

**Netsecuris**  
Who's watching your network?

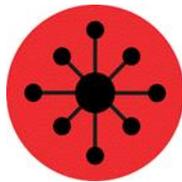
# Trains, Planes, & Automobiles Reducing cyber security risks

Presented by Leonard Jacobs, MBA, CISSP, CSSA  
Founder, President and CEO of Netsecuris Inc.



## **What is it about? What it is not?**

- This presentation is about:
  - The What-ifs
  - The possibilities
- This presentation is not about:
  - Absolutes
  - Products



**Netsecuris**  
Who's watching your network?

# Are we still sure there is no cyber risk?

## The Telegraph

Search - enhanced by OpenText

Sunday 11 October 2015

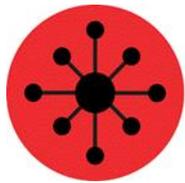
[Home](#) [Video](#) [News](#) **[World](#)** [Sport](#) [Finance](#) [Comment](#) [Culture](#) [Travel](#) [Life](#) [Women](#) [Fashion](#) [Luxury](#) [Tech](#) [Cars](#) [Film](#) [TV](#)

[USA](#) [Asia](#) [China](#) [Europe](#) [Middle East](#) [Australasia](#) [Africa](#) [South America](#) [Central Asia](#) [KCL Big Question](#) [Expatriate](#) [Honduras](#)

---

[HOME](#) » [NEWS](#) » [WORLD NEWS](#)

### Schoolboy hacks into city's tram system



**Netsecuris**  
Who's watching your network?

# Is Rail Immune?



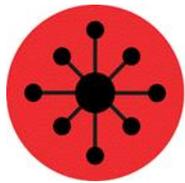
## **HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS**



By [Aliya Sternstein](#)

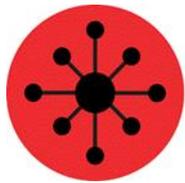
January 23, 2012

 1 Comment



# Rail Systems Potentially Vulnerable

- Train Operations
  - HMI
  - Propulsion
  - Braking
  - Door Controls
  - Signaling Interfaces
  - Automatic Train Control
- Fire Detection
- Emergency Systems
- Remote Diagnosis/Fault Monitoring
- Remote Software Updates



**Netsecuris**  
Who's watching your network?

# Are Aircraft Immune to Cyber Attacks?



## The Ever-evolving Cyber Threat to Planes

By [AFP](#) on June 17, 2015



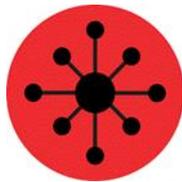
**Netsecuris**  
Who's watching your network?

# Are Aircraft Really Immune to Cyber Attacks?



## FBI Says Researcher Admitted Hacking Airplane in Mid-Flight

By [Eduard Kovacs](#) on May 18, 2015



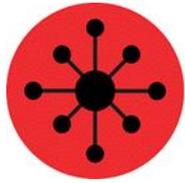
**Netsecuris**  
Who's watching your network?

# What about Internet Connectivity with Aircraft Systems?



## Internet Connectivity Could Expose Aircraft Systems to Cyberattacks: GAO

By [Eduard Kovacs](#) on April 15, 2015



**Netsecuris**  
Who's watching your network?

# Aircraft controls are getting more sophisticated





**Netsecuris**  
Who's watching your network?

# Is there cyber security risk in the world of motion?



Cyber-Safe

## Chryslers can be hacked over the Internet



**Netsecuris**  
Who's watching your network?

# Are we absolutely, positively sure?



Technology

CyberSecurity

## Canadian military seeks hackers to build exploits and defences against connected car cyberattacks



By *Mary-Ann Russon*

October 7, 2015 14:29 BST





**Netsecuris**  
Who's watching your network?

# A Different Cyber Attack on Car



Hackers Cut a Corvette's Brakes Via a Common Car Gadget

[ANDY GREENBERG](#) SECURITY 08.11.15 7:00 AM

## HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET



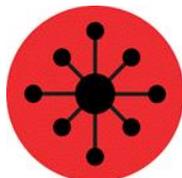
**Netsecuris**  
Who's watching your network?

