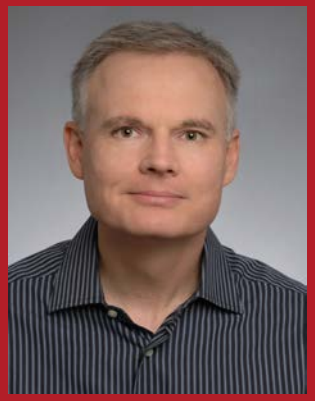
Hacking in the Automotive Industry



Michael R. Overly, ***Esq., CISSP, CISA, COP, ISSMP, CIPP, CRISC***

Foley & Lardner LLP

Los Angeles, California

213.972.4533

moverly@foley.com

#NADA2016

The views and opinions presented in this educational program and any accompanying handout material are those of the speakers, and do not necessarily represent the views or opinions of NADA. The speakers are not NADA representatives, and their presence on the program is not a NADA endorsement or sponsorship of the speaker or the speaker's company, product, or services.

Nothing that is presented during this educational program is intended as legal advice, and this program may not address all federal, state, or local regulatory or other legal issues raised by the subject matter it addresses. The purpose of the program is to help dealers improve the effectiveness of their business practices. The information presented is also not intended to urge or suggest that dealers adopt any specific practices or policies for their dealerships, nor is it intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

Agenda

- State of the world
- Why Now?
- Security Rules of the Road
- Questions

State of the World

Rising Information Security Risks: Data Breaches

- In total, Almost 1 Billion Records compromised in 2014 worldwide – up 81% from 2013.
  - 2013 – approximately 552 Million
  - 2012 – approximately 93 Million
- July 2014: JP Morgan Chase, 76M accounts
- March 2014: Ebay, 145M accounts
- December 2013: Target, 70M accounts
- September 2013: Adobe, 152M accounts
- Neiman Marcus, Home Depot, Jimmy John's restaurants, Dairy Queen, K-Mart.

Rising Information Security Risks: Denial of Services

- February 2014: Cloudflare, the largest DDOS attack in history, lasting over 10 hours and peaking at 400 Gbps, slowing the Internet in parts of Europe
- The average DDOS costs $100,000 every hour

Rising Information Security Risks: Intellectual Property

- May 2014, US Charged 5 Chinese Military hackers with 31 counts of Cyber-espionage against US corporations:
  - Westinghouse, SolarWorld, U.S. Steel, Allegheny Technologies, Alcoa to name a few.
- Some estimates - $200-250B annually in US, up to $538B/year globally.
  - Estimated to cost 200,000 jobs in the US alone.
- Companies likely to underestimate the loss, underestimate the risks.
- Most intellectual property breaches are not publicized.

Rising Information Security Risks: Significant Costs

- Total cost to global economy: $400B (approximately 15-20% of the revenue due to the Internet lost).
- Average cost of a breach in the US: $5.85M
- Cost for each record compromised: $201

Shodan

Like living on the edge? Try out the beta website for Shodan.

Shodan | Exploits | Scanhub | Maps | Blog | Membership | Register | Login

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR | FREE SIGN UP

Popular Search Queries: cisco-ios last-modified - Finds Cisco-IOS results that do not require any authentication ;-)

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

Shodan pinpoints shoddy industrial controls. — The Register

It greatly lowers the technical bar needed to canvas the Internet... — threatpost

