communication with a C&C server. Description Locker ransomware seens very effective. Certain functions or the engine from starting. • Proventing the use into paying. • Proventing the use into paying. Importance Very High • Proventing the use into paying. • Proventing the use into paying. • Proventing the engine from starting. Influenced by • Protocol Vulnerability • Operating System • Propology </td <td></td> <td></td> <td></td> <td>Description</td> <td>The payment must not expose the attackers' identities</td> | | | | Description | The payment must not expose the attackers' identities |
| Persistence Mechanism Persistence Mechanism Inconcision of lock the ransomware removal possibilities. the ransom has to be considered. The components User Interaction and Communication may be used for implementing the payment process. Description In order for the ransomware to be effective it must be hard to remove. All does, re-flashing, update and response to repair shops can reset the ECU firmware to remove the ransomware. Importance Very High Importance High • Operating System • Attack Surface Attackability • Hardware Properties Definition Behaviour forcing the victim to pay the ransom. Definition Behaviour forcing the victim to pay the ransom. Definition Behaviour forcing the victim to pay the ransom. Description Attack Surface Attackability Definition Behaviour forcing the victim to pay the ransom. Description Attack surface Stability Definition Behaviour forcing the victim to pay the ransom. Description Attack Surface Attackability Definition Behaviour forcing the victim to pay the ransom. Description Attack Surface Attackability Definition Behaviour forcing the victim to pay the ransom. Description Attack Surface Attackability Description Description Description Pressures the user into paying. Frotocol | | | | 1 | |
| a bytendin ites. menting the payment process. b pescription In order for the ransonware to be effective it must be to remove. All debug, re-flashing, update and it for mere all debug, re-flashing, update and it for mere all debug re-flashing, update and it for the consonware to remove the ransomware. Importance Very High Effect Increases the costs for removal. Influenced by • Attack Surface Attackability influenced by • Operating System • Attack Surface Attackability • Attack Surface Scalability Malicious Activity • Update Mechanism • Update Mechanism • Operating System Definition Behaviour forcing the victim to pay the ransom. Definition Addata lake for the communication with a C&C server. Description Locker ransonware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about attack surface Attackability • Nallows information exchange with a C&C. Importance Very High • Topology • Protocol Vulnerability • Topology <td></td> <td>Persistence M</td> <td>echanism</td> <td></td> <td></td> | | Persistence M | echanism | | |
| 235 Description In order for the ransomware to be effective it must be hard to remove. All debug, re-flashing, update and restore mechanisms may be disabled. In this case, not even it the ECUs Original Equipment Manufacturer (OEM) or repair shops can reset the ECU firmware to remove the ransomware. Importance Very High 236 Effect Increases the costs for removal. Influenced by Attack Surface Attackability Number of Vulnerable Vehicles Vehicle Attractiveness Update Mechanism Definition Behaviour forcing the victim to pay the ransom. Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Importance Very High Definition Behaviour forcing the victim to pay the ransom. Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Importance Very High Importance Very High Inportance Very High Inportance Very High Inportance Vehicle Attractiveness Vehicle Attractiveness | | Definition | A mechanism to lock the ransomware removal possibili- | • • | |
| Importance Hard to remove. All debug, re-flashing, update and restore mechanisms may be disabled. In this case, not even the ECUS original Equipment Manufacture (Okdo or repair shops can reset the ECU firmware to remove the ransomware. This may be achieved by using a cryptocurrency that allows attaching a vehicle specific identifier as a payment increases. Effect Increases the costs for removal. Influenced by • Attack Surface Attackability Influenced by • Operating System • Vehicle Attractiveness Update Machine Materia Cubic Cubic Science • Vehicle Attractiveness Definition Behaviour forcing the victim to pay the ransom. Definition Description Locker ransomware seems very effective. Certain functions and more. A data connection is increded in order to implement this. Effect Pressures the user into paying. • Attack Surface Attackability Importance Very High • Operating System Effect Pressures the user into paying. • Operating Cubic Cubic Certain functions and more. A data connection is increded in order to implement this. Importance Very High • Operating System Effect Pressures the user into paying. • Operating System Influenced by • Topology • Protocol Vulnerability • Operating System Operating System • Opology </td <td>255</td> <td></td> <td>ties.</td> <td>A 1 Y</td> <td></td> | 255 | | ties. | A 1 Y | |
| store mechanisms may be disabled. In this case, not even the ECUs Original Equipment Manufacturer (OEM) or repair shops can reset the ECU firmware to remove the ransomware. Effect Increases the costs for removal. Influenced by Operating System Operating Operating System Operating System Operating System Operating System Operating System Operating System Operating Operating System Operating System Operating System Operating Operating System Operating Operating System Operating System Operating Operating Operating System Operating Operating Operating System Operating Operating System Operating Operating System Operating Operating Operating System Operating Operating Operating System Operating System Operating Operating System Operating Operating System Operating Operating Operating System O | 256 | Description | | Importance | Very High |