# Not another automobile attack!



## **BMW Patches Security Flaw That Let Hackers Open Doors**

By [Brian Prince](#) on February 02, 2015



**Netsecuris**  
Who's watching your network?

# Oh no! Can we safely drive a car?

**welivesecurity**  
Security news, views and insight from the ESET experts

## FBI warn that automobiles are vulnerable to cyberattacks

BY **KARL THOMAS** POSTED 18 MAR 2016 - 06:40PM



**Public Service Announcement**  
FEDERAL BUREAU OF INVESTIGATION

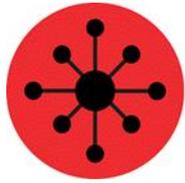
This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

**March 17, 2016**

Alert Number  
**I-031716-PSA**

### **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*



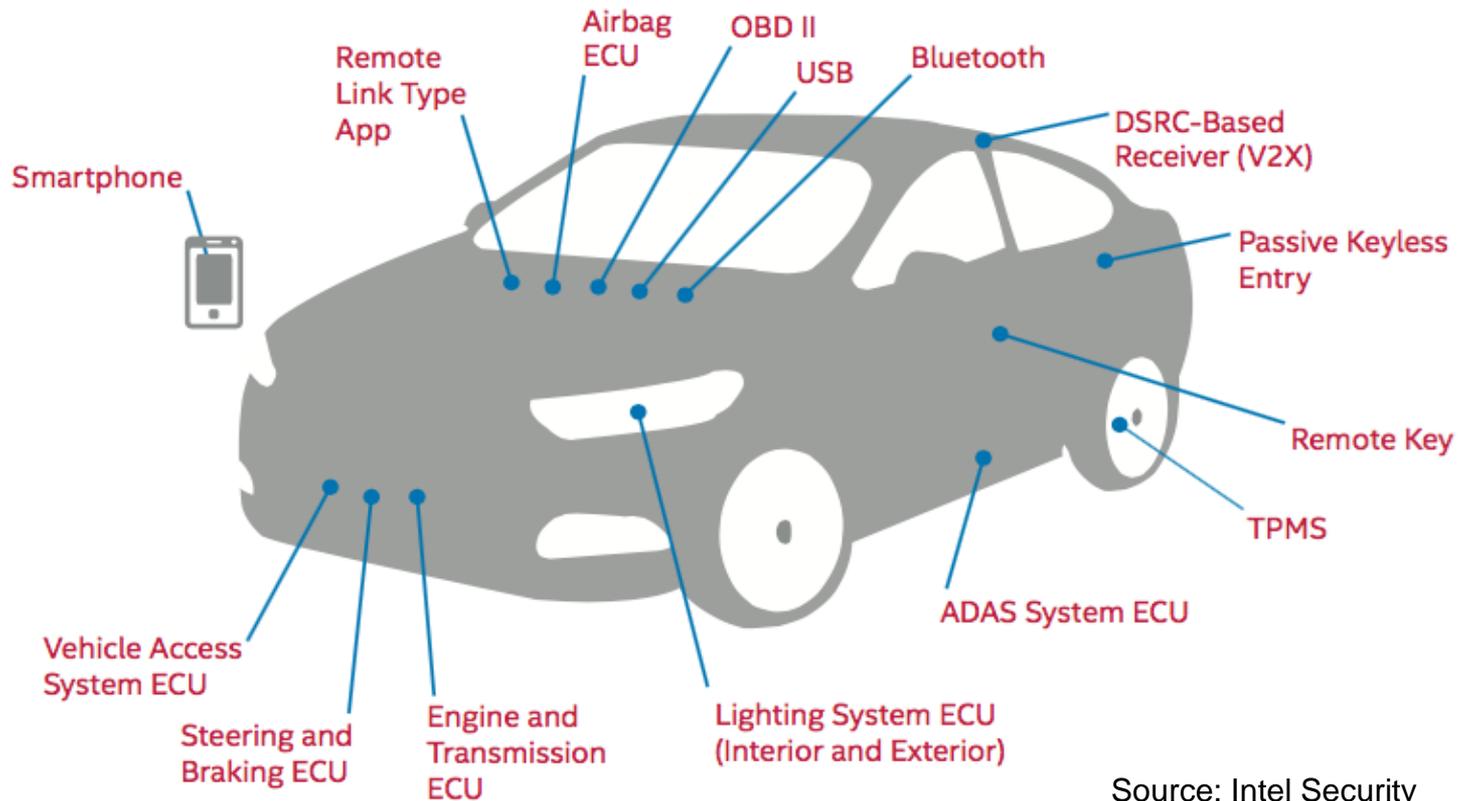
**Netsecuris**  
Who's watching your network?

When you connect a car to the Internet, it is no longer just a car: It is a computer on wheels.

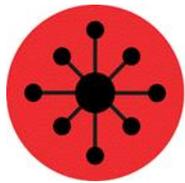
There is legislation aptly named the “Security and Privacy in your Car Act” is currently in consideration by Congress.



# Cyber Attack an Automobile

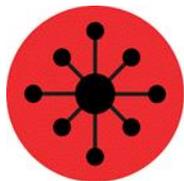


Source: Intel Security

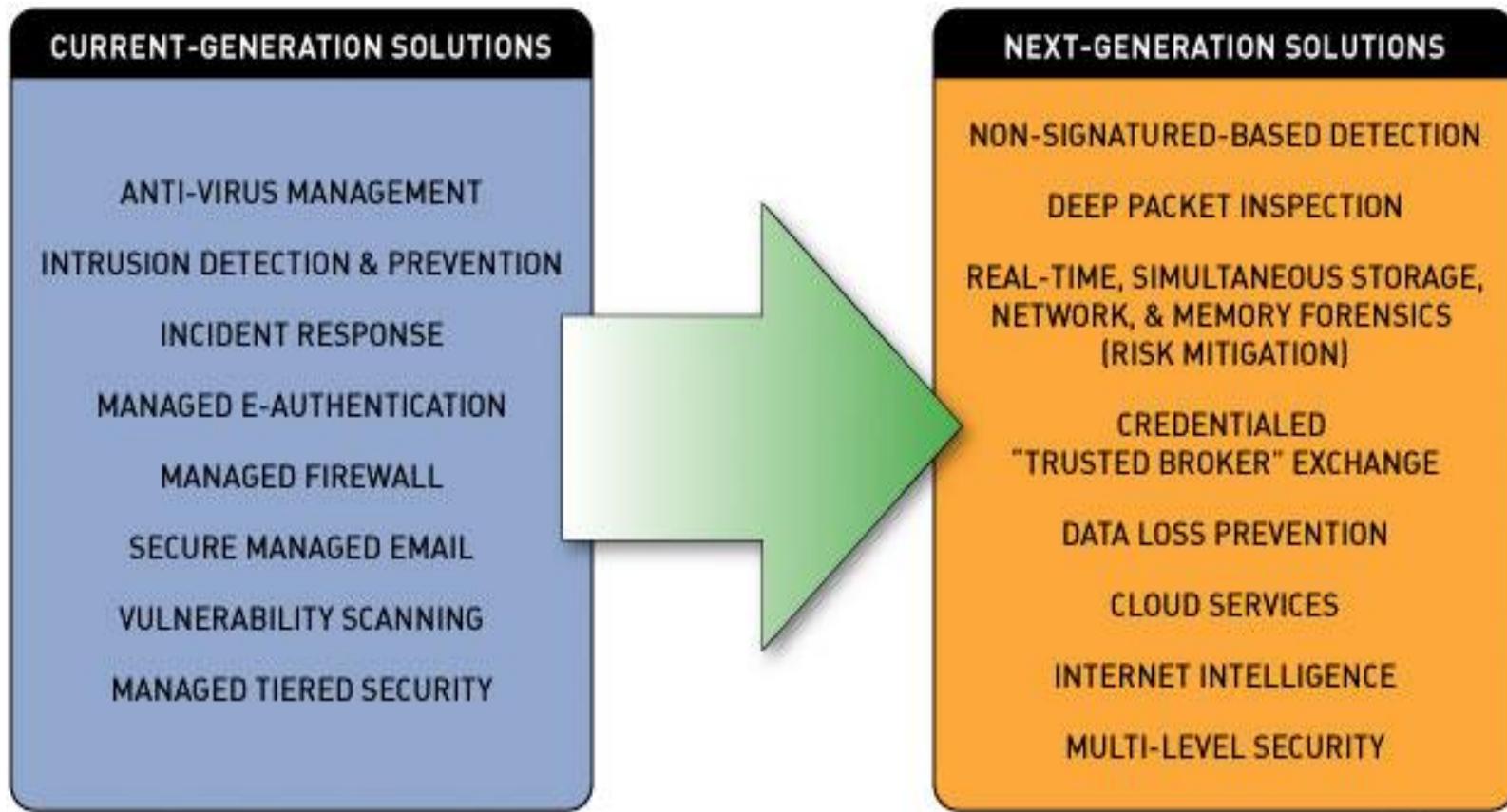


# Internet of Things

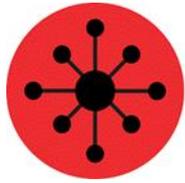
- Shift in Cybersecurity Thinking
  - Expands the cybersecurity landscape
  - Old ways vs. New ways
    - Take traditional cybersecurity security measures and adapt
    - Ability to apply traditional cybersecurity measures as is
- IOT Sensors



# Cybersecurity Solutions

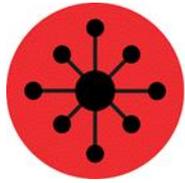


Source: U.S. General Services Administration (GSA)



# Non-signature based Detection/Prevention

- Not traditional Anomaly Detection/Prevention
- Behavioral Baselineing
  - Determining what is normal
  - Looking for the unusual



**Netsecuris**  
Who's watching your network?

# Network Security Monitoring

- Not dependent on any one source of data
- Uses the best computer we have
- Threat Centric vs. Vulnerability Centric
  - Goalie vs. Brick Wall



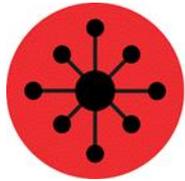
# Network Security Monitoring

- Threat Centric
  - Prevention will eventually fail
  - Focuses on collection
  - Combines intelligence with every attack
  - Cyclical process
  - Not just reliant on known signatures



# Network Security Monitoring

- Tools
  - Suricata (Open Information Security Foundation)
  - Bro
  - Wireshark (Tshark)
  - TCPDump
  - Netflow
  - Security Onion



# Network Cloaking

- Host Identity Protocol (HIP)
  - IETF RFC 7401 Host Identity Protocol v2 and RFC 4423 HIP Architecture
  - HIP separates the end-point identifier and locator roles of IP addresses.
  - In HIP networks, IP addresses are eliminated and replaced with cryptographic host identifiers.
  - HIP is ideal for cloaking the identity of ICS devices and hiding their IP address.



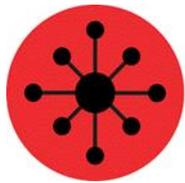
# Network Cloaking

- Implements “Zero Trust” Model
  - Device A trusts Device B but not Device C
  - But Device B can be allowed to trust Device C
- Secure the communications even further with high level of encryption so no traffic can be interpreted except by the end points that trust each other.
- All orchestrated efficiently and quickly



# Cybersecurity Intelligence

- Those with the data will be the “winner.”
- Provides an “early warning system.”
- Feeds your cybersecurity control devices
- Examples:
  - CRISP Program
  - SoltraEdge
  - A whole slew of commercial and free resources



# Miniaturization of Cybersecurity™

- Integration of cybersecurity onto silicon
  - EZ Chip -> Mellanox (Tilera) and Suricata
  - Intel's acquisition of McAfee
- Firewall and IDS/IPS Everywhere
- Fast Response Times



**Netsecuris**  
Who's watching your network?

# Contact Information

**Leonard Jacobs, MBA, CISSP, CSSA**

President/CEO

Email: [ljacobs@netsecuris.com](mailto:ljacobs@netsecuris.com)

Office: +1 (952) 641-1421

# Thank You and Questions