'Shodan for Penetration Testers' presented at DEF CON 18 — Defcon 18

It's a reminder to many to know what's on your network... — darkREADING

Shodan is the Google for hackers. — ZDNet

Shodan vereinfacht die Suche nach SCADA-Systeme erheblich... — heise online

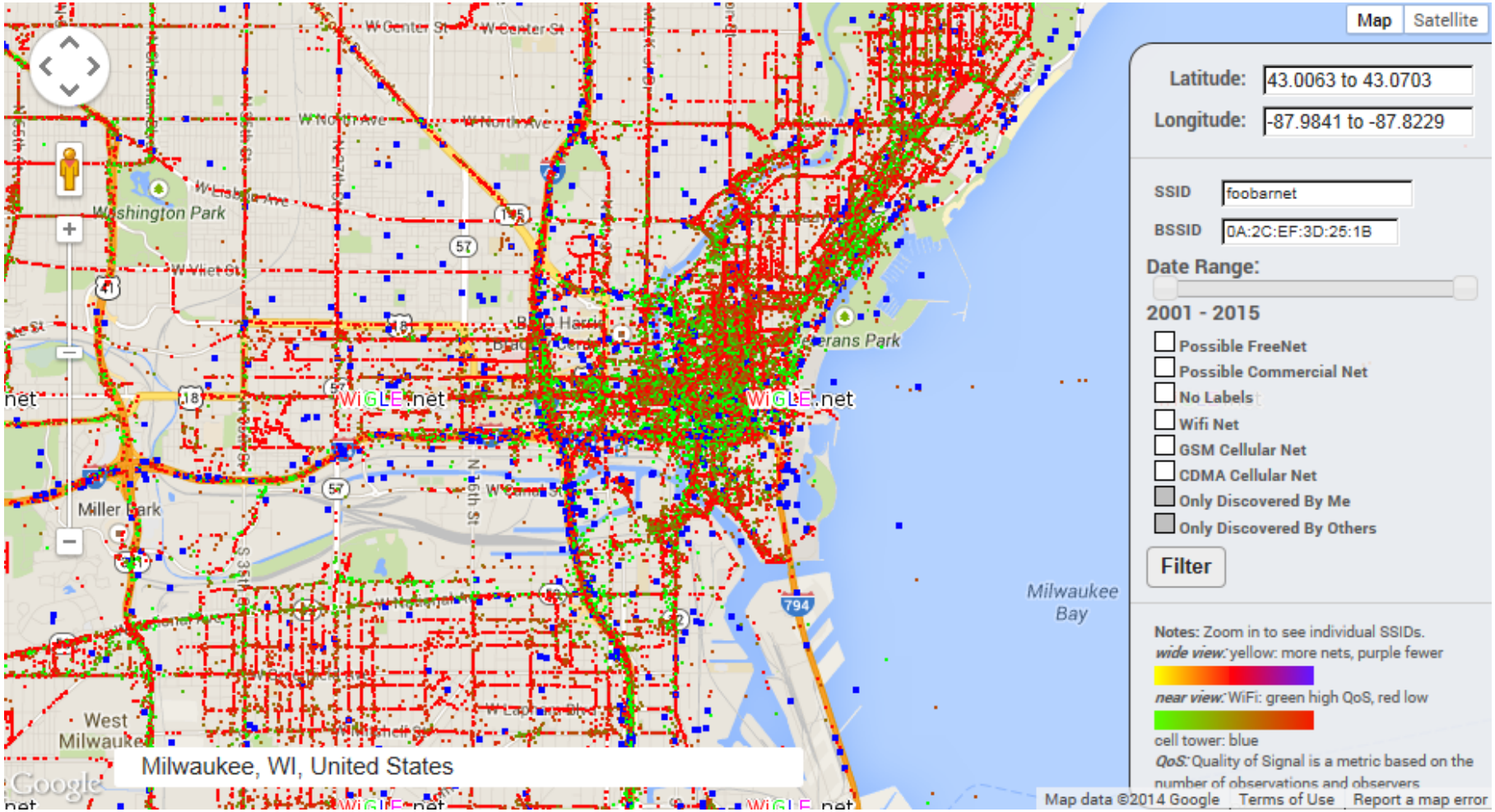
Firmen öffnen Stuxnet und Co. selbst die Tür. — CIO

Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan. — Aargauer Zeitung

Privacy Policy | Terms of Service © SHODAN

http://www.shodanhq.com/

Wireless Networks



http://wigle.net

Why Now?

Big Data/Telematics

Connectivity/Internet of Things/Connected nature of cars

Automotive and related System Complexity

Interconnectivity With Car Makers, Dealerships, Vendors, Business Partners, and Other Third Parties