| the ECUs Original Equipment Manufacturer (OEM) or repair shops can reset the ECU firmware to remove the ransomware. Effect Increases the costs for removal. Influenced by Operating System Influenced by Operating System Hardware Properties Update Mechanism Definition Behaviour forcing the victim to pay the ransom. Definition Description Locker ransomware seems very effective. Certain functions or the entire vichicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Pressures the user into paying. Inportance Very High Effect Pressures the user into paying. Inportance Very High Effect Pressures the user into paying. Inportance Very High Effect Protocol Vulnerability Opology Protocol Vulnerability Opology Protocol Vulnerability Opology Protocol Vulnerability Opology < | 257 | | | Example | |
| repair shops can reset the ECU firmware to remove the ransomware. Influenced by • Attack Surface Attackability Effect Increases the costs for removal. • Attack Surface Attackability Inportance High • Attack Surface Scalability Influenced by • Operating System • Attack Surface Scalability • Hardware Properties • Vehicle Attractiveness • Vehicle Attractiveness Malicious Activity Bedravour forcing the victim to pay the ransom. Definition A data link for the communication with a C&C server. Definition Behaviour forcing the victim to pay the ransom. Description A data link for the communication and this. Definition Behaviour forcing the victim to pay the ransom. Description Adata link for the communication and the C&C. Importance Effect Pressures the user into paying. Effect Allows information exchange with a C&C. Importance Very High • Topology • Protocol Vulnerability • Protocol Vulnerability Influenced by • Topology • Operating System • Vehicle Attractiveness Importance Very High • Operating System • Protocol Vulnerability • Operating System • Vehicle Attractiveness • | 258 | | | | |
| 201 ransomware. Influenced by - Attack Surface Attackability 202 Effect Increases the costs for removal. - Attack Surface Scalability 203 Influenced by - Operating System - Attack Surface Scalability 204 Influenced by - Operating System - Vehicle Attractiveness 205 - Update Mechanism - Operating System - Vehicle Attractiveness 205 Definition Behaviour forcing the victim to pay the ransom. Definition A data link for the communication with a C&C server. 205 Definition Behaviour forcing the victim to pay the ransom. Description A data link for the communication with a C&C. 205 Decoription Locker ransomware seems very effective. Certain function addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. 206 Importance Very High - Topology - Topology 207 Influenced by - Topology - Protocol Vulnerability - Operating System 208 - Operating System - Vehicle Attractiveness - Stription - Attack Surface Attackability 208 - Topology | 259 | | | | message. |
| 252 Effect Increases the costs for removal. Importance High Number of Vulnerable Vehicles Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Description Decker ransomware seems very effective. Certain function about disabled safety features increases the pressure to pay. Effect Preventing the engine from starting. Importance Influenced by Protocol Vulnerability Operating System Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness Vehicle Attractiveness | 260 | | | Influenced by | • |
| Importance High • Operating System Influenced by • Operating System • Vehicle Attractiveness Malicious Activity • Update Mechanism • Vehicle Attractiveness Malicious Activity • Definition Behaviour forcing the victim to pay the ransom. Definition Behaviour forcing the victim to pay the ransom. Description A data link for the communication with a C&C server. Definition Behaviour forcing the victim to pay the ransom. Description This might be used for key exchanges, transmitting IDs, payment confirmations and more. A data connection is needed in order to implement this. Bescription Locker ransomware seems very effective. Certain function addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. Importance Very High • Topology • Topology • Protocol Vulnerability • Topology • Protocol Vulnerability • Operating System • Vehicle Attractiveness • Protocol Vulnerability • Operating System • Vehicle Attractiveness • Vehicle Attractiveness • Protocol Vulnerability • Operating System • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness | | Effect | Increases the costs for removal. | | |
| Influenced by Operating System Hardware Properties Update Mechanism Update Mechanism Update Mechanism Definition Behaviour forcing the victim to pay the ransom. Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Pressures the user into paying. Importance Preventing the engine from starting. Influenced by Operating System Vehicle Attractiveness Vehicle Attractiveness | | | | | 2 |
| Infuture and possible • Operating system • Hardware Properties • Update Mechanism Malicious Activity Definition A data link for the communication with a C&C server. Definition Behaviour forcing the victim to pay the ranson. Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. Importance Very High • Topology • Topology • Protocol Vulnerability • Protocol Vulnerability • Operating System • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness | | - | 5 | | |
| 266 • Update Mechanism Communication 267 • Update Mechanism Definition A data link for the communication with a C&C server. 268 Malicious Activity Definition Behaviour forcing the victim to pay the ransom. Description Locker ransomware seems very effective. Certain functions on the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. 279 Effect Pressures the user into paying. - Attack Surface Attackability - Topology 279 Importance Very High - Notocol Vulnerability - Protocol Vulnerability 279 • Topology - Topology - Protocol Vulnerability - Protocol Vulnerability 279 • Operating System - Vehicle Attractiveness - Vehicle Attractiveness - Vehicle Attractiveness | | Influenced by | | | |
| 267 Definition Definition A data link for the communication with a C&C server. 268 Malicious Activity Definition Behaviour forcing the victim to pay the ransom. Description Locker ransomware seems very effective. Certain func- tions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. 274 Effect Pressures the user into paying. - Attack Surface Attackability - Topology - Topology 275 Example Preventing the engine from starting. - Topology - Protocol Vulnerability - Operating System - Protocol Vulnerability 283 - Vehicle Attractiveness - Vehicle Attractiveness - Vehicle Attractiveness | | | | Communicat | ion |
