# GENIVI Security Architecture Overview

October 19, 2016 | **AMM Burlingame - All Members**

GENIVI Security Team Lead
Stacy Janes - Irdeto

# Why Do We Care?

GENIVI®

# The Who

GENIVI®

# Researchers – Exploit but Disclose

## Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

August 10, 2015

# Researchers – Exploit but Disclose

- Unauthenticated Dbus

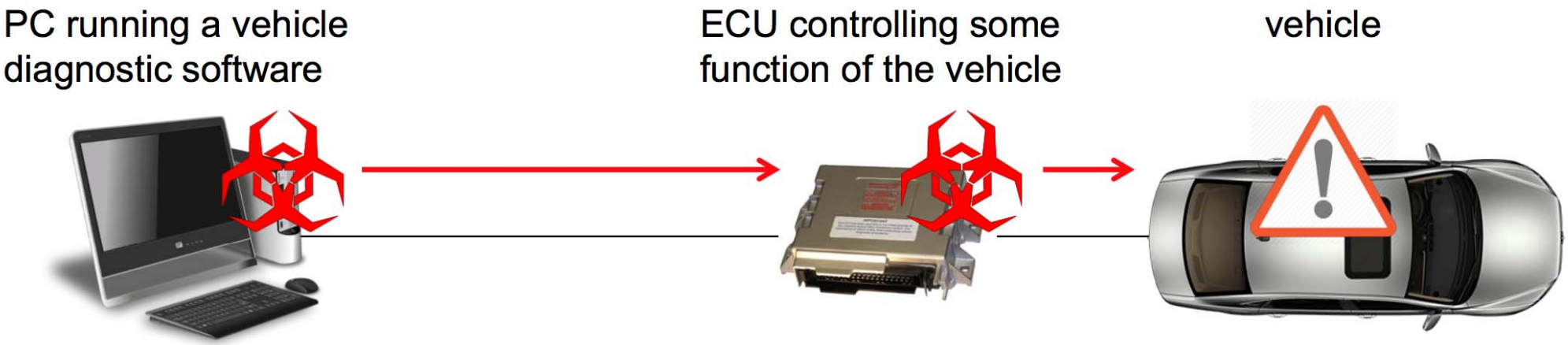
```
telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.
Escape character is '^]'.
AUTH ANONYMOUS
OK 4943a53752f52f82a9ea4e6e00000001
BEGIN
```

- Multiple Dbus interfaces usable for code injection
- Signature verification ‘hole’ allows jailbreaking headunit
- V850 Firmware reverse engineered
- Firmware modified to allow malicious commands
- Firmware reinstalled

# Researchers - Exploit but Disclose

# Researchers - Exploit but Disclose

Malware installed on Windows PC, replacing a DLL for a popular aftermarket diagnostic application



# Researchers - Exploit but Disclose

Methods used:

- DLL replacement attack
- protocol reverse engineering
  - Message formats
  - Checksum computation
  - encryption scheme
- man-in-the-middle attack
  - logging and replaying sessions
  - modifying messages on-the-fly
- experiments

# Researchers - Exploit but Disclose

# Researchers - Exploit but Disclose

Attack appeared to start with a MITM attack on the charging station search function.

Researchers were able to gain remote control of the car due to lack of firmware signing, allowing them to:

- Open/close the sunroof
- Move driver’s seat
- Write images to IVI / cluster
- Apply brakes

# Researchers - Exploit but Disclose

# Researchers - Exploit but Disclose

```
GET https://[redacted].com/orchestration_1111/gdc/BatteryStatusRecordsRequest.php?
RegionCode=NE&lg=no-NO&DCMID=&VIN=SJNFAAZE0U60XXXXX&tz=Europe/Paris&TimeFrom=2014-09-
27T09:15:21
```

Researcher performed a MITM attack on an unauthenticated API on mobile app to vehicle connection, allowing them to:

- Access battery status
- Access HVAC status
- Control A/C on/off

# Motivations – When Disclosure Stops

# Criminals– Exploit and Profit!

# Ransomware – Moving on From Mobile

EDITION: US

ZDNet

VIDEOS CXO WINDOWS 10 CLOUD INNOVATION SECURITY APPLE MORE NEWSLETTERS ALL

MUST READ SAMSUNG CUTS PROFIT FORECAST BY $2.3 BILLION AFTER GALAXY NOTE 7 SAGA

## 'Massive' Locky ransomware campaign targets hospitals

FireEye researchers have spotted a surge in cyberattacks on hospitals in the US -- and they're using a new infection technique.

By Danny Palmer | August 19, 2016 -- 07:35 GMT (00:35 PDT) | Topic: Security

# Ransomware – Willingness to Harm

KrebsonSecurity

In-depth security news and investigation

22 MAR 16

## Hospital Declares 'Internal State of Emergency' After Ransomware Infection

A Kentucky hospital says it is operating in an "internal state of emergency" after a ransomware attack rattled around inside its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.

# Ransomware – Willingness to Harm

Healthcare IT News

TOPICS SIGN UP MAIN MENU

Privacy & Security

## Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By Bill Siwicki | May 23, 2016 | 02:58 PM

SHARE 823

# Ransomware – Is Auto a Target?

Driving | NEWS | REVIEWS | BUYER'S GUIDE | CAR COMPARISON

MotorMouth

HOME / AUTO NEWS / NEWS /

Motor Mouth: Ransomware is the future of car theft

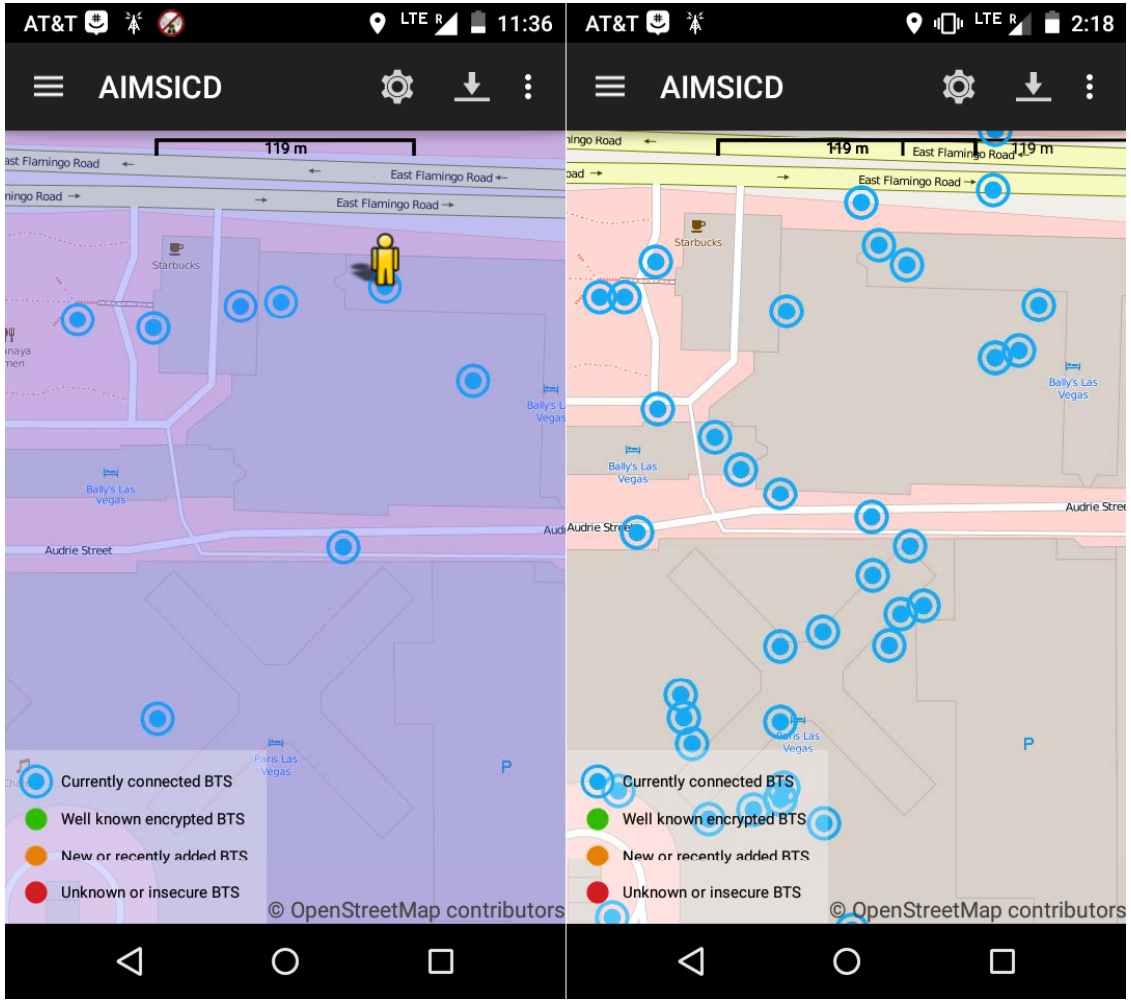
# The How

GENIVI®

# Methods – Wifi Hacking.

# Methods – Wifi Hacking

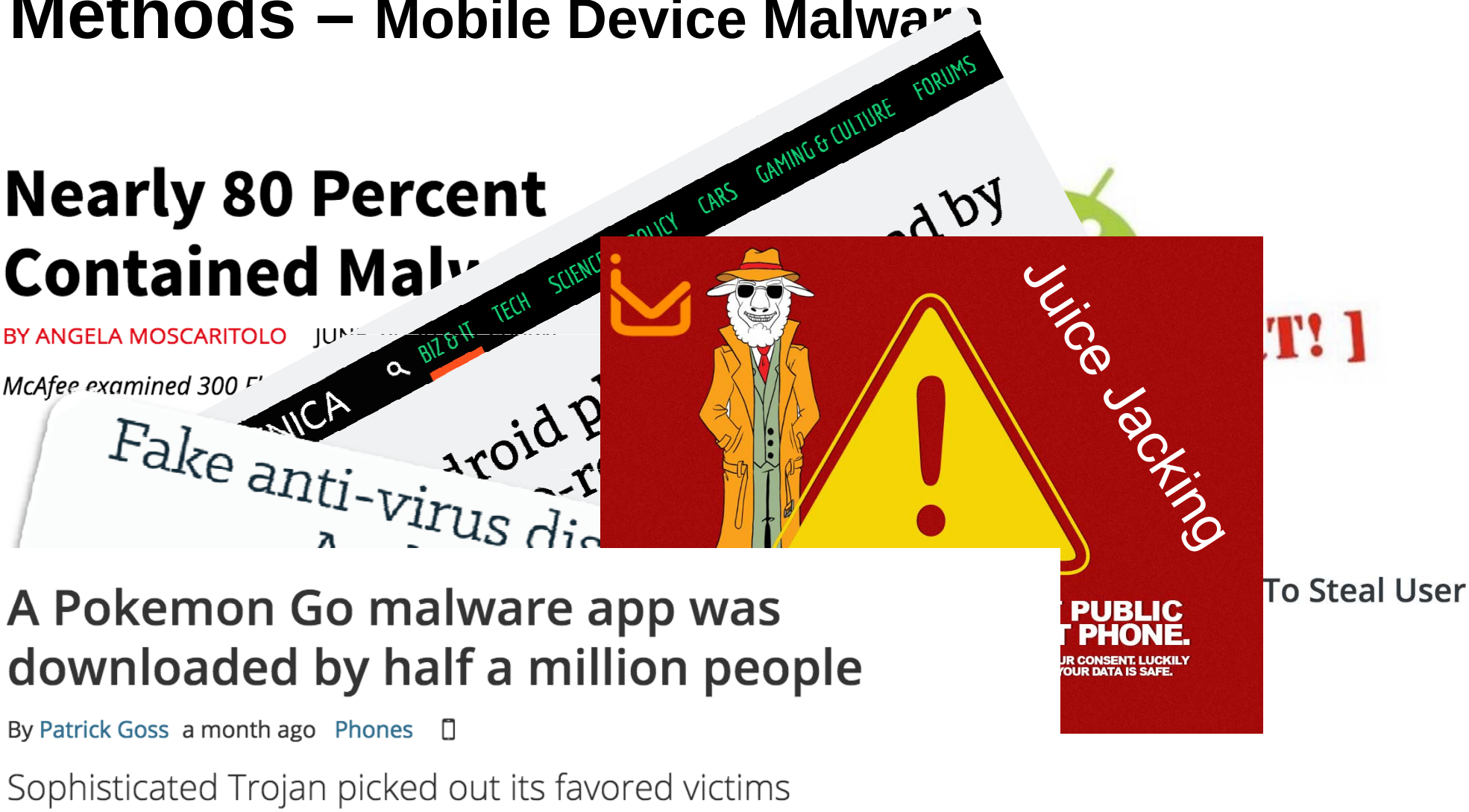
# Methods – Cellular Hacking with IMSI-Catchers




