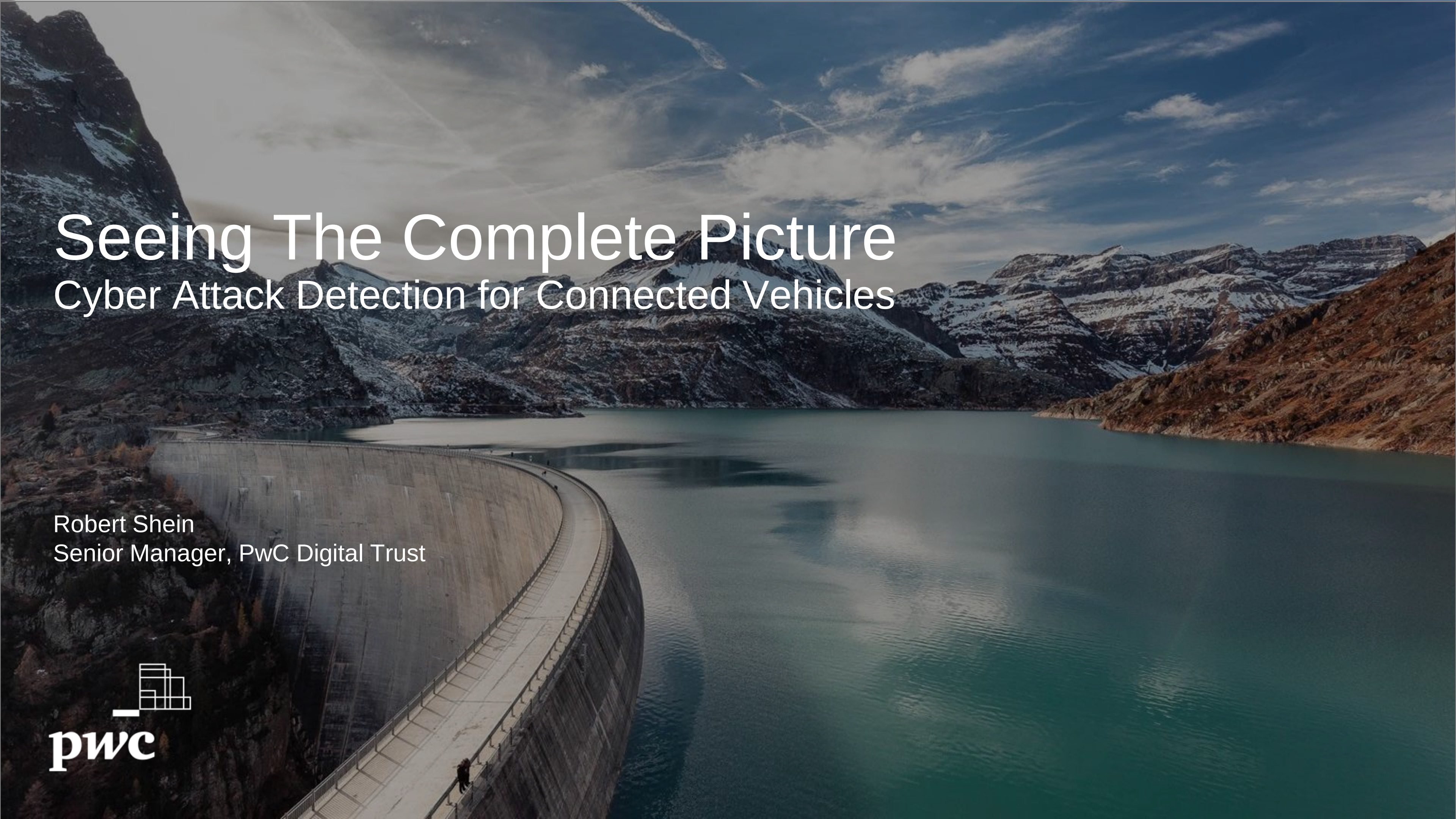


Seeing The Complete Picture

Cyber Attack Detection for Connected Vehicles

Robert Shein
Senior Manager, PwC Digital Trust

The Challenge:

How do we monitor for future attacks we have never seen with unproven technology?

Introduction

Who I Am

- Senior Manager with PwC Consulting, LLC
- Focused on IoT, Connected/Autonomous Vehicles, Industrial Control Systems
- This is my third time speaking at SIP-adus

My Experience

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

Why I Think This Is Important

- Connected vehicles need to be both trustworthy and trusted
- Autonomous vehicles can bring enormous benefits when safely and securely designed
- Potential for significant harm on a large scale exists if they are not secure
- Vehicles are a crucial part of national infrastructure, everywhere

The Security Monitoring/Attack Detection Challenge: How Do You Find What You Haven't Seen Yet?

Proprietary Devices, Commands, and Data

- Unlike standard IT environments, the devices in vehicles are largely proprietary in nature. Vulnerabilities in a car made by one OEM are not necessarily found in other cars by other OEMs.

Data Backhaul Challenges

- Telematics connectivity is less reliable than within IT ecosystems and is often blocked (tunnels, underground garages, rural areas).

Attacks Are an "X-Factor"

- Nearly all IDPS systems depend upon signatures of known attacks. But attacks against and within vehicles are still largely unknown, making it difficult for a vendor to produce a solution that can recognize attacks that happen before a vehicle is already compromised.

Cost Constraints

- Even a small added cost to each vehicle results in tens or hundreds of millions of dollars of lost profit. This problem becomes worse for solutions that need to monitor more than one part of a CAN bus, or more than one type of network simultaneously.

The Encryption Problem

- Implementation of encryption within a vehicle can impair or entirely prohibit an internally-based IDPS solution from seeing attacks.

