Netsecuris
Who's watching your network?

Trains, Planes, & Automobiles - Reducing Cybersecurity Risks

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

Netsecuris
Who's watching your network?

Bio in a Nutshell

- Over 34 years of technology experience
  - Minicomputers in Industrial Control, Medical Equipment, Healthcare, and Financial Services
- Over 14 years of cybersecurity experience
  - Financial Services and Utilities/Industrial Controls
- Started Netsecuris in Year 2000 to provide cost-effective cybersecurity assessment services. Morphed into a Managed Security Service Provider 5 years later that still performs assessment services too.

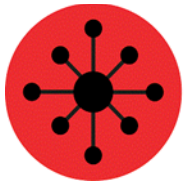
Netsecuris
Who's watching your network?

Albert Einstein stated, "We cannot solve our problems with the same thinking we used when we created them."

Netsecuris
Who's watching your network?

What is it about? What it is not?

- This presentation is all about:
  - What-ifs
  - Possibilities
  - Promoting Concepts
- This presentation is not about:
  - Absolutes
  - Promoting Products per se



Cybersecurity of Motion

- Our World is full of motion
  - Planes
  - Trains
  - Automobiles
  - Trucks
  - Ships
  - Motors
  - All sorts of industrial devices
- What if they were cyber attacked?

Netsecuris
Who's watching your network?

Are Aircraft Immune to Cyber Attacks?

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

AFP

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?

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

FBI Says Researcher Admitted Hacking Airplane in Mid-Flight

By Eduard Kovacs on May 18, 2015

Netsecuris
Who's watching your network?

Aircraft controls are getting more sophisticated

Netsecuris
Who's watching your network?

Internet Exposed Aircraft Control Systems

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Internet Connectivity Could Expose Aircraft Systems to Cyberattacks: GAO

By Eduard Kovacs on April 15, 2015

Netsecuris
Who's watching your network?

Are we 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 | Expat | Honduras

HOME » NEWS » WORLD NEWS

Schoolboy hacks into city's tram system

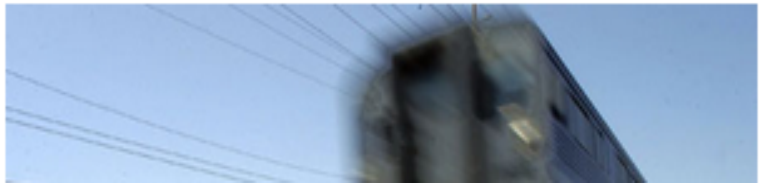
Netsecuris
Who's watching your network?

Is Rail Immune?

HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS

Share 5

Tweet this



By Aliya Sternstein

January 23, 2012

1 Comment

Netsecuris
Who's watching your network?

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?

What about that car you drive?

Cyber-Safe

Chryslers can be hacked over the Internet

Netsecuris
Who's watching your network?

Is government worried?

INTERNATIONAL BUSINESS TIMES | Automotive IT New

News | World | Business | Politics | Technology | Science | Sport | Entertainment

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?

Just Another Cyber Attack on Cars

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?

Really? Another automobile attack!

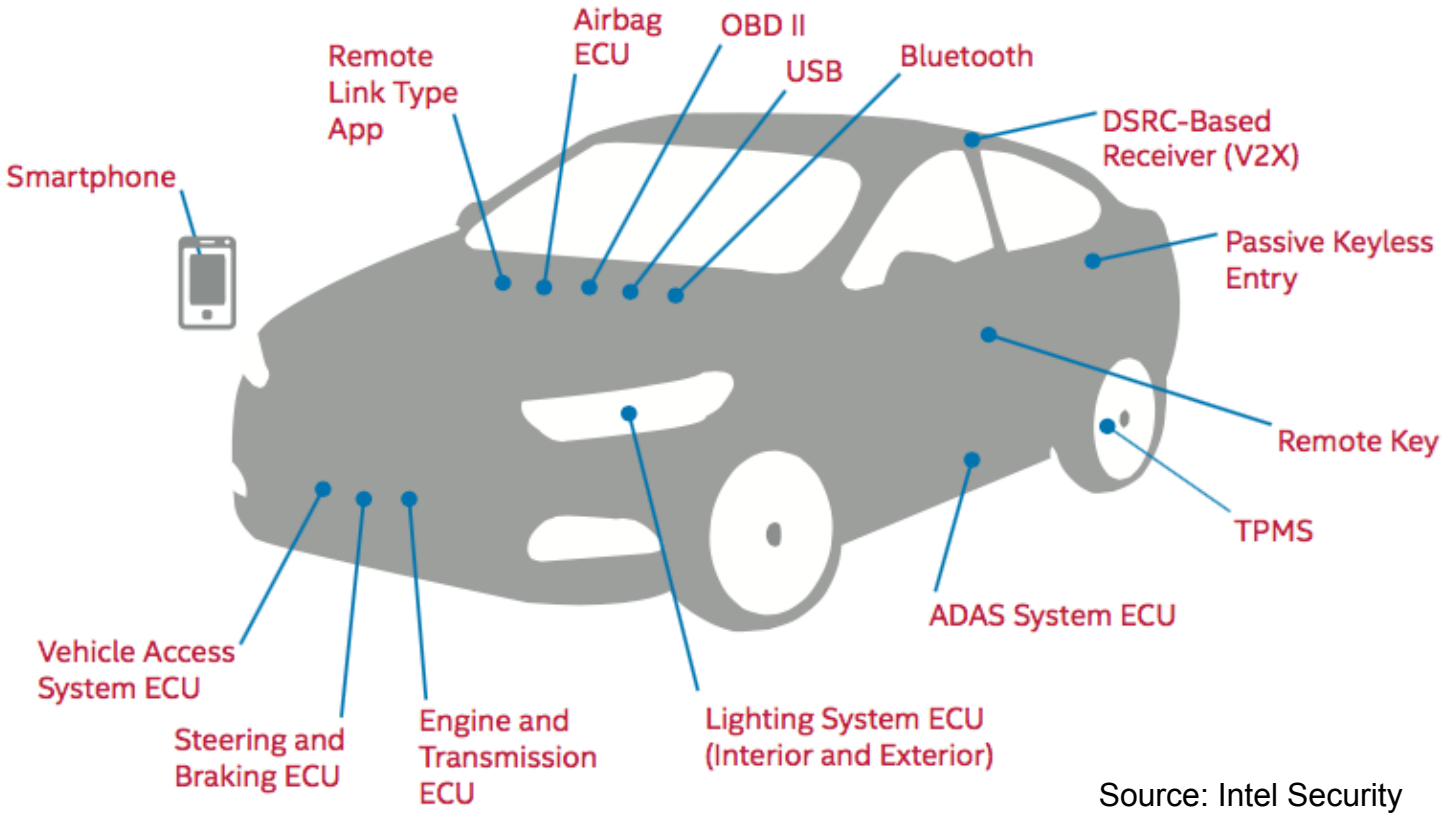
SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

BMW Patches Security Flaw That Let Hackers Open Doors

By Brian Prince on February 02, 2015

Netsecuris
Who's watching your network?

Cyber Attack an Automobile



Source: Intel Security

Automation

- Port of Hamburg
  - Highly automated
  - https://youtu.be/WxXZQ7emHC0
  - Great economic harm