| 269 Definition Behaviour forcing the victim to pay the ransom. payment confirmations and more. A data connection is needed in order to implement this. 270 Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. 274 Effect Pressures the user into paying. Importance Low 275 Importance Very High • Attack Surface Attackability • Topology 275 Enfluenced by • Topology • Protocol Vulnerability • Operating System 286 • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness | 267 | | | Definition | A data link for the communication with a C&C server. |
| Definition Behaviour forcing the victim to pay the ransom. payment confirmations and more. A data connection is needed in order to implement this. Description Locker ransomware seems very effective. Certain functions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. Importance Importance Influenced by • Attack Surface Attackability Preventing the engine from starting. • Topology • Protocol Vulnerability • Operating System • Vehicle Attractiveness • Vehicle Attractiveness | 268 | Malicious Act | tivity | Description | This might be used for key exchanges, transmitting IDs, |
| Description Locker ransonware seems very effective. Certain func- tions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. Effect Allows information exchange with a C&C. 274 Effect Pressures the user into paying. Importance Low 275 Importance Very High • Attack Surface Attackability • Topology • Topology 276 Influenced by • Topology • Protocol Vulnerability • Protocol Vulnerability 280 • Operating System • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness | 269 | | - | | |
| 271tions or the entire vehicle could be made unusable. In addition, random behaviour and telling the victim about disabled safety features increases the pressure to pay. <i>Effect</i> Allows information exchange with a C&C.274 <i>Effect</i> Pressures the user into paying.Influenced by• Attack Surface Attackability276 <i>Importance</i> Very High• Topology• Protocol Vulnerability277 <i>Example</i> • Topology• Protocol Vulnerability280• Operating System• Vehicle Attractiveness281• Vehicle Attractiveness• Vehicle Attractiveness | | Description | Locker ransomware seems very effective. Certain func- | | - |
| 273 isabled safety features increases the pressure to pay. Importance Low 274 Effect Pressures the user into paying. • Attack Surface Attackability 275 Importance Very High • Protocol Vulnerability 276 Influenced by • Topology • Protocol Vulnerability 278 Influenced by • Topology • Protocol Vulnerability 279 • Operating System • Vehicle Attractiveness • Vehicle Attractiveness 281 • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness 282 • Vehicle Attractiveness • Vehicle Attractiveness • Vehicle Attractiveness | | 1 | tions or the entire vehicle could be made unusable. In | Effect | Allows information exchange with a C&C. |
| 274 Effect Pressures the user into paying. • Attack Surface Attackability 275 Importance Very High • Topology 277 Example Preventing the engine from starting. • Protocol Vulnerability 278 Influenced by • Topology • Protocol Vulnerability 280 • Operating System • Vehicle Attractiveness 281 • Vehicle Attractiveness • Vehicle Attractiveness 282 • Vehicle Attractiveness • Vehicle Attractiveness 283 • Vehicle Attractiveness • Vehicle Attractiveness 284 • Vehicle Attractiveness • Vehicle Attractiveness 285 • Vehicle Attractiveness • Vehicle Attractiveness 286 • Vehicle Attractiveness • Vehicle Attractiveness 287 • Vehicle Attractiveness • Vehicle Attractivenes 288 • Vehicle Attractivenes • Vehicle Attractivenes 289 • Vehicle Attractivenes • Vehicle Attractivenes 281 • Vehicle Attractivenes • Vehicle Attractivenes 282 • Vehicle Attractivenes • Vehicle Attractivenes 283 • Vehicle Attractivenes • | 070 | | | Importance | Low |
| Effect Pressures the user into paying. • Topology 276 Importance Very High • Protocol Vulnerability 277 Example Preventing the engine from starting. • Topology 278 Influenced by • Topology • Protocol Vulnerability 280 • Operating System • Vehicle Attractiveness 281 • Vehicle Attractiveness • Vehicle Attractiveness 283 • Vehicle Attractiveness • Vehicle Attractiveness 284 • Vehicle Attractiveness • Vehicle Attractiveness 284 • Vehicle Attractiveness • Vehicle Attractiveness 285 • Vehicle Attractiveness • Vehicle Attractiveness 286 • Vehicle Attractiveness • Vehicle Attractiveness 288 • Vehicle Attractiveness • Vehicle Attractiveness 289 • Vehicle Attractiveness • Vehicle Attractiveness 289 • Vehicle Attractiveness • Vehicle Attractiveness | | | disabled safety features increases the pressure to pay. | Influenced by | Attack Surface Attackability |
| ImportanceVery High• Protocol VulnerabilityExamplePreventing the engine from starting.Influenced by• Topology• Protocol Vulnerability• Operating System• Operating System• Vehicle Attractiveness283• Vehicle Attractiveness284• Vehicle Attractiveness285• Vehicle Attractiveness | | Effect | Pressures the user into paying. | | |
| 278 Influenced by • Topology 279 • Protocol Vulnerability 280 • Operating System 281 • Vehicle Attractiveness 282 • 283 • 284 • 285 • 286 • 287 • 288 • 289 • | | Importance | Very High | | Protocol Vulnerability |
| 279 • Protocol Vulnerability 280 • Operating System 281 • Vehicle Attractiveness 282 283 283 284 284 285 285 286 286 288 287 288 288 289 | 277 | Example | Preventing the engine from starting. | | |
| 279 • Protocol Vulnerability 280 • Operating System 281 • Vehicle Attractiveness 282 283 283 284 284 285 285 286 286 288 287 288 288 289 | 278 | Influenced by | • Topology | | |
| Sprang System Vehicle Attractiveness 282 283 284 285 286 287 288 289 | 279 | 5 | 1 05 | | |
| 282 283 284 285 286 287 288 289 | 280 | | | | |
| 283 284 285 286 287 288 289 | | | Vehicle Attractiveness | | |
| 284 285 286 287 288 289 | | | | | |
| 285 286 287 288 289 280 | | | | | |
| 286 287 288 289 | | | | | |
| 287 288 289 | | | | | |
| 288 289 | | | | | |
| 220 | | | | | |
| ²⁹⁰ 2019-08-29 11:27 page 3 (pp. 1-9) Submission ID: 123-A12-B3 | 289 | | | | |
| | 290 | 2019-08-29 11:27 p | bage 3 (pp. 1-9) Submission ID: 123-A12-B3 | | |