Important Points

IDPS solutions in the IT space have evolved over decades and still miss a large number of attacks.

The IT world has addressed this by moving their visibility to the endpoints; this is why EDR (Endpoint Detection and Response) have become popular.

The Ability to Learn is Important

Vehicle monitoring needs to take a “Blue Team” approach

Learning from IT security’s lessons

Without better understanding of what attacks may look like in a vehicle, the best approach is creating the ability to gather information to find new patterns.

This is the same approach used in IT security, against advanced attackers who change their tactics.

Fortunately, most vehicles produced these days contain a system that can be used to do this quite effectively: an EDR (Event Data Recorder).

Important Points

Data gathering in the IT world to detect new types of attacks is a relatively new approach, and it works very well.

There is no need to repeat the same mistakes that were made in security monitoring in other industries; their lessons can be applied to vehicular security.

Event Collection Has Other Uses

By defining a standardized approach to data definition, collection, and handling, additional benefits can help offset the cost of security monitoring

Useful Data for Multiple Functions

By collecting data in a coordinated fashion, it becomes possible to support not only security efforts but other business functions including:

- Defect management
- Bulk (anonymous) census gathering of models still in use
- Recall coverage measurement
- Product lifespan assessment

Many of these capabilities can reduce in lower costs, and can also lead to other services that can be offered to clients (such a fleet management) which can generate revenue.

This revenue can help offset the cost of security monitoring.

Important Points

Vehicles can produce many forms of useful data.

In many automotive companies, this data is collected inconsistently with no central governance over privacy or data handling.

Doing this in a more strategic way can allow security to help support other business functions and save money.

Other Ways to Approach IDPS

Monitoring can be done at the vehicle perimeter by putting IDPS in the telematics support infrastructure

Using the Tools Available Today

Traffic passing over remote telematics communication can be monitored for suspicious traffic by putting IDPS solutions into the networks that support telematics.

This approach scales well, and is easier to update over time as more information becomes available about types of attacks.

This approach also allows a hybrid view of attacks, and provides understanding of whether attacks happen locally at the vehicle or remotely across telematics communication networks.

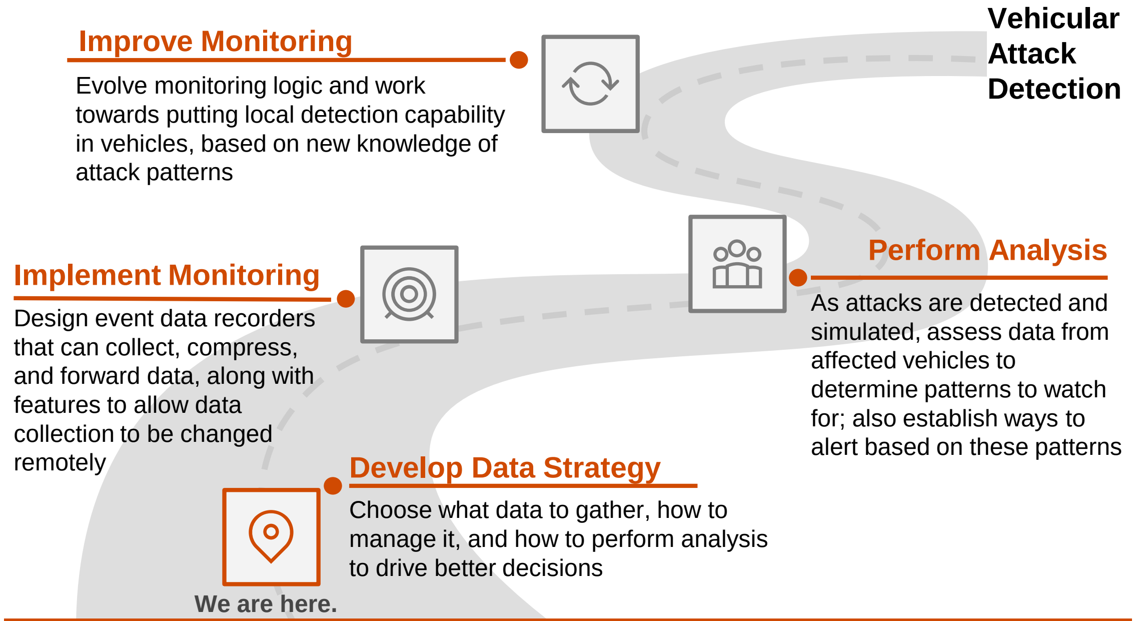
Important Points

Traffic passing over telematics is easier to monitor than traffic within a vehicle, as it uses communications protocols which are already suited for monitoring with existing technology.

Telematics is still the largest attack surface for vehicles; monitoring this avenue of attack is important.

Evolution of IDPS Over Time: A Point of View

When all of these steps are seen together, a pathway towards cost-efficient and effective security monitoring within vehicles emerges.



We are here.

Develop Data Strategy

Choose what data to gather, how to manage it, and how to perform analysis to drive better decisions

Implement Monitoring

Design event data recorders that can collect, compress, and forward data, along with features to allow data collection to be changed remotely

Perform Analysis

As attacks are detected and simulated, assess data from affected vehicles to determine patterns to watch for; also establish ways to alert based on these patterns

Improve Monitoring

Evolve monitoring logic and work towards putting local detection capability in vehicles, based on new knowledge of attack patterns

Vehicular Attack Detection

Cost-effective, in-vehicle IDPS devices may not be possible using current technology and understanding of attacks. More understanding is needed to develop an effective solution that meets the needs of both OEMs and customers.

Thank you

pwc.com/consulting