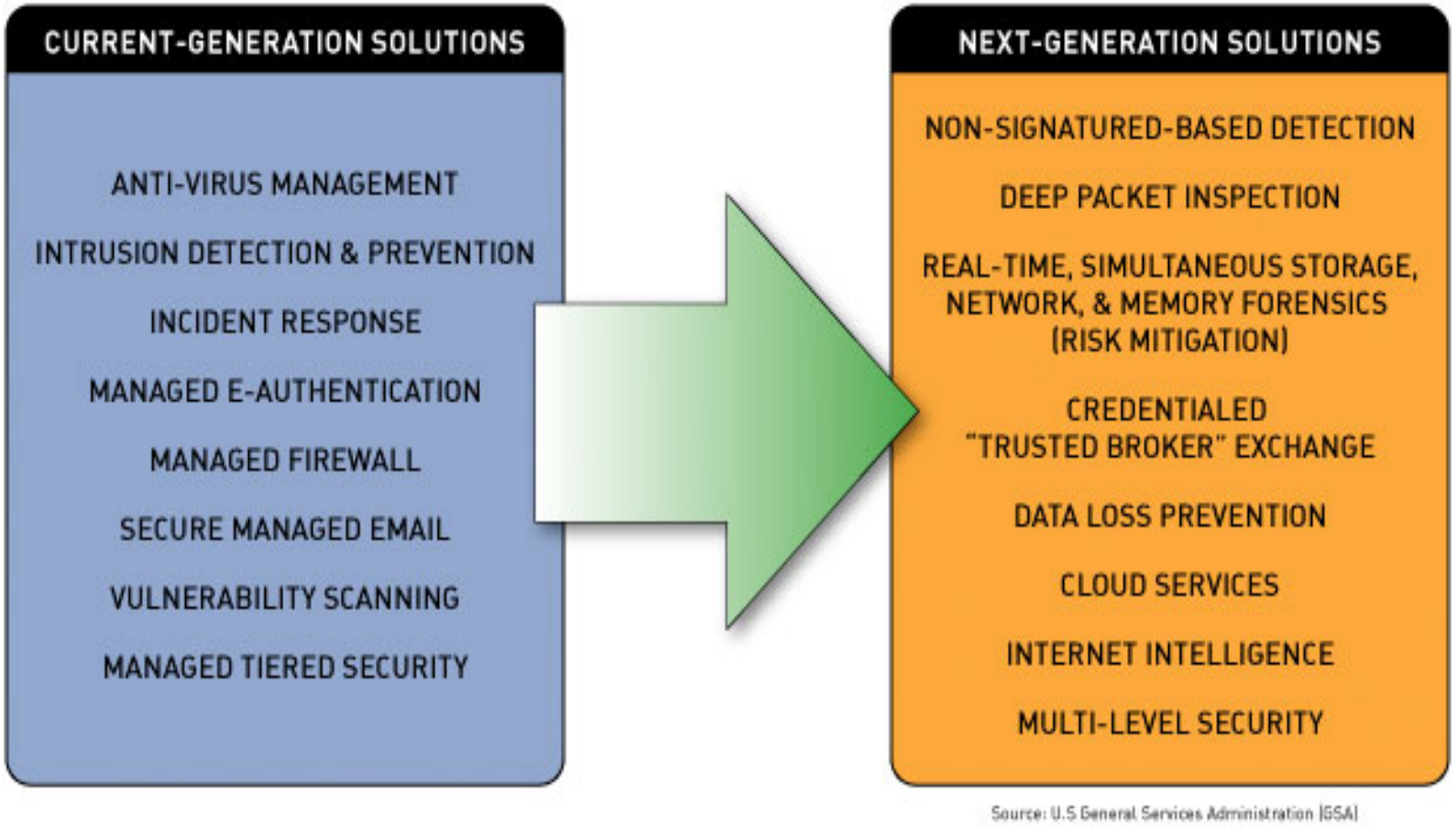
Netsecuris
Who's watching your network?

Internet of Things

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

Netsecuris
Who's watching your network?

Cybersecurity Solutions



Source: U.S General Services Administration (GSA)

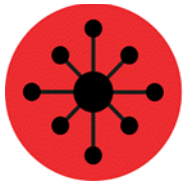
Non-signature based Detection/Prevention

- Not traditional Anomaly Detection/Prevention
- Behavioral Baselining
  - Determining what is normal
  - Looking for the unusual
  - There are some systems that can kind of do this today
  - Going to require more data

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

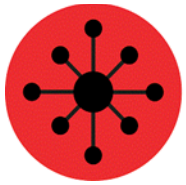


Network Security Monitoring

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

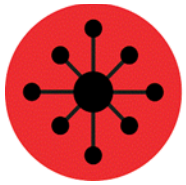
Network Security Monitoring

- Tools
  - Suricata (Capable of processing ICS Protocols)
  - Bro
  - Wireshark (Tshark)
  - TCPDump
  - Netflow and the like
  - 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.

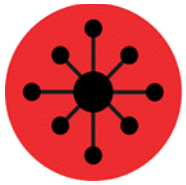


Network Cloaking

- Implements "Zero Trust" Model
  - Device A trusts Device B but not Device C
  - Device B can be allowed to trust Device C
- Secure the communications
  - High level of encryption
  - Cloak the IP Address of end devices
- All orchestrated efficiently and quickly

Cybersecurity Intelligence

- Those with the data are 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
  - Mellanox Technology (EZ Chip) (Tilera) and Suricata
  - Intel's acquisition of McAfee
  - Adapteva Epiphany
- 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

Office: +1 (952) 641-1421 ext. 20