| N. | Weiss | et a | ١. |
|----|-------|------|----|
| | | | |

| 349 | Revert Trigger | | Anti-Reinfee | tion | 407 |
|------------|----------------------|---|--|---|------------|
| 350 | Definition | A process for initiating the revert mechanism. | Anti-Reinfection Definition Prevent infections of a vehicle that was already paid for. | | 408 |
| 351 | Description | In order to initiate the revert mechanism, a trigger is | Description | Reinfections after the payment may make the victims | 409 |
| 352 353 | Description | needed. It must be implemented in a way that only the | Description | lose trust of regaining the car. A mechanism to prevent | 410 411 |
| 354 | | attackers approval releases a specific car. | | another infection is required. | 412 |
| 355 | Effect | Authenticated ransomware removal. | Effect | Increases trust in the ransomware payment. | 413 |
| 356 | Importance | High | Importance | Medium | 414 |
| 357 | Example | On payment the attacker provides a secret for regaining | Influenced by | Operating System | 415 |
| 358 | Example | access to the car. | influencea by | Operating System Hardware Properties | 416 |
| 359 | Influenced by | Attack Surface Attackability | | · · · · · · · · · · · · · · · · · · · | 417 |
| 360 | injiaeneea o y | Attack Surface Attackability Topology | | | 418 |
| 361 | | Protocol Vulnerability | | | 419 |
| 362 363 | | · | | CX | 420 421 |
| 364 | Revert Mechan | iism | | | 421 |
| 365 | Definition | A mechanism to uninstall a ransomware. | 4 RATIN | G METRICS FOR RISK EVALUATION | 423 |
| 366 | Description | Victims have to be certain that after unlocking everything | OF AU | TOMOTIVE RANSOMWARE | 424 |
| 367 | | will be as safe as without the ransomware, otherwise | These metrics | are the core components of the introduced risk eval- | 425 |
| 368 | | they might not pay. A malfunctioning car as a result | | The model is the result of an evaluation of difficulties | 426 |
| 369 | | of an incomplete removal can be life-threatening. Even after the ransomware removal driving might be against | | plementation of an automotive ransomware. It is based | 427 |
| 370 | | the law and insurance companies might refuse to pay | on a general | understanding of a car's structure, several research | 428 |
| 371 | | in case of an accident. Additionally the car's warranty | | [7] and on our own proof of concept implementation. | 429 |
| 372 | | might be gone. This may lead to the entire car having | | sic vehicle properties of a modern vehicle and puts | 430 |
| 373 374 | | to be reprogrammed or certain components need to be | | text for a risk estimation on how prone the vehicle is | 431 432 |
| 374 | 700 | replaced. | | re attacks. These properties are known by car man- | 432 |
| 376 | Effect | Removal of a ransomware. Reward for paying. | | the necessary information can be acquired through e vehicle of interest. When estimating the risk, the | 434 |
| 377 | Importance | High | | bility and the effort for the attack creation have to | 435 |
| 378 | Influenced by | Operating System | | account. Unless attackers want to directly harm a | 436 |
| 379 | | Hardware Properties | | <i>t</i> , these are the factors they most likely consider. | 437 |
| 380 | | Update Mechanism | | | 438 |
| 381 | | | | ce Attackability | 439 |
| 382 | Hardening Me | <i>chanism</i> Mechanisms to increase the difficulty for reverse engi- | Description | Attack Surface in terms of attackability measures the qual- ity of an attack surface to be utilized by a ransomware. | 440 |
| 383 | Definition | neering and countermeasures. | | | 441 |
| 384 385 | Effect | Increase the ransomware resilience. | Vehicle Propert | | 442 443 |
| 386 | | | | bood of unauthorized or insecure devices being con - considers devices like smartphones or On-board diagnostics | 444 |
| 387 | Importance | Medium | (OBD-II) | | 445 |
| 388 | Example | Disabling ways to read the ransomware's code from the | · · · · · | back end servers can be used as attack vector | 446 |
| 389 | | ECU is one example. The ransomware using encrypted messages within the vehicle is another one. Also a mech- | Critical | features on interfaces increase the possibilities for ex- | 447 |
| 390 | | anism to stop any bad behaviour when a virtual environ- | ploits | | 448 |
| 391 | | ment or a development board is detected would counter | | ayers of separation from the attack surface to the ve- ner network lead to less steps for accessing critical func- | 449 |
| 392 | | examinations within a simulated environment. | tionality | 1 0 | 450 |
| 393 | Influenced by | Operating System | | ectors over a large distance lead to less restrictions of at- | 451 |
| 394 | | Hardware Properties | | cause there is no need to be physically close to the target | 452 |
| 395 396 | | Update Mechanism | 1 | bibility of temporary or permanent data connection al- C server communication | 453 454 |
| 397 | | | | | 455 |
| 398 | | | Ransomware C | 1 | 456 |
| 399 | | | Initial InSelf-Dist | | 457 |
| 400 | | | | ad Functionality | 458 |
| 401 | | | Payment | | 459 |
| 402 | | | Commun | | 460 |
| 403 | | | • Revert T | rigger | 461 |
| 404 | | | | | 462 |
| 405 | | | | | 463 |
| 406 | | | | 2019-08-29 11:27 page 4 (pp. 1-9) Submission ID: 123-A12-B3 | 464 |