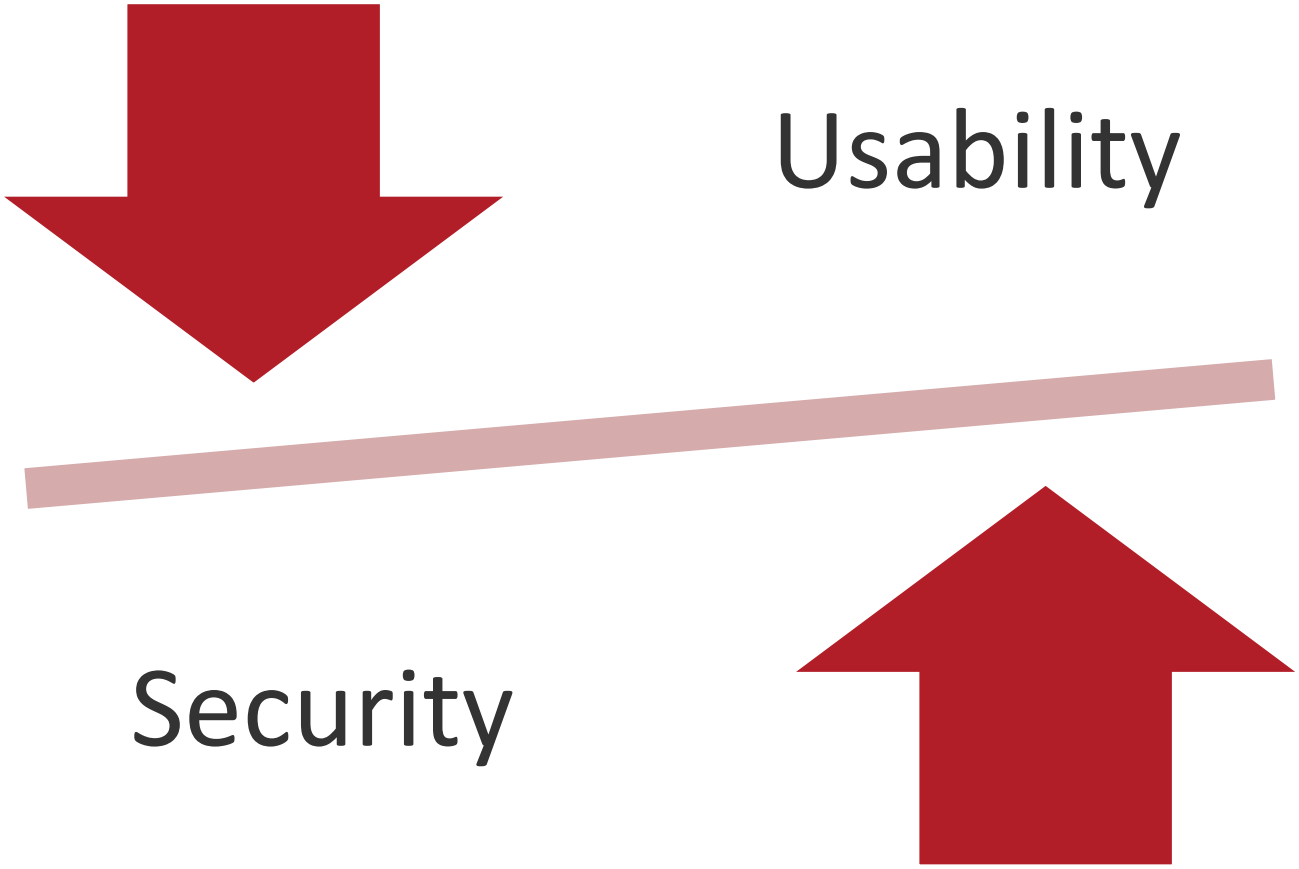
Common Security Myths

- Myth #1: “It’s all about the data”
  - It’s also about security of systems
  - It’s also about security of data
- Myth #2: “It’s all about confidentiality”
  - It’s about CIA: Confidentiality, Integrity, and Availability

Common Security Myths

- Myth #3: "To be a hacker, you must be a technology genius"
- Myth #4: "It's an IT Department issue"
- Myth #5: "I can achieve (need) 100% security"
  - Impossible to budget or use

Impossible to Use



The Biggest Myth of All

- Myth #6: "I'm safe. I have great security."
  - Thousands of new viruses and exploits developed every **day**.
  - Imperva/Technion-Israel Institute of Technology Study: initial threat detection (zero day) only 5%.
  - Verizon Study: 62% of intrusions took at least two months to detect.
  - Trustwave Holding Study: Average time to detect intrusion is 210 days.

Sources of Risk

Sources Of Risk

- Malicious “insiders”
- Script kiddies
- Hackers
- Spies (industrial, governmental, etc.)
- Organized crime
- Cyber Terrorists
- Hactivists

Sources Of Risk

- Your laptop manufacturer
- Disk drive manufacturer
- Google/Microsoft/Apple/Yahoo/Amazon
- Smartphone Apps

Social Engineering

- No technical skill required
- Phishing/Spear Phishing
  - In 2013, nearly 450,000 phishing attacks and estimated losses of over $5.9 billion
  - Leverage social media and corporate bio information to create targeted attacks
  - Large enterprises have a 1 in 2.3 chance of being targeted
  - Executives/management are common targets

Security Rules of the Road

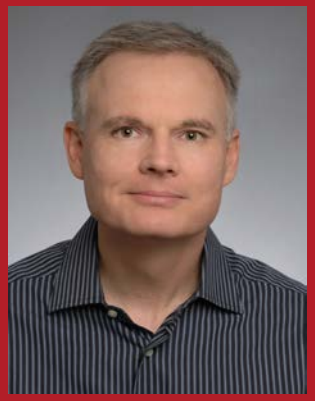
- Auto ISAC (Information Sharing and Analysis Center)
- Inform yourself regarding information security, including security plans and policies.
- Require formation of information security committee to oversee day-to-day security compliance efforts.

Security Rules of the Road

- Require the committee to issue regular reports threats and mitigation strategies.
- Prioritize security efforts and exercise prudence in allocating resources.
- Ensure security is addressed with critical suppliers and vendors.

Questions ?

Hacking in the Automotive Industry



Michael R. Overly, ***Esq., CISSP, CISA, COP, ISSMP, CIPP, CRISC***

Foley & Lardner LLP

Los Angeles, California

213.972.4533

moverly@foley.com

Please visit the **NADA Pavilion** in the Expo Hall for information on accessing electronic versions of this presentation and the accompanying handout materials, and to order the workshop video recording.

#NADA2016