Approaches to Vehicle Security Monitoring

Presentation by **Robert Shein**
November 2019

Introduction

Who I Am

- Senior Manager with PwC Consulting, LLC
- Focused on IoT, Connected/Autonomous Vehicles, Industrial Control Systems
- On secondment to Japan for three years
- This is my second time speaking at SIP-adus
- SIP-adus is where my journey to Japan began!

My Experience

- Nearly 40 years of experience with computer technology
- Approximately 25 years of cybersecurity experience
- Past work includes:
  - Penetration Testing/Red Teaming
  - Incident Response
  - Product Security Testing
  - Security Monitoring
  - Industrial Control System Security

Why I Think This Is Important

- Connected vehicles represent everything that needs defending:
- Enormous amounts of private data
- Potential for significant harm on a large scale
- Payment processing for Mobility as a Service (MaaS) and driverless ride-sharing
- Critical infrastructure; this relates to trucks, and even applies indirectly to shipping

“

Vehicle security monitoring is the greatest challenge that has ever existed in the security monitoring field, but with the correct processes and technology, it can be done. Furthermore, it must be done because without monitoring, the growing level of risk in connected and autonomous vehicles (CAVs) will be unmanageable.

The Challenge of Scale

250,000,000

“By 2020, Gartner predicts there will be a quarter-billion connected vehicles on the road, providing more opportunities for drivers to access information, their content, and stay productive while in the car. As a result, driver safety, and how to keep their data protected, have become a critical topics in the mobile, automotive and security industries.”

Gartner
Staying on Track With Connected Car Security, 2016

The Challenge of Complexity

110-150

Connected Devices per Car

Each vehicle is not a singular device to monitor, but a complete networked environment that includes products from dozens of vendors. The interdependencies between these devices require this level of connectivity to provide a competitive user experience in cars today.

12

Types of Points of Entry

- Telematics
- Bluetooth
- Wi-Fi
- USB
- SD/Micro-SD
- ODB II
- DVD
- SiriusXM
- Digital FM
- Keyless Entry
- TPMS
- Hosted Services

64 Million

New Connected Vehicles Shipping in 2019

Between worldwide consumer demand for features and eCall legislation in Europe, the market penetration of connected vehicles is growing rapidly.

The Challenge of Uniqueness

Proprietary Event Data

In standard IT environments, common communities exist with similar platforms (operating systems, cloud services, applications) which all generate standardized event data.

In vehicles, event data is unique to the manufacturer, and is also proprietary in nature.

As a result, collaboration is difficult or impossible to determine common event patterns.

Vehicles are Unlike Other Devices or Systems

Vehicles are not designed or built like either IT or OT environments.

Communications (especially over CAN) and the limited computing power of most microcontrollers make both event analysis and event generation difficult.

As a result, current approaches to security monitoring are insufficient to monitor vehicles.

Security Monitoring in Vehicles is a Lifetime Cost

Unlike security monitoring in one’s own IT environment, security monitoring of a vehicle that has been sold exists long after the architecture/design/construction of that vehicle has been retired.

As a result, security monitoring of vehicles will pose cost challenges long after those vehicles have been sold.

Other Assorted Challenges

Whose Network is it, Anyway?

Unlike an IT environment, the vehicle belongs to someone other than the organization doing the monitoring.

This means that an attacker can often disable/stop monitoring of a vehicle, if they are in possession of that vehicle.

“Sure, We Would LOVE to Sell You $12,000,000,000 Worth of Licenses For <INSERT SIEM HERE>”

Current models for scaling, pricing, and deploying SIEMs do not work for vehicles.

No SIEM solution made today is well-suited to monitoring vehicles.

“What Data *Do* We Have to Work With?”

Both event data generation and collection is uneven, even within a single manufacturer.

Traditionally, data has been collected for reasons related to entire fleets, not single vehicles.

Goal: Cooking

Security monitoring is like cooking…

The technology is the kitchen

The events are the ingredients

The event correlation logic are the recipes

The best security monitoring capabilities work like a restaurant…

A variety of prepared foods

Able to serve food to a variety of diners and tastes

Reliable quality

Technology (The Kitchen)

These are the tools used to collect and monitor event data

SIEM – “Security Information and Event Manager”

Examples:

- ArcSight
- LogRhythm
- AlienVault
- Splunk

Current licensing models for SIEM tools do not fit the use case for vehicle security monitoring

Event Data (The Ingredients)

Identity:

- Data must be tied to vehicle
- The device(s) to which they relate must also be clearly identifiable

Delivery:

- Unreliable communications (car parked in an underground garage, car in a tunnel)
- Devices generating events which have no concept of a network or routing

A New Problem:

- *No two car manufacturers generate the same events*

Correlation Logic (The Recipes)

Since the majority of security events are new, the majority of recipes are unknown

The proprietary nature of the underlying systems means that information sharing is not possible:

- No existing community to draw upon
- Third-party vendors cannot define correlation logic for the manufacturer
- Every manufacturer's body of events is unique

Summary

There are several challenges unique to security monitoring in vehicles, related to the nature of the data, collecting it, and identifying attacks

Things that need to be done to address these challenges:

- Define a data plan defining event data to be generated by vehicles
- Determine how to tag and transport that data to collect it
- Establish baseline rules to identify known attacks
- Build processes to maintain security monitoring capabilities and improve them over time

Thank you

pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.