| | | 523 |
|---|--|---|
| Operating Sys | | 524 |
| Description | The Operating System metric measures the ease of attack- ing an ECU considering operating system related vehicle properties. | 525 526 |
| Vehicle Propert | * * | 527 |
| A well k be easier and its vu If an OS o industry, If the OS may be p | nown Operating System (OS) (e. g. a unix-like system) can to attack because attackers may already be familiar with it alnerabilities or a software component is widely used in the automotive more ECUs may be affected by the same vulnerability offers high abstraction , easier and more generic attacks ossible | 528 529 530 531 532 533 533 |
| less explo | is implemented and designed securely , it might contain bitable security flaws zation or separation reduces the possibilities for privilege n | 535 536 537 538 |
| Ransomware C | omponents | 539 |
| Initial InfInternal SDynamic | fection Spread | 540 541 542 |
| | d Functionality | 543 |
| | ce Mechanism | 544 |
| Malicious User Inte | | 545 |
| Revert M | | 546 |
| • Hardenin | ng Mechanism | 547 |
| Anti-Reir | nfection | 548 |
| Hardware Pro | operties | 549 550 |
| Description | Hardware Properties measures the attackability by tak- ing the ECUs hardware capabilities and properties into account. | 551 552 |
| Vehicle Propert | ies | 553 |
| | ECU having high processing power some computation- | 554 |
| intensive | attack scenarios may become realizable | 555 556 |
| | persistent memory access is available, a ransomware is ermanently infect an ECU | 557 |
| 0 | ariety in hardware architectures results in the demand dual exploits and compilations for each architecture | 558 559 |
| With a la to be atta | rger number of ECUs , more individual targets may have icked | 560 561 |
| | re several different firmware versions for the same ECU n attack might have to be customized depending on the version. | 562 563 564 |
| Ransomware C | omponents | 565 |
| Initial Inf | * | 566 |
| Internal S | Spread | 567 |
| • Dynamic | | 568 |
| | ce Mechanism | 569 |
| Payment Payment M | | 570 |
| Revert M Hardenin | echanism ng Mechanism | 571 |
| Hardenin Anti-Reir | 5 | 572 |
| | | 573 |
| | | 574 |
| | | 575 |

Topology

| Description | Topology measures the ease of attacking a vehicle by |
|-------------|--|
| | considering the vehicle's network layout. |

Vehicle Properties

- Through a high **variety in network-technologies** an attack will be significantly harder
- Isolation of critical ECUs onto separated network domains makes it necessary to infect several networks for advanced malicious activity
- Presence of a gateway or a firewall between networks increases the effort to spread attacks between networks and protects the internal network from outside attack surfaces
 - ECUs that bridge networks may allow for bypassing the network separation
 - Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) might prevent the infiltration of safety-critical networks

Ransomware Components

- Initial Infection
- Self-Distribution
- Internal Spread
- Download Functionality
- Malicious Activity
- User Interaction
- Communication
- Revert Trigger

Protocol Vulnerability

Vehicle Properties

- If the used protocols are common with other vehicles more generic attacks may be possible
- Criticality of communication considers messages to be misused for malicious activity
- Both **authenticated** and **encrypted communication** increase the difficulty to manipulate the communication

Ransomware Components

- Initial Infection
- Self-Distribution
- Internal Spread
- Download Functionality
- Malicious Activity
- User Interaction
- Communication
- Revert Trigger

522 2019-08-29 11:27 page 5 (pp. 1-9) Submission ID: 123-A12-B3

Description Protocol Vulnerability measures the ease of manipulating the communication.

| N. Weiss et al. |
|---|
| measures the impact on the payout utes. |
| for a more complex infection which a repair shop gh, the ransom to be paid may be |
| s the ransom that can be demanded eatures to be misused for malicious tes to threaten the car owner ty possible to be misused to col- ype automotive ransomware could |
| nsiders vehicles that are used fre- easily |
| |
| ic vehicle being targeted with c can be estimated through the n of the introduced components provide a structured approach evaluated for a vehicle by eval- with a checklist procedure. The associated with a ransomware the difficulty of its implementa- r very high importance need to ansomware. If the average diffi- se necessary components is low, Components of low importance rare attack. These components an attacker. |
| IMPLEMENTATION |
| mware was implemented for a is ransomware created insights of a real world automotive ran- nsible disclosure we choose to r the specific car used as it may e all rating metrics derived from tion gives us knowledge about specific component. Lastly, we ndividual components and give plementation. The estimated im- pared with real implementation |

5.1 Vehicle specific rating metrics

The following metrics were derived based on the properties of a real car.

- The exploit will be easier if a common bootloader is used. Flashing mechanism might be standardized and therefore the exploit might be applicable on several different ECUs.
- Having the firmware available online for download means that it is easily acquirable by attackers. This simplifies the reverse engineering process since attackers do not need to extract firmwares from ECUs
 - This is not the case when the firmware image is **encrypted**
 - An update mechanism only accepting cryptographically signed firmwares increases the difficulty of manipulating the firmware.

Ransomware Components 597

Update Mechanism

Vehicle Properties

Description

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

598

599

600

601

602

603

607

608

609

610

611

612

613

614

615

616

617

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

- Initial Infection
- Internal Spread
- Download Functionality
- Persistence Mechanism
 - Revert Mechanism
 - Hardening Mechanism

Attack Surface Scalability 604

Description Attack Surface in terms of scalability measures the quality 605 of attack surfaces for large-scale attacks. 606

Vehicle Properties

- Long-range attacks over a large distance are able to target more vehicles.
- The reachability and availability of a potential attack vector is considered because of features disabled by default or ones that only work with the vehicle turned on.
- If the infection is fully automatable without the need of an attacker's or car owner's manual operation, a large-scale attack will be easier to execute.
- Ransomware Components
 - Payment

Number of Vulnerable Vehicles 618

- Description Number of Vulnerable Vehicles measures the number of possible targets.
- Vehicle Properties
 - Commonness of architectures used considers architecture-based vulnerabilities that affect not only a single car model.
 - Similarly, if the ECUs are widespread and reused in many different vehicles, those may also be prone to an attack.
 - Over-The-Air updates decrease the number of vulnerable vehicles if the vulnerabilities are fixed.

Ransomware Components

- Dynamic Attack
- Payment

695

696

639

640

641

642

643

Vehicle Attractiveness

Description Vehicle Attractiveness out through a car's attrib

Vehicle Properties

- A large number of ECUs allows nich increases the cost for removal at
- If the average repair cost is his be higher
- A higher car value also increases ided
- A large number of advanced fe ious behavior increases the possibiliti
- If a vehicle contains functionali collect sensitive data a doxware-t mld be created
- · Importance of availability co. frequently and can not be replaced

Ransomware Components

- Malicious Activity
- Payment

4.1 Risk

The general likelihood of a specif vith an automotive ransomware attack the introduced model. The combination ents with vehicle specific rating metrics bach for this. Each rating metric can be valuating each influencing property v The combination of all rating metrics are component gives an estimation on entation. All components with a high o d to be implemented for a functioning r lifficulty for the implementation of the low. a ransomware attack is more likely. nce increase the impact of a ransomw ents will increase the possible profit of

5 PROOF OF CONCEPT

To prove this model, a basic ranso or a real car. The implementation of thi ghts in the implementation difficulties ransomware. In the context of respon e to not provide details on the exploit o may endanger car owners. First, we state rom the vehicle properties. This evalua out the implementation difficulty of a we explain the implementation of all in give a rating for the difficulty of the imp implementation difficulty will be com ion difficulty to prove this model.

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

723

724

725

726

727

728

729

730

742

743

High

Attack Surface Attackability High The investigation object has several attack surfaces (LTE/GSM, WiFi, Bluetooth, OBD-II). Critical features, for example unprotected flashing mechanisms, are available without authentication on OBD-II. Internal ECUs are not protected through a network architecture with separated domains. Large distance attack vectors are not vulnerable for well known exploits. Attacks on low-distance interfaces (e.g. OBD-II) are easy to implement. The car's cellular communication can be utilized for a permanent data connection. Topology Very High No central gateway. All internal networks are connected to the OBD-II connector. Safety-critical ECUs share a communication bus with remotely attackable ECUs. Some vulnerable ECUs can be used as a bridge between networks. This network topology makes the vehicle very prone to attacks. Protocol Vulnerability High The same protocols are used for different car brands. Safety-critical commands are available in the protocol and can be abused by an attacker. Weak authentication and no encryption are present. An attacker can fake or replay any Controller Area Network (CAN) message. **Operating System** Low Most ECUs are using a proprietary real time OS. Only two ECUs are using the unix-like OS QNX. The absence of a common function set for every ECU leads to customized attacks for every ECU which increases the effort for an attacker. Virtualized ECUs are not present in this car. Hardware Properties Low Most ECUs have a comparable low processing power. Every ECU is designed for a single purpose. Hardware-Watchdogs will reset ECUs if the Central Processing Unit (CPU) utilization is too high. A large variety of processor architectures increases the difficulty of an attack. Since hardware-watchdogs supervise the CPU utilization of safety-critical ECUs, exploits have to be crafted very carefully. Update Mechanism High Over-The-Air update mechanism are present but not enabled. ECU updates are not cryptographically signed. Firmware images are not encrypted. Update mechanism can be exploited over the vehicle internal networks. Attack Surface Scalability Low Large-Distance attack surfaces are present. A built-in Telematic Commu-

731 nication Unit (TCU) provides a permanent data connection to a backend 732 system. Exploitation of large-distance attack vectors is very difficult. 733

Number of Vulnerable Vehicles High 734

Value priced car. ECUs are identical on many different brands of the same 735 OEM. Only small changes are required to port the implementation of a 736 ransomware to different car models or brands from the same OEM.

737 Vehicle Attractiveness

738 Absence of cryptographically signed firmware images gives an attacker 739 all possibilities on malicious activities. Any actuator of the vehicle could 740 potentially be used to frighten the owner of the car. 741

Very High

5.2 Implementation of Ransomware components

744 This section describes, how the components were implemented on 745 a real car. A rating for the effort of the implementation of a specific 746 component is given as well. If a component could be implemented 747 in short time or without the necessity to overcome any protection 748 mechanism the effort was rated very low to low whereas if the 749 opposite was the case, we rated it high to very high. 750

Initial Infection Medium 751

The software update mechanism over OBD-II was used for the initial infec-752 tion. A vulnerable repair shop tester [16] or a vulnerable OBD-II dongle [8] 753 can distribute an initial ransomware infection to the car. 2019-08-29 11:27 page 7 (pp. 1-9) Submission ID: 123-A12-B3 754

Self-Distribution

This component was not implemented for the proof of concept.

Internal Spread

Since the software update mechanism of this car was vulnerable, the internal spread component could have been implemented through the same software update mechanism, already used for the initial infection. To achieve an internal spread, exploits for further ECUs would need to be included in the ransomware. This would increase the size and the complexity of this ransomware.

Dynamic Attack

This component was not implemented since the ransomware was planted in only one ECU.

Download Functionality Very High

The targeted ECU did not have any communication capabilities with a remote server. An implementation of this would become possible by forwarding the data connection of the communication component.

Persistence Mechanism

Since the initial infection modified the firmware image of the targeted ECU, this component could have been implemented easily. A modification of the security access mechanisms would be sufficient to lock out the OEMs repair shop tools. This would stop a repair shop from removing the ransomware through reprogramming the infected ECU. At this point, a hardware replacement and the man-hour costs of a repair shop are required to remove the ransomware from a car.

Malicious Activity

Very Low

Medium

Repair shop tester functions were used to implement this component. These functions are used to trigger specific functions during a car repair. Our ransomware was able to abuse these commands by sending requests to various ECUs over the inner network.

User Interaction

Low

The proof of concept ransomware was able to abuse a service used for displaying WiFi settings to the car owner. This service allows the ransomware to display text messages on the multimedia screen of the car. Button presses on the touch screen were sent on the vehicle internal CAN bus. The ransomware, running on a different ECU, achieves a bi-directional communication just by sending and receiving CAN and CAN-Layer Transport Protocol (ISOTP) messages.

Payment

Low

To process the payment, the user was provided with a bitcoin account number through the multimedia interface. A way to tie the payment to a vehicle was not implemented for the proof of concept ransomware.

Communication

Very High Data communication to a backend server was not possible to be implemented during the proof of concept development. This component would require an attack of the TCU of this car.

Revert Trigger

A revert trigger was not necessary for the proof of concept implementation. **Revert** Mechanism Low

The ransomware execution was achieved through a hijack of interrupt vectors in the ECU firmware. A simple restore of the original interrupt vectors in the program memory of the ECU was sufficient to revert the ransomware.

Hardening Mechanism

Hardening mechanisms were not implemented on the proof of concept ransomware.

Anti-Reinfection

This component was not necessary for the proof of concept. The simplest implementation would be to fix the vulnerability.

755

5.3 Comparison between model and implementation

The effort for the implementation of the most important components of a ransomware is compared to the difficulty derived from the model. This shows how our model can be applied to identify critical vehicle properties. An estimated effort for the implementation of a component is indicated by the combination of all vehicle metrics influencing this component.

Initial Infection

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

The estimated effort for an initial infection is medium. Also the effort for a real implementation is medium. The difficulty for this implementation is lowered through the metrics Attack Surface Attackability, Protocol Vulnerability, Update Mechanism and Topology. Therefore, a secured update mechanism and signed firmware updates would increase the difficulty of an implementation. An initial infection would not be possible with medium effort if these countermeasures would be present in the car.

Persistence Mechanism

Considering the model, the effort for the implementation of the Persistence Mechanism is medium to high. We rate the difficulty for the implementation medium. The weak security of the update mechanism made it possible. Again, a very effective countermeasure to prevent the implementation of this component would be the use of signed firmwares.

Malicious Activity

Evaluating the model indicates very low effort to implement the component Malicious Activity. During the implementation of the real world ransomware, very low effort was required to implement this component. Changes in the vehicle internal network topology and authenticated communication for repair shop testers would increase the difficulty for the implementation of this component.

User Interaction

Through the combination of all metrics influencing the component User Interaction, very low effort for the implementation was predicted. For the implementation in a real car, low effort was spent. Authenticated internal communication would be a sufficient mitigation to raise the difficulty for this component. Since this component is crucial for a ransomware, the likelihood of a ransomware attack could be lowered through this countermeasure extensively.

Payment

The estimated difficulty for the implementation of the Payment component is low to very low. Our proof of concept implementation was not fully functional but could have been extended with little effort to tie the payment to the car. Since an attacker could use the bitcoin cryptocurrency for the payment process, a real world implementation would require low effort. In order for this component to have effect, it requires the User Interaction component. If an attacker can not show instructions for the payment, the implementation of this component is not possible. Therefore this is the easiest way to increase the difficulty for a payment process.

Revert Mechanism

Our model predicted a medium difficulty for the implementation of the component Revert Mechanism. Through the absence of signed firmware images for ECUs, the effort spent on the implementation of this component was low.

5.4 Summary

Using encrypted communication and a signed update mechanism would have increased the difficulty for implementing many crucial ransomware components. Therefore, with very few changes, the risk could be decreased dramatically. Analyzing the metrics influencing the components with the highest importance allows for finding the weaknesses with the highest impact in the vehicles' design. This allows for well-aimed countermeasures.

6 CONCLUSION

Our proof of concept implementation shows that, from a technical point of view, automotive ransomware attacks are possible in real world scenarios. It is likely that an automotive ransomware attack has the potential to scale very well. A locker ransomware is the most expectable type of ransomware for automotive systems. In addition to ransomware components that are absolutely necessary there are optional ones that increase the impact. Basic factors that influence the risk of a specific vehicle were found and put together as vehicle specific rating metrics. As shown, the introduced model can be used to identify problematic vehicle properties. Through the correlation between vehicle properties and ransomware components, a car manufacturer can identify effective countermeasures against specific components. These insights can be used for creating a security concept and security architecture within the security extended V-model[18][1]. This way, the vehicle's design can be improved in terms of the ransomware threat and overall.

7 FUTURE WORK

With time passing and new technologies being developed it may be necessary to extend or adjust the automotive ransomware components introduced in section 3.1. This also means that the model may have to be extended by new rating metrics. Extensive research on many different vehicles and a deep evaluation of all vehicle properties may allow a unified rating of vehicles. This abstract model is a first step for a unified risk estimation model which allows comparisons of the security level of different vehicles.

Additional contributions to this work includes the research and demonstration of a mass infection of many ECUs. An analysis on how different attack surfaces can be utilized for automotive ransomware may be worth investigating. Even though there are already researches focusing on attack surfaces [7][11][10], they do not consider any special requirements an automotive ransomware might have.

Lastly a security concept or a maturity model can be created based on this paper's findings.

REFERENCES

 Cornelius Bittersohl and Timothy G. Thoppil. [n. d.]. Automotive Cybersecurity. Developing a thriving security ecosystem within automotive. P3 North America, Inc.

On Threat Analysis and Risk Estimation of Automotive Ransomware

[2] CERT-MU. 2017. THE WANNACRY RANSOMWARE. Technical Report. CERT-MU.

- [3] Computest. 2018. The Connected Car: Ways to get unauthorized access and potential implications. (2018).
- [4] ENDGAME. 2017. WCry/WanaCry Ransomware Technical Analysis. (2017). Retrieved January 10, 2019 from https://www.endgame.com/blog/technical-blog/ wcrywanacry-ransomware-technical-analysis
- [5] Karl Koscher et al. 2010. Experimental Security Analysis of a Modern Automobile. (2010).
- Marko Wolf et al. 2018. WANNA DRIVE? Feasible Attack Paths and Effective [6] Protection Against Ransomware in Modern Vehicles. (2018).
- [7] Stephen Checkoway et al. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. (2011).
- [8] Rudolf Hackenberg, Nils Weiss, Sebastian Renner, and Enrico Pozzobon (Eds.). 2017. Extending Vehicle Attack Surface Through Smart Devices. IARIA.
- [9] LogRhythm Labs. 2017. A Technical Analysis of WannaCry Ransomware. (2017). Retrieved January 7, 2019 from https://logrhythm.com/blog/ a-technical-analysis-of-wannacry-ransomware/
- [10] Dr. Charlie Miller and Chris Valasek. 2014. A Survey of Remote Automotive Attack Surfaces. (2014).
- [11] Dr. Charlie Miller and Chris Valasek. 2015. Remote Exploitation of an Unaltered Passenger Vehicle. (2015).
- Dr. Charlie Miller and Chris Valasek. 2016. CAN Message Injection. (2016). [12]
- [13] International Organization of Motor Vehicle Manufacturers. 2015. Motorization rate 2015 - WORLDWIDE. (2015). Retrieved January 11, 2019 from http://www. oica.net/category/vehicles-in-use/
- , a , yan/ .are. (2017). .ve Domain. PWIN [14] International Organization of Motor Vehicle Manufacturers. 2017. 2005-2017 Sales Statistics. (2017). Retrieved January 11, 2019 from http://www.oica.net/ category/sales-statistics/
- [15] Kevin Savage, Peter Coogan, and Hon Lau. 2015. The evolution of ransomware. Technical Report, Symantec, Version 1.0.
- [16] András Szijj, Levente Buttyán, and Zsolt Szalay. 2015. Hacking cars in the style of Stuxnet. (2015). Retrieved May 21, 2019 from http://www.hit.bme.hu/~buttyan/ publications/carhacking-Hacktivity-2015.pdf
- Brian Thorne. 2017. Computer Security: Enter the next level: Doxware. (2017). [17] Retrieved May 14, 2019 from http://cds.cern.ch/record/2291225
- [18] Dr. Markus Tschersich. 2018. Cybersecurity in the Automotive Domain. PWIN Guest Lecture. Continental AG.

2019-08-29 11:27 page 9 (pp. 1-9) Submission ID: 123-A12-B3