These screenshots show a scan of cell towers before Defcon (left) and during (right).

Images: Geoffrey Vaughan

# Methods – Mobile Device Malwa



# Methods – TLS Exploits

The DROWN Attack (**D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption)

Heartbleed

*KCI (Key Compromise Impersonation)*

POODLE Vulnerability (**P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption)

CRIME (**C**ompression **R**atio **I**nfo-leak **M**ade **E**asy)

BEAST (**B**rowser **E**xploit **A**gainst **S**SL/**T**LS)

See RFC 7457 for more details

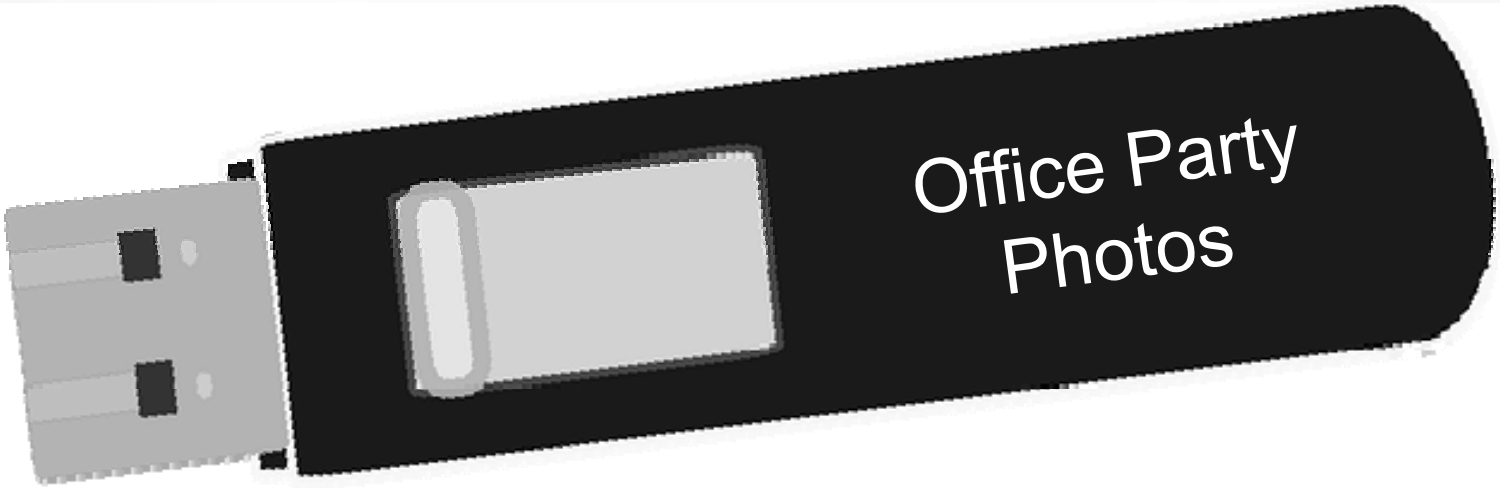
# Methods – Bad USB

**BADUSB - ON ACCESSORIES THAT TURN EVIL**

**PRESENTED BY**

Karsten Nohl & Jakob Lell

USB has become so commonplace that we rarely worry about its security implications. USB sticks undergo the occasional virus scan, but we consider USB to be otherwise perfectly safe – until now.



# Mirai – Botnet on Steroids

KrebsOnSecurity.com was knocked offline by 620Gbps DDos. One of the biggest ever recorded.

