Digital forensics in the age of the Internet of things: Challenges and opportunities

Dr. Samuel Liles
Associate Professor
Purdue University College of Technology

What do I do?

• **Military and Law Enforcement**: Army(NG), Marine Corps, Police Department, Sheriffs Department
• **Industry**: Networking, telecommunications, defense, corporate incident response
• **Higher Education**: Purdue Calumet, National Defense University (iCollege), Purdue University
• PhD dissertation title: “Cyber warfare as a form of conflict: Evaluation of models of cyber conflict as a prototype to conceptual analysis” May 2012
• **DHS and NSA STEM Fellowship**
• **Blog**: [http://selil.com](http://selil.com)
• **Twitter**: @selil
What are we going to talk about?

• The term “Internet of things” has different meaning to each of the constituent communities building services and devices. One community though is having to rapidly evolve and that is the digital forensics and incident response community. Whether it is the acquisition, analysis, reporting, or validating of results each of the steps in the forensic process is customized at almost a device level.

• Through rapid advancement and practical application of the principles of digital forensics, a series of processes are discussed that give an indication of the future of this problem set to the digital forensics scientific community. As a work in progress, positive and negative results are discussed to give a grounding in the solutions and challenges of this research.

• Tools, techniques, and procedures are provided as an overview utilizing an interesting case study and the challenges of that case study are discussed. Participants should learn about using current tools, new tools, and a few different strategies if they are challenged with a similar case in the future.

What is forensics?

• Relating to or denoting the application of scientific methods and techniques to the legal process.

• The application of science to the finding of fact for use in a court of law or by the state to compel.

*My students and I do forensic analysis of stuff classified as the Internet of Things*
Technology

• **Technology**, the study of the art and craft of doing work with tools
• **Technologist**, a person who enhances the quality, efficiency, or capability of work through tools

**Mission!** *Study the art and craft of doing forensic analysis on the Internet of Things with better quality, efficiency, and enhance the capability of the forensic community*

What is the Internet of Things (IoT)

• The next big thing?
• Baloney?
• What was all that TCP/IP connected stuff called before IoT?
• What about the peeping Tom in your thermostat?

Dear Abby, my thermostat is asking a Chinese ZeusBot for relationship advice with my refrigerator. Should I intervene?
How did we get to Internet of Things?

- Conversation with Jim Christie (formerly FBI, formerly DC3) ... Say what would you do if you got a device that wasn't traditional forensics.
- IOT is more than SCADA/ICS/DCS/BCS/SCS etc..
- Suunto T6D sports watch uses a protocol ANT+, connects to the Internet.
- SATCOM uses other than Internet (OTI) but is a gateway (SPOT, to HF multimode)
- There is lots of "stuff" going on in the Industrial Scientific Medical (ISM) bands besides WiFi
- Add in near field communications (NFC) and RFID (EZ Pass)
Internet of Things

- RFID
- Sensors
- Actuators
- Devices
- Mobile phones
- Tablets
- Medical devices
- GPS devices
- Auto entertainment systems
- Auto driving assist or control systems
- Industrial Control Systems
- Autopilot collision avoidance systems
- Need not be a physical instantiation

Analyzing all the things

In the lab we have done preliminary analysis on Roku, Surface, Kenwood Stereo, NEST Thermostat, Pebble Watch, iPad, Google Glass, Garmin Nuvi, TomTom, Nintendo Wii, Nikon Coolpix, iPod Touch, Kindle 2 (plus all the rest) Symbian, DVR, Samsung Galaxy Watch.

http://selil.com/archives/tag/581cfm
Controlling the edge

• Generally open architectures and connection types
• Sensors and actuators represent the real world connectivity via the digital domain
• Localized behaviors are globally connected
• Protocols are often “esoteric”

Stages of the process

• NIST stages of the process, “collect, examination, analysis, reporting”
• Our stages, “acquire, analyze, validate, report”
• What is the evidence on the device?
  – Time, date, location, direction, pictures, audio, video
  – Logs, meta-data, registry or app data
• What is the “use” of certain evidence
• Focus on validity, reliability, and generalizability of the results.
Acquire phase

• What are the IO functions of the device
  – Ethernet, USB2/3, LEDs, video, audio, g-force, keyboard, mouse, screen, wifi, Bluetooth, more
• What is the storage mechanisms of the device
  – Persistent, volatