CompTIA

Academy Educator & Learning Partner Conference

July 31 - August 2, 2015 | Hilton Chicago

Lunch with Guest Speaker: John Dvorak, CTO Information Innovators Inc.

Information Innovators Inc.

Insight • Integration • Impact

CompTIA Hacking Cars and Spearphishing

July 31, 2015

John Dvorak

Overview

1. Very brief introduction
2. Car Hacking; or Why You No Longer Need the Mob
3. OPM Data Breach: the Ultimate Spear Phishing Database
4. Interesting Topics at Black Hat
5. Your Summer Reading List

Very brief introduction

Company Profile

- Providing services since 1994 (2001 as Triple-i)
- ~1000 employees nationwide
- **Government Customers**

Centers for Medicare and Medicaid
Defense Contract Management Agency
Defense Health Agency
Defense Logistics Agency
Federal Aviation Administration
Food and Drug Administration
Intelligence Community Agencies
Patent and Trademark Office
Air Force
Army
Department of Energy
Department of Health & Human Services
Department of Homeland Security
Department of Housing and Urban Dev
Department of the Interior
Department of Justice
Department of Transportation
Department of the Treasury
Department of Veterans Affairs

- **Certifications and Awards**

We are CMMI Level 3 assessed for Software and Systems Engineering and maintain corporate ISO 9001:2008, 20000-1:2011, and 27001:2013 certifications. We are also a Third-Party Assessment Organization (3PAO), providing awareness, readiness, and assessment services to cloud service providers working toward FedRAMP compliance.

Triple-i has received numerous awards and certifications demonstrating our ability to deliver. In 2014, we received the Army Fort Sam Network Enterprise Center (NEC) of the year award, FDA's Group Recognition Award, and DHS's HQ Information Systems Security Officer of the year award and the DHS's HQ Compliance Professional of the year award.

- **Facilities Clearance**

Triple-i has a Top Secret facilities clearance.

Capabilities to Address Client Needs

- **Solutions oriented** by working closely with each client – drawing on our portfolio of integrated service offerings to ensure that each client derives the greatest value from their investment in our services
- **Vendor agnostic** approach leverages an array of tools, technologies, and partner relationships to meet your organization's mission.

- Adobe Authorized Reseller
- Atlassian Enterprise Expert
- Amazon Web Services Partner
- Citrix Silver Partner
- Google Enterprise Professional Partner
- Help Desk Institute Corporate Training Partner
- Hortonworks Partner
- Microsoft Silver Midmarket Solution Provider
- Oracle Gold Partner
- Rackspace Platinum Strategic Partner

eITSM (IT Service Management)

- Data Center Services
- Network Operations
- End-User Services
- Services Consolidation
- ITIL and Continuous Improvement
- Performance Management
- Business Transformation
- Communications

Cloud/Data Solutions

- Tier 3 Data Center Operations
- COOP Site Operations
- Private Cloud Design and Build
- Enterprise Architecture
- Public/Hybrid Cloud Hosting/Managed Services
- Cloud Brokering

Cybersecurity Services

- 3PAO/FedRAMP Services
- Security Design & Configuration
- Assessment & Accreditation
- Identity and Access Management
- Cryptography
- Physical Security
- Security Training and Awareness
- Software Development Security
- Telecom and Network Security

Health IT Solutions

- eScreening
- VistA Data Analytics
- Tele-health Solutions
- "Big Data" Solutions
- Mobility Solutions

Health Services

- Clinical Care Design & Informatics
- Outreach and Communications Programs
- Scientific Support for R&D
- Education Program Design
- Program Management Expertise

Agile Development

- Software Engineering
- Mobile and Telework Solutions
- Content Management Systems
- Enterprise Search
- SharePoint Development

Intelligence and Geospatial

- Predictive Analytics/Modeling
- MIMOSA anomaly detection software

Program and Quality Management

Car Hacking; or Why You No Longer Need the Mob

Oh, the Internet of Things

A short side discussion of IoT to start us off…

Challenges of IoT with respect to security:

1)Low Powered, limited overhead
2)Data collection standards, or lack thereof
3)Blackbox coms and convenience-based interconnections
4)Velocity of releases – billions of potential devices

Major in my mind:

5) Companies with limited/virtually no IT and IT Security staff are releasing products, often with limited supporting standards or expectations

Car Hack – The general concept

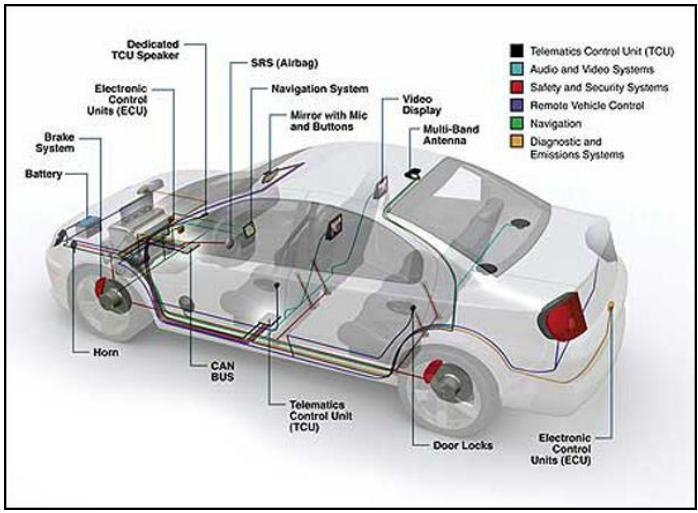
Charlie Miller and Chris Valasek hack a Jeep

Vector: Hack exploited a vulnerability in Uconnect (to be revealed at Black Hat next week) to hack the entertainment system, granting access to the car's CAN bus and, from there, the car's components.

We were discussing attack vectors for cars 5 years ago: http://www.autosec.org/publications.html

CAN bus/LIN and connected components not typically (ever?) designed with remote exploitation in mind

Once in, then what?



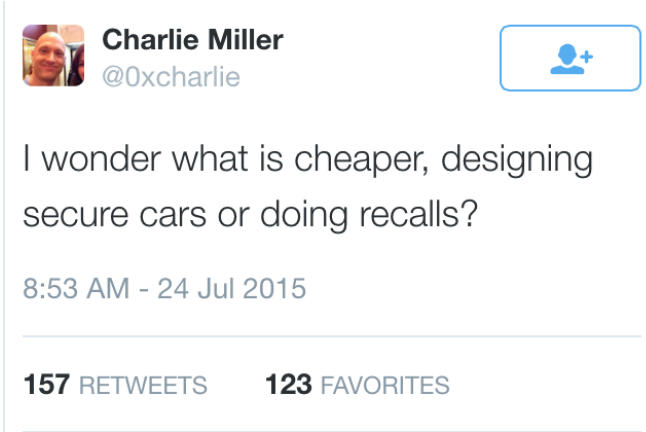
Source: www.motor.com

Car Hack – The implications

Are we building mitigation into our plans for connected things?

Chrysler case:

- ***No* remote update solution**
- **Three offers to fix:**
  - **Build your own patch (ha!)**
  - **Take it to a dealer (maybe?)**
  - **THEY WILL MAIL YOU A USB STICK (!)**



Okay, so they did have Sprint block the offending port…

What might one do with such a powerful capability?

1)Sure, a criminal could monitor someone's driving habits

- **Pattern of life analysis**

2)But, causing a crash is so much more interesting

- **What would forensic analysis reveal after a crash?**
- **Potential ability to obfuscate the cause**
- **Take out a former business partner?**

Beyond cars

Should we assume their security engineering is better?

Velocity of new products may not be as much of a threat as the velocity of change within the companies providing these new products

Industries that have not needed to think about cyber security when developing products must now learn how to do it right.

In our desire to connect it all up, will we lose sight of good security practice?

As security educators, what role do we play in getting ahead of this problem?

OPM Data Breach: the Ultimate Spear Phishing Database

What does the OPM Database Represent?

As a data asset, what does the OPM Database Represent?

Initial press immediately focused on identity theft. But what does it really represent to a foreign intelligence agency?

1)A massive social network map over nearly 10% of the US population, and almost everyone of high interest
2)An incredibly rich, highly trustworthy data set – want to verify intel you have on someone?
3)Monster recruiting tool
4)The word's greatest social engineering reference set – spear phishing was never so good

Monetizing this dataset through credit card fraud is the possibly the least likely use.

In the realm of exploitable data in the human intelligence game, it doesn't get much better than this.

Social Engineering – the persistent threat

Real social engineering spear phishing test
(Testing NIST 800-53: AT-02 Security Awareness Training)

Target: system administrators and IT security staff with 5-20 years experience

General method:
1) **Obtain new domain similar to corporate domain**
2) **Copy website**
3) **Send email from external mail server, spoofing a known internal identity**
4) **Email includes link to website and requests users fill out a form, to include PII**

Tested two questions:
1) **Would user confirm that the link was valid before clicking it?**
2) **Would the user enter identifying information in the fake web page?**

Result:

10% of administrators opened the email and took no further action (good!)
40% opened the email and clicked the link, then cancelled
50% opened the email, clicked the link, and submitted information through the fake portal

23% open phishing messages

11% click on the attachments

Source: Verizon 2015 DBIR

95%

of phishing incidents attributed to state sponsors

2/3 of cyber espionage cases involve phishing

Source: Verizon 2013 DBIR

Now imagine what the enemy can do with a rich data source

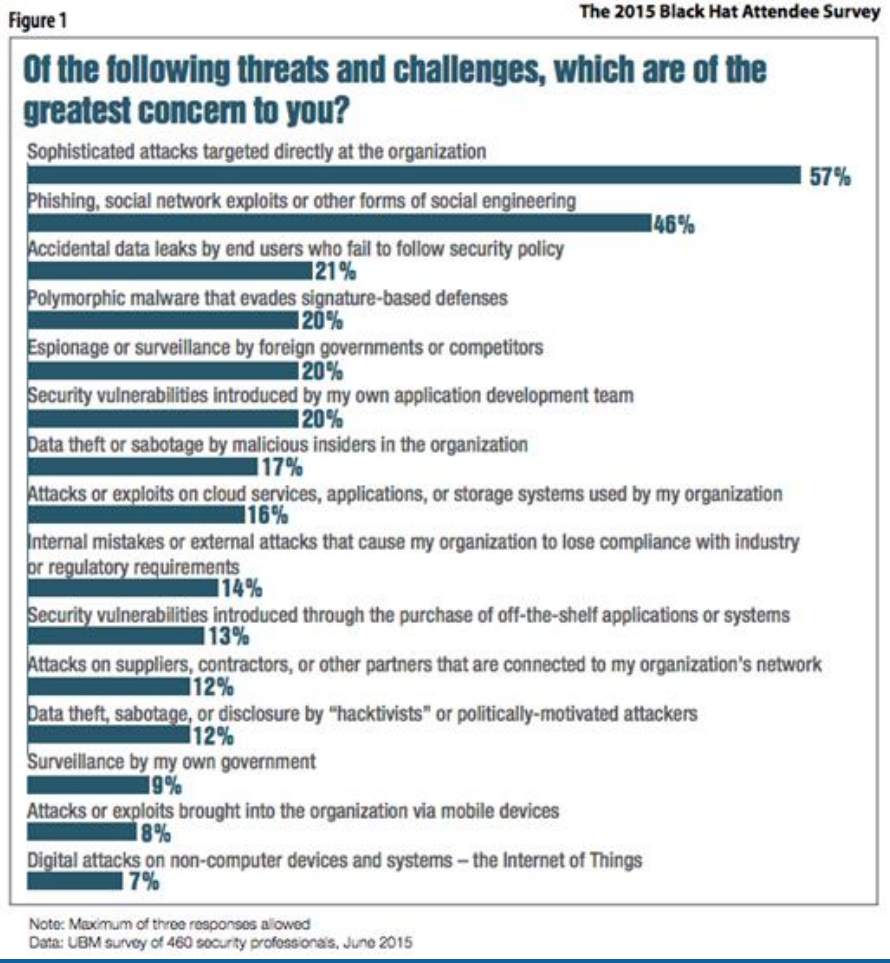
But I'm not the target!

Users have an historic attitude issue:

I'm not a target. What do they want with me?

A revelation in the 2015 DBIR that the security community has suspected for a long time: "**nearly 70% of the attacks where we know the motive for the attack, there's a secondary victim**" (DBIR 2015, 5)

As security educators, how can we craft better training programs to reduce the risk of Social Engineering?



Black Hat
And Your Summer Reading List

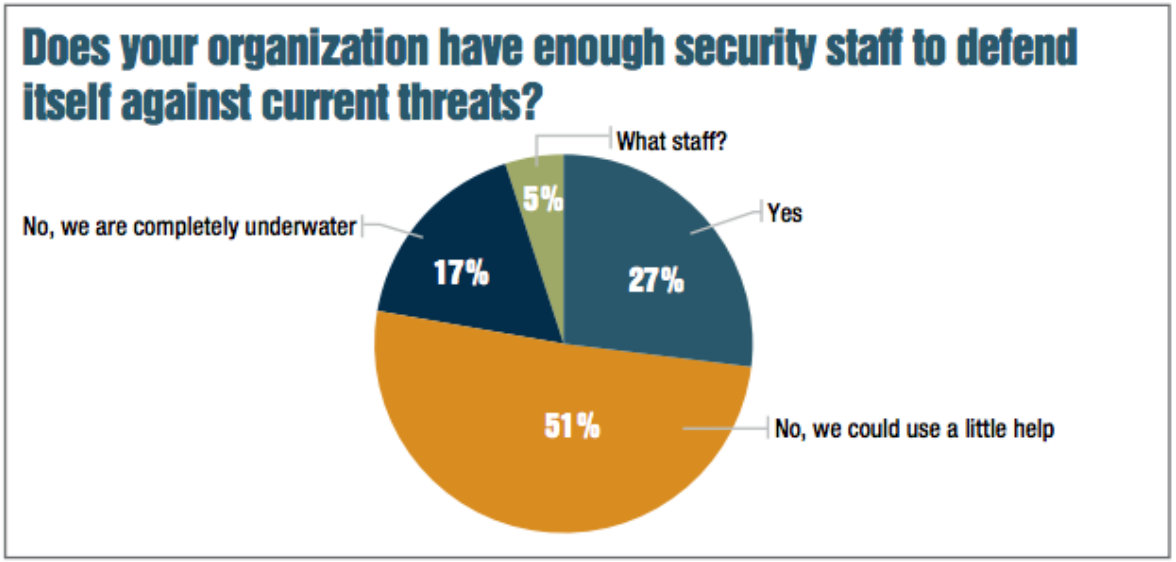
Black Hat starts tomorrow…

Some other exciting topics for next week's Black Hat:

1)Stagefright: Yet another zero-day Android exploit, but not easy for user to patch
2)How to defeat machine learning defenses
3)Review and exploit neglected attack surfaces in IOS 8
4)Hacking Chemical Plant for Competition and Extortion – one of several SCADA hacking presentations
5)Spread spectrum SATCOM hacking: attacking Globalstar Simplex Data Service

Figure 6

The 2015 Black Hat Attendee Survey



Data: UBM survey of 460 security professionals, June 2015

Threat Landscape – Recommended Reading

Your recommended summer reading to understand the current threat landscape:

Verizon's 2015 Data Breach Investigations Report (DBIR): http://www.verizonenterprise.com/DBIR/2015/
- historically not only one of the most comprehensive, but certainly the most entertaining

Cisco's 2015 Annual Security Report: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html?keycode=000657685 or http://cs.co/9001x5ZP

Radware's "2014-2015 Global Application and Network Security Report" (minor registration required): http://www.radware.com/ert-report-2014/

FireEye's Threat Intelligence Reports: https://www.fireeye.com/current-threats/threat-intelligence-reports.html

And, of course, the briefs from Black Hat – good, bad, and ugly

QUESTIONS?

Contact Information:
John N. Dvorak
Chief Technology Officer
jdvorak@iiinfo.com
@jndvorak