Indications are that an estimated 145,000 IoT devices such as security cameras and DVRs were used as a botnet for the attack.

Botnet of passenger cars? Would we even know it was happening?

# BotNet – Now Open Source

**[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release**

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

**Anna-senpai**

L33t Member

L33T

## Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every [redacted] dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

# Our View – The Car is a Hostile Environment

**CVE Details**
*The ultimate security vulnerability datasource*

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search View CVE

Log In Register

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Home
**Browse :**
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
**Reports :**
CVSS Score Report
CVSS Score Distribution
**Search :**
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
**Top 50 :**
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
**Other :**
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
**External Links :**
NVD Website
CWE Web Site
**View CVE :**

**Linux » Linux Kernel : Security Vulnerabilities (CVSS score between 7 and 7.99)**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **310** Page : 1 (This Page) 2 3 4 5 6 7

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2016-6187 | 119 | | Overflow +Priv | 2016-08-06 | 2016-08-11 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The apparmor_setprocattr function in security/apparmor/lsm.c in the Linux kernel before 4.6.5 does not validate the buffer size, which allows local users to gain privileges by triggering an AppArmor setprocattr hook. | | | | | | | | | | | | | | |
| 2 | CVE-2016-5829 | 119 | | DoS Overflow | 2016-06-27 | 2016-08-16 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call. | | | | | | | | | | | | | | |
| 3 | CVE-2016-5828 | 20 | | DoS | 2016-06-27 | 2016-08-16 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call. | | | | | | | | | | | | | | |
| 4 | CVE-2016-5342 | 119 | | DoS Overflow | 2016-08-30 | 2016-09-06 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| Heap-based buffer overflow in the wcnss_wlan_write function in drivers/net/wireless/wcnss/wcnss_wlan.c in the wcnss_wlan device driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact by writing to /dev/wcnss_wlan with an unexpected amount of data. | | | | | | | | | | | | | | |
| 5 | CVE-2016-5340 | 20 | | Bypass | 2016-08-07 | 2016-08-11 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The is_ashmem_file function in drivers/staging/android/ashmem.c in a certain Qualcomm Innovation Center (QuIC) Android patch for the Linux kernel 3.x mishandles pointer validation within the KGSL Linux Graphics Module, which allows attackers to bypass intended access restrictions by using the /ashmem string as the dentry name. | | | | | | | | | | | | | | |
| 6 | CVE-2016-4997 | 264 | | DoS +Priv Mem. Corr. | 2016-07-03 | 2016-10-04 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement. | | | | | | | | | | | | | | |
| 7 | CVE-2016-4951 | | | DoS | 2016-05-23 | 2016-09-28 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation. | | | | | | | | | | | | | | |
| 8 | CVE-2016-4913 | 200 | | +Info | 2016-05-23 | 2016-09-28 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem. | | | | | | | | | | | | | | |

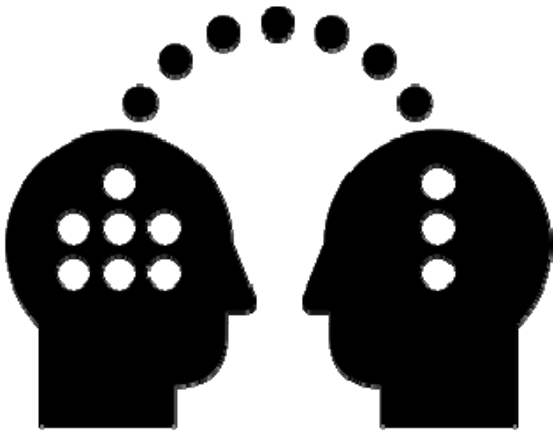
# How We Help

GENIVI®

# Focus – A Confident and Informed Customer

Our Focus is to assemble detailed information about the security requirements of a GENIVI project into an easy to understand document.

We want to present this information in a manner such that the customer of the Expert Group can make informed decisions about product security for their final solution and be confident in the decisions they made.



# Deliverable – Quality Deliverables to our Customer

Our Customers are the GENIVI Expert Groups. We intend to work closely with the Expert Groups to produce a product that is beneficial to them and their final customers. This product will contain:

- A detailed threat assessment of the GENIVI solution
- Security mitigations included with the solution
- Security Requirements around the use of the solution

# Focus – More Secure GENIVI Projects

We will recommend security mitigation to GENIVI Expert Groups for their projects based on a security threat analysis.

We will provide Security education that is relevant to the work of GENIVI developers.

# Deliverable – Recommendations and Information

Our Customers are the GENIVI Expert Groups. During the threat assessment, we will work with the group to suggest architectural or design changes that we think will make the project more secure. We will also recommend an open source security solutions that will address a specific attack vector.

We will strive to provide relevant and educational security talks and other forms of security information.

# Charter

Define a comprehensive set of robustness and compliance rules to enable GENIVI Expert Groups to more easily determine the software security requirements for their solutions

Work with individual Expert Groups to identify and document the software security requirements and risks related to their domains

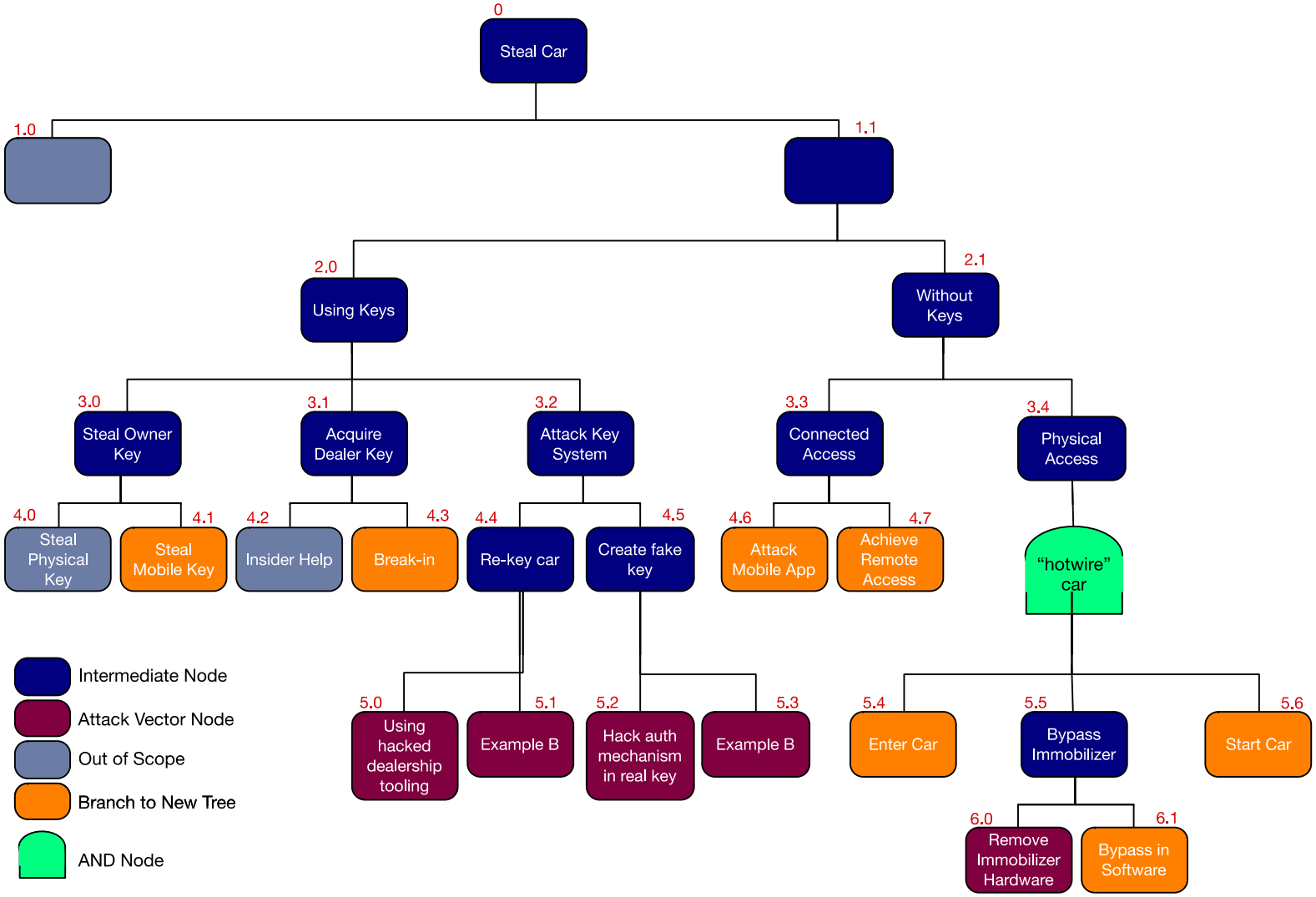
Define and promote in the Expert Groups the architectural and open source solutions for achieving the software security requirements.

Provide and promote security education to the Expert Groups

# Example – Asset Description

| Asset | Description | Threat |
|---|---|---|
| Physical Vehicle Key | Standard physical key fob with cryptographic authentication. Allows for vehicle entry and vehicle start. | If this key is compromised such that it can be spoofed, it will allow an unauthorized person to enter and start the vehicle, resulting in vehicle theft. |
| Mobile Vehicle Key | Key data on mobile device capable of unlocking and/or starting vehicle. Allows for vehicle entry and vehicle start. | If this key data is compromised in manner such that it can be spoofed or replayed, it will allow an unauthorized person to enter and start the vehicle, resulting in vehicle theft. |
| Mobile cryptographic key | Cryptographic key on mobile device for purpose of establishing secure communication with cloud or vehicle. | If this key is compromised, or can be guessed, an attacker would be able decrypt traffic between the device and server or pose as a valid mobile device to the vehicle or cloud in order to send malicious traffic. |
| Vehicle cryptographic key | Cryptographic key in vehicle telematics unit for purpose of establishing secure communication with cloud or mobile device. | If this key is compromised, or can be guessed, an attacker would be able decrypt traffic between the vehicle and server or pose as a valid mobile device to the device or cloud in order to send malicious traffic. |
| Cloud cryptographic key | Cryptographic key in cloud server for purpose of establishing secure communication with vehicle or mobile device | If this key is compromised, or can be guessed, an attacker would be able decrypt traffic between the cloud and client or pose as a valid server to the vehicle or device in order to send malicious traffic. |
| Vehicle Immobilizer | Hardware based security feature that prevents fuel and spark delivery if not properly authenticated against a vehicle key. | If this device can be bypassed or defeated, an unauthorized person would be able to start the vehicle, resulting in possible vehicle theft. |

# Example – Attack Tree



# Example – Attack Vector Description

| Attack Description: Node 5.2 |
| --- |
| An attacker reverse engineers both the cryptographic cipher and/or authentication protocol of vehicle key fob to simulate a valid vehicle key. Using this simulated key, the attacker is able to start and drive the vehicle as if they had used the proper key. |
| **Attack Classification** |
| Spoofing: The attacker was able to spoof a valid vehicle key by exploiting weaknesses in the cipher and/or protocol. |
| **Attack Threat** |
| This can be considered a ‘class based’ attack where the attack will work against an entire class of devices and not just a single device. In this case, the device class consists of multiple model years of multiple vehicles from multiple manufacturers.<br><br>With the success of this attack, the technology could be sold to potential car thieves. |
| **Suggested Mitigation** |
| [mitigation suggestions go here] |

# Example – Attack Vector Descriptions (EVITA)

| Node 5.2 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Severity[1] | | | | Attack Potential [2] | | | | | Attack Potential Total | Attack Probability [3] | Controllability (safety) | Risk [4] | | | |
| Financial | Operational | Privacy | Safety | Elapsed Time | Expertise | Knowledge | Window of Opportunity | Equipment Required | | | | Financial | Operational | Privacy | Safety |
| 4 | 0 | 0 | 0 | 19 | 8 | 0 | 0 | 0 | 27 | 1 | 0 | 2 | 0 | 0 | 0 |

See http://evita-project.org/Deliverables/EVITAD2.3.pdf for value definitions:

1. table 4
2. table 5
3. table 6
4. table 9

# Questions?

GENIVI®

# Thank You!

GENIVI®