MULTILAYERED CYBERSECURITY ARCHITECTURE AND SUITE

ALON ATSMON
VP TECHNOLOGY STRATEGY

HARMAN

CTG
Corporate Technology Group

WHY CYBERSECURITY

cybersecurity
Search term

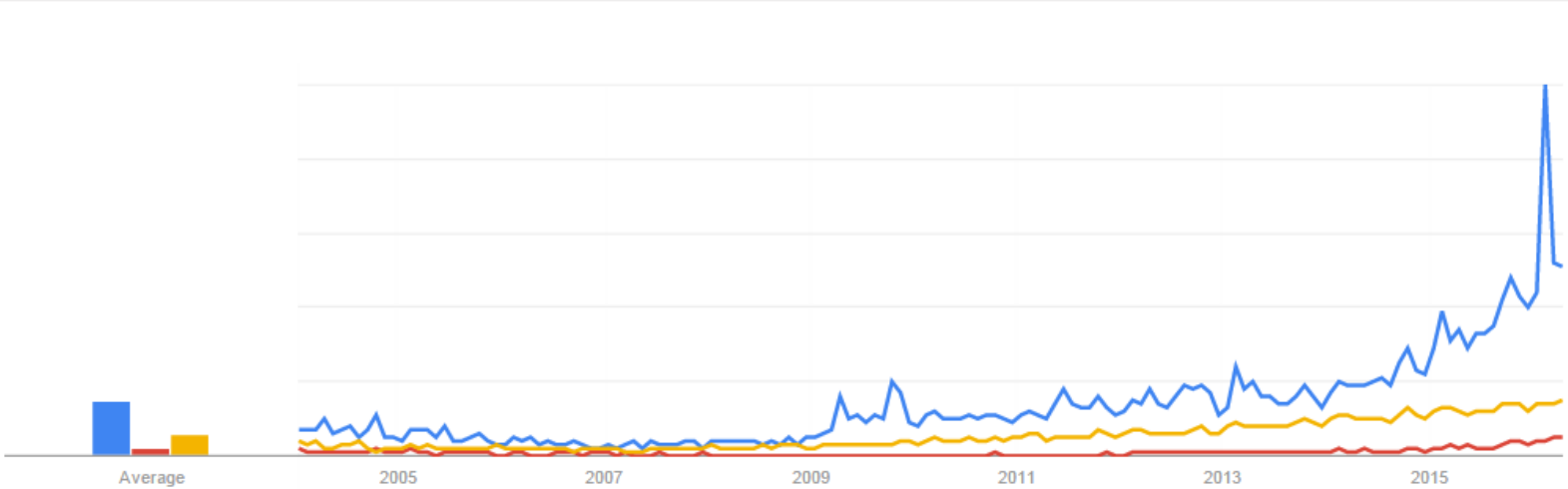
autonomous driv...
Search term

connected car
Search term

+ Add term

Interest over time

News headlines Forecast



AGENDA

1. Industry Background
2. What We Do
3. The Problem
4. The 5+1 Solution
5. Network Protection
6. Summary

WHO WE ARE

HARMAN IN NUMBERS

- **$6.5** Billion revenues*
- **$23** Billion automotive order backlog**

*Last 12 Months as of December 31 2015
**As of June 30, 2015

MARKET LEADER

- **28,000** Professionals worldwide
- **12,600** Engineers
- **25+** Countries: Americas, Europe and Asia
- **16+** Legendary brands

GLOBALLY DIVERSE

- **5,900** Patents and patents pending
- **51** Design awards in 2014
- **3** GRAMMY® Awards-AKG, JBL, Lexicon
- **2** Academy Awards

INNOVATION LEADER

WHAT WE DO

CONNECTED CAR

Navigation, Multimedia, Connectivity, Telematics, Safety & Security Solutions

LTM Revenue* $2,981M

LIFESTYLE AUDIO

Premium Branded Audio products for use at home, in the car and on the go

LTM Revenue* $1,975M

PROFESSIONAL SOLUTIONS

Audio, Lighting, Video Switching and Enterprise Automation for Entertainment and Enterprises

LTM Revenue* $1,023M

CONNECTED SERVICES

Cloud, Mobility and Analytics Software Solutions along with OTA update technologies for Automotive, Mobile and Enterprises

LTM Revenue* $583M

EBITDA is non-GAAP measure and excludes restructuring, non-recurring charges and acquisition-related items. LTM = Last 12 Months ending Dec 31, 2015.
**Includes intercompany revenues.*

IN THE MOST ADMIRED VEHICLES

WHO WE ARE

A CENTURY OF INNOVATION

1928
World's first talking movie features Lansing's HD loudspeakers

1937
MGM-Lansing sound System wins first of two Academy Awards

1948
First ever in-car radio

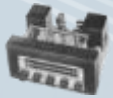
1949
Crown introduces first open reel tape recorder with built-in power amp

1953
Harman Kardon introduces first FM tuner

1953
AKG invents world's first dynamic cardiod microphone

1956
Sidney Harman buys out Bernard Kardon and creates Harman International

1958
Harman Kardon releases the world's first stereo receiver



1969
JBL powers first of three Woodstocks

1970's
JBL co-develops the Wall Of Sound for the Grateful Dead

1971
DBX brings realism of live performance to recorded music

1975
Becker launches first car cassette radio

1983
Crown taps JBL to develop first THX licensed system

1983
George Lucas selects JBL to develop the first THX licensed theater audio system

1984
JBL in Lincoln Town Car Premiers as First OEM Branded Car Audio System

1987
Martin lights up the dance floor with disco lights and fog machines

1989
Digitech Whammy first foot-controlled pitch shifting guitar pedal

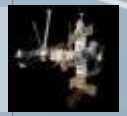
1997
First car radio/CD/nav. system

1999
HK Soundsticks debut at MOMA

2002
Three JBL engineers receive Academy Awards

2004
Harman enables first Bluetooth wireless connectivity in the car

1991
AKG binaural products used on Mir Space Station



2004
JBL one of first to release audio docks for iPod.

2008
STC joins OHA and enables Android for the CDMA market

2012
JBL introduces Flip

2013
STC developed the first dual-sided smartphone for Yota

2014
HARMAN wins third GRAMMY

2015
STC launches Marimba Cloud– World's first, most comprehensive cloud based IoT management platform

THE PROBLEM

CONNECTED CAR

BENEFITS COME WITH CHALLENGES

HARMAN

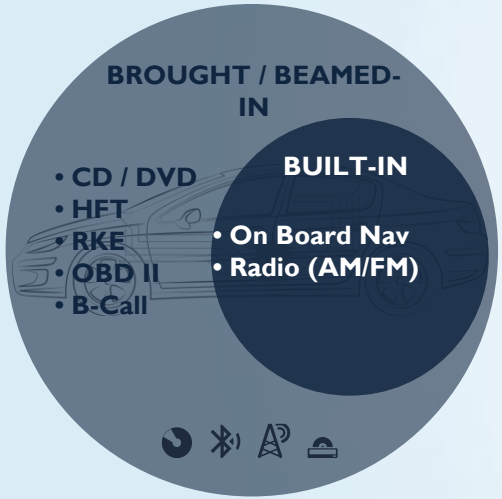
CONNECTED CONTENT aha by HARMAN

CONNECTED SERVICES st symphony teleca

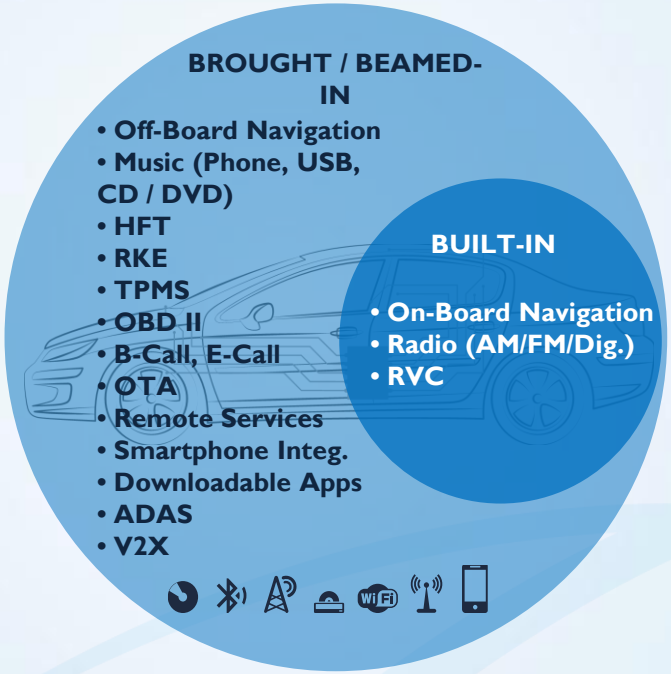
CONNECTED UPGRADES redbend

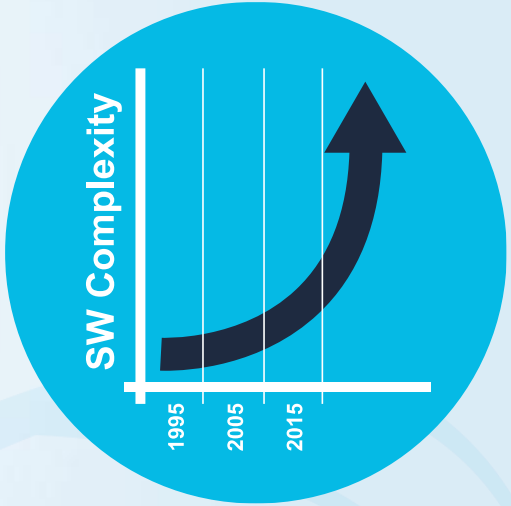
EXPONENTIAL COMPLEXITY

NOT SO DISTANT PAST

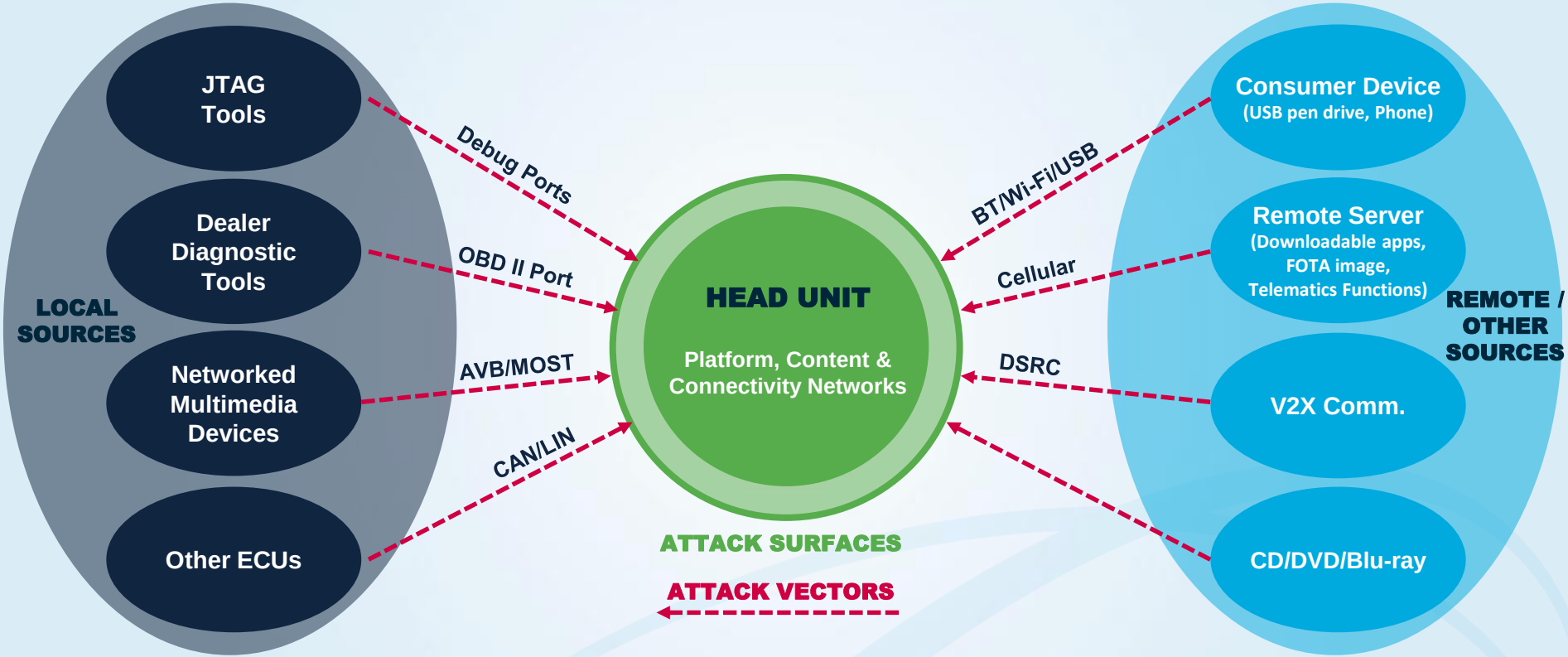


NOW & THE NEAR FUTURE

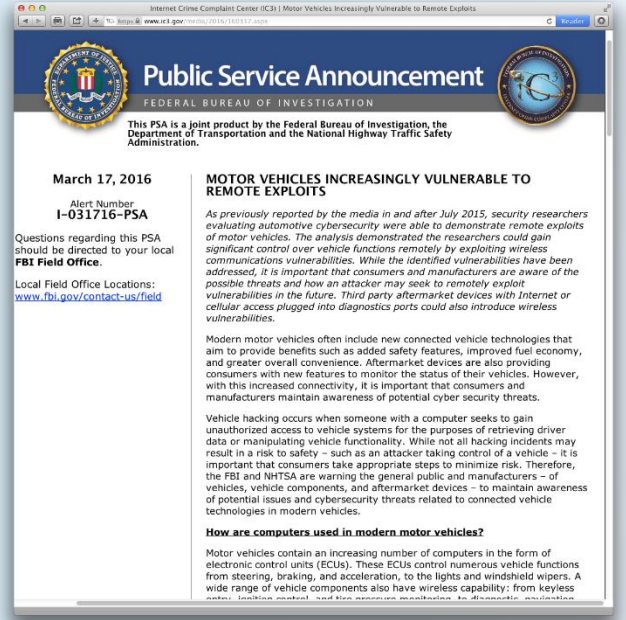




POTENTIAL ATTACK SURFACES



SECURITY CONCERNS ARE GROWING



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

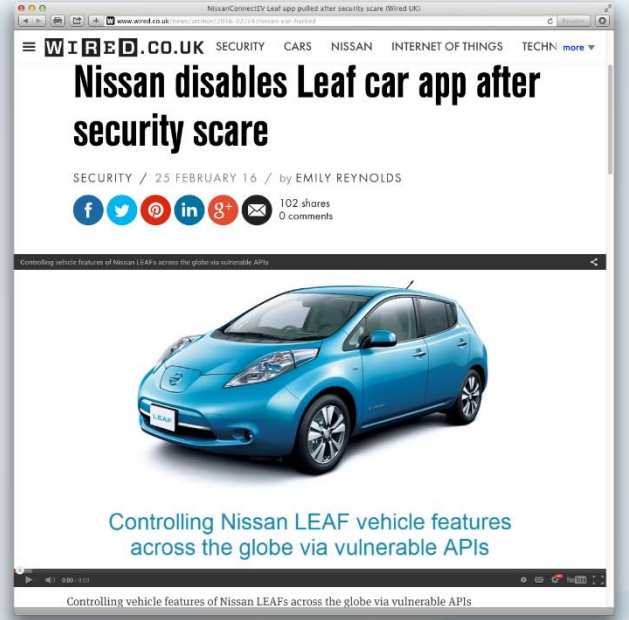
As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. While not all hacking incidents may result in a risk to safety – such as an attacker taking control of a vehicle – it is important that consumers take appropriate steps to minimize risk. Therefore, the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles.

How are computers used in modern motor vehicles?

Motor vehicles contain an increasing number of computers in the form of electronic control units (ECUs). These ECUs control numerous vehicle functions from steering, braking, and acceleration, to the lights and windshield wipers. A wide range of vehicle components also have wireless capability: from keyless



WIRED.CO.UK SECURITY CARS NISSAN INTERNET OF THINGS TECHN more

Nissan disables Leaf car app after security scare

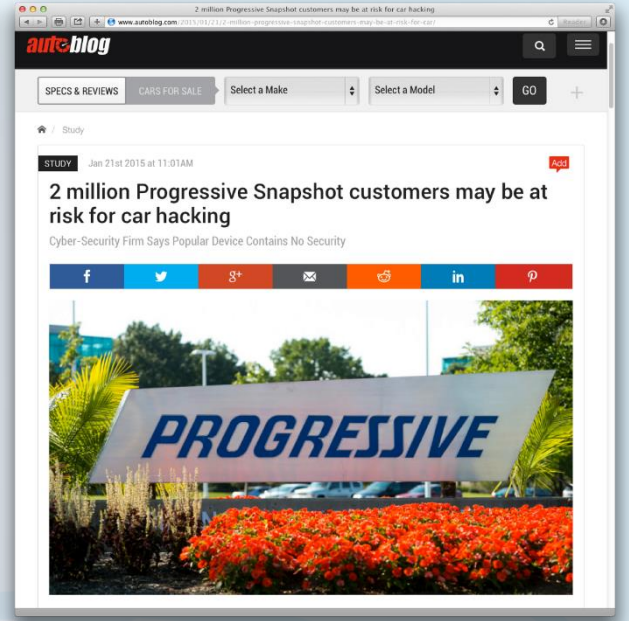
SECURITY / 25 FEBRUARY 16 / by EMILY REYNOLDS

102 shares
0 comments

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs

Controlling Nissan LEAF vehicle features across the globe via vulnerable APIs

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs



autoblog

SPECS & REVIEWS CARS FOR SALE Select a Make Select a Model GO

Study

STUDY Jan 21st 2015 at 11:01AM

2 million Progressive Snapshot customers may be at risk for car hacking

Cyber-Security Firm Says Popular Device Contains No Security

GOVERNMENT

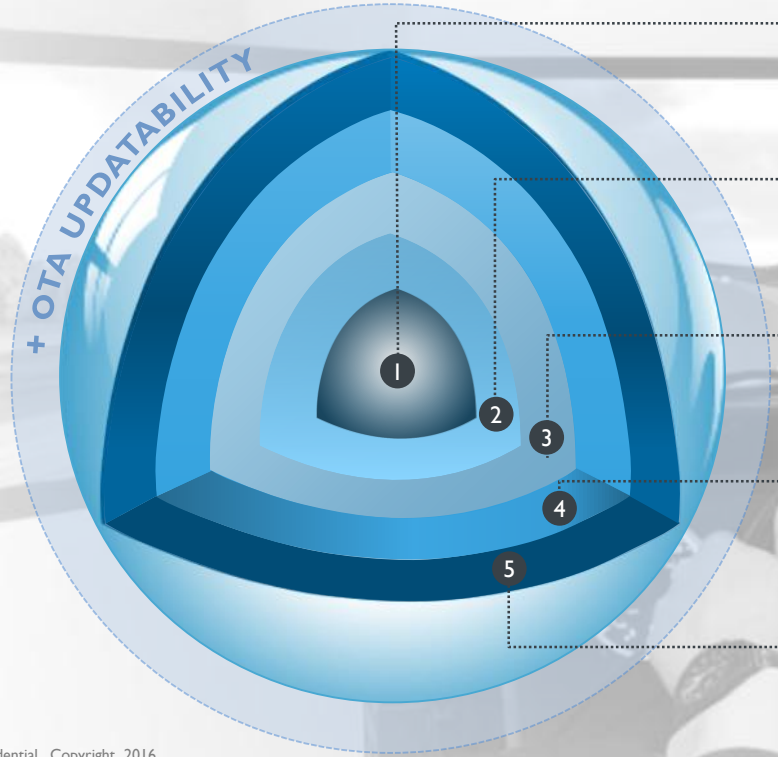
OEM

AFTERMARKET

THE SOLUTION

MUTILAYERED APPROACH

5+1 CYBERSECURITY ARCHITECTURE



1. SECURE HW PLATFORM

TAMPER RESISTANCE

2. HYPERVISOR

DOMAIN SEPARATION

3. OS ACCESS CONTROL

AUTHORIZATION POLICY

4. APPLICATION SANDBOXING

APPLICATION ISOLATION

5. NETWORK PROTECTION

INTRUSION PROTECTION

LAYERS 1 AND 2

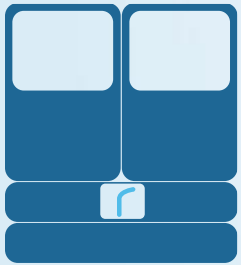
5+1 CYBERSECURITY ARCHITECTURE

SECURE HARDWARE PLATFORM

Ensures product security with trusted execution environment

1. Secure Boot and "Chain of Trust" ensures only authorized SW runs in the system
2. Protected storage and generation of cryptographic keys
3. Can control access to peripherals thru HW Firewall
4. Improves performance thru HW accelerated encryption/ decryption

HYPERVISOR



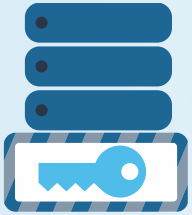
Multiple operating systems on the same hardware

1. Separates environments with different security requirements
2. Isolates the virtual machines using hardware mechanisms
3. Reduces system cost by eliminating the need for a second processor to provide isolation

5+1 CYBERSECURITY ARCHITECTURE

HARMAN

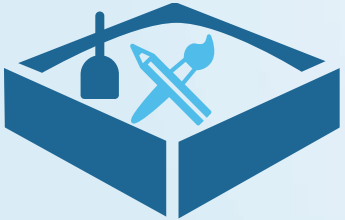
SYSTEM RESOURCE ACCESS CONTROL



Controls access based on system and functional requirements

1. Authenticated and authorized access to critical resources and sensitive data
2. Restricted Access to resources as per defined policies

APPLICATION SANDBOXING



Multiple applications run in isolated environment

1. Separates "external facing" (vulnerable apps) from other apps in the system
2. Limits system resources usage by each application
3. Limits capabilities of privileged apps

LAYER 5 AND OTA

5+1 CYBERSECURITY ARCHITECTURE

NETWORK PROTECTION

Secure communication channels and external interfaces

1. Secure, Encrypted Networking
2. Detect and protects against anomalous external data

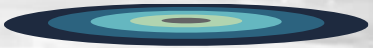
OTA UPDATABILITY

Continuous security of software and digital assets

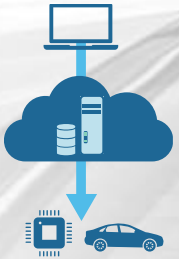
1. Secure SW updates against exploits and vulnerabilities
2. Reduces risk of eavesdropping and impersonation by updating compromised authentication vectors

KEY TAKEAWAYS

CONNECTED CAR BENEFITS COME WITH CHALLENGES



MULTILAYERED SOLUTION NEEDED



OTA AND NETTWORK PROTECTION ARE KEY

THANK YOU

ALON ATSMON, VP TECHNOLOGY STRATEGY

ALON.ATSMON@HARMAN.COM

WHAT IS ECUSHIELD?

ECUSHIELD

is an embedded software solution which provides an on-board automotive Cyber Security against hacking, intrusion and critical communication disruptions.

PROTECTING AGAINST

HARMAN

SPOOFING	ABUSE OF "LEGITIMATE" OPERATIONS	SOFWARE EXPLOITS	DENIAL OF SERVICE
Example: Spoofing of CAN messages from an external device / compromised ECU	**Example:** Using Diagnostic commands to cause undesired actions	**Example:** Manipulate the communication to exploit vulnerabilities in the code	**Example:** Flooding the CAN bus

ECUSHIELD KEY FEATURES

DETECT NEW THREATS

MARK THE MALICIOUS COMMUNICATION

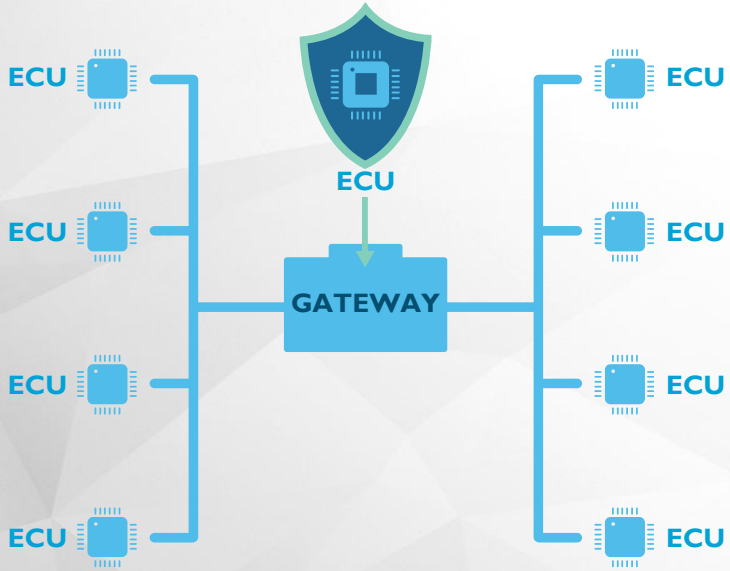
MITIGATE THE THREAT IN REAL-TIME

IDENTIFY THE THREAT SOURCE

NO PREVIOUS KNOWLEDGE ABOUT THE SPECIFIC ATTACK IS NEEDED !

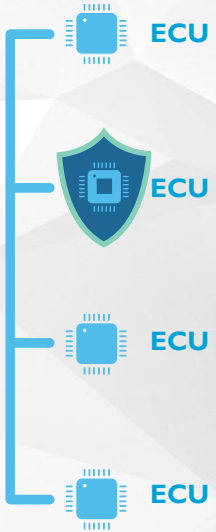
TYPICAL APPLICATIONS

SMART FIREWALL



ECUSHIELD installed on Gateway ECU acting as both an IDS and as a Firewall

IDS / IPS



ECUSHIELD installed on one of the ECUs acting as either an IDS or and IDS/IPS

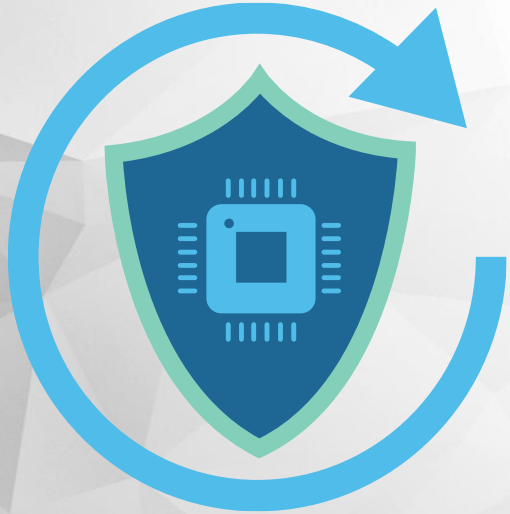
PRODUCT HIGHLIGHTS

HARMAN

- Easily embedded into proprietary systems and various OS
- No redesign - integration into existing CAN architectures
- Built for low resources and real-time environments
- Built-in Secured update mechanism
- Single installation provides full mitigation capability "Cooperative Mitigation"

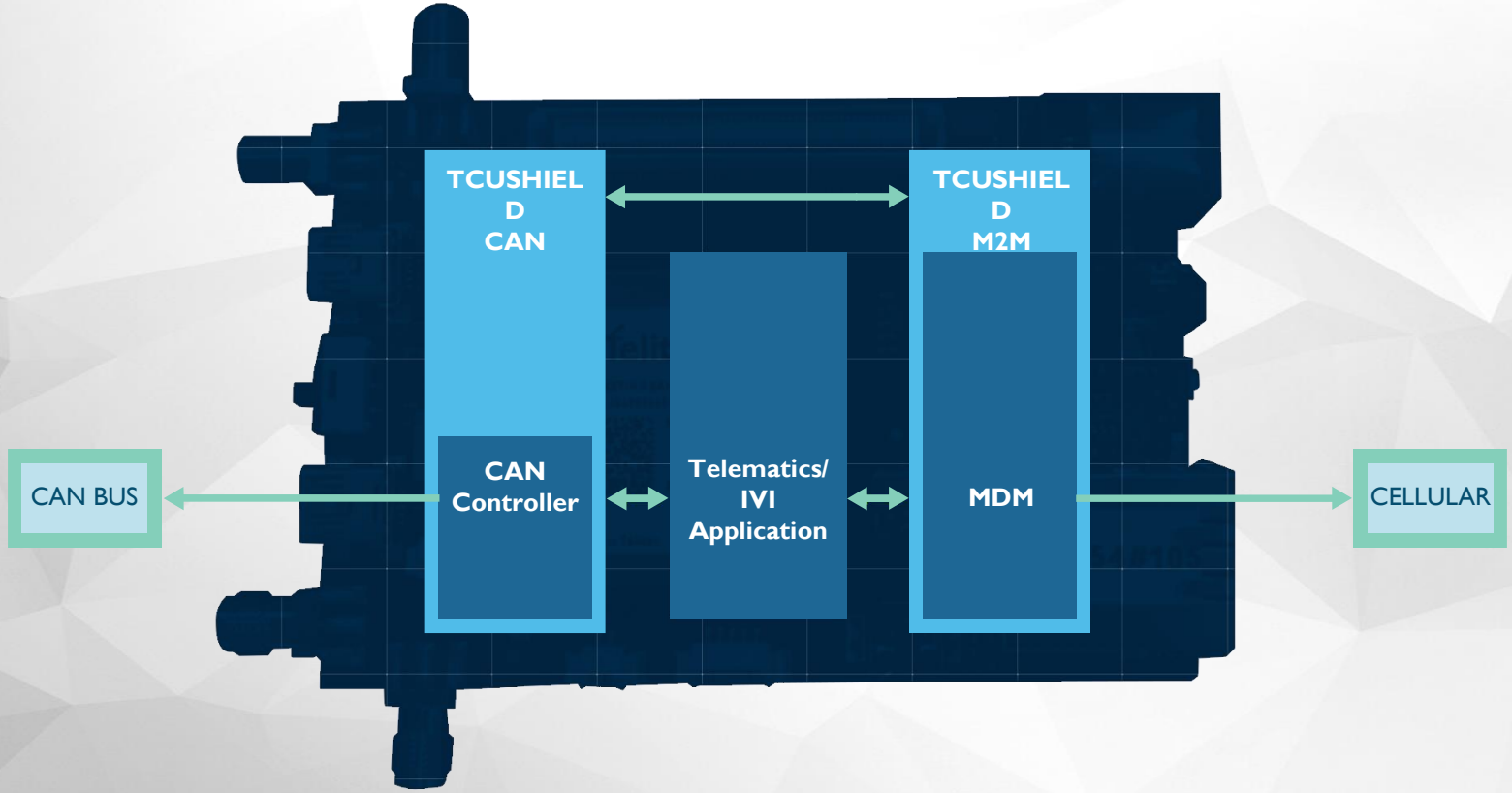
NO PREVIOUS KNOWLEDGE ABOUT THE SPECIFIC ATTACK IS NEEDED !

TCUSHIELD KEY FEATURES



- **Secure Telematics based on existing hardware**
- **24/7 monitoring & prevention**
- **Zero installation downtime**
- **Always updated**
- **What does it do ?**
  - Identify the malicious communication
  - Selectively blocks communication in real-time
  - Provide information for further analysis
  - Safe-guards the in-vehicle network against compromised TCU/IVI

TCUSHIELD KEY FEATURES



INTEGRATED INTO EXISTING TSP INFRASTRUCTURE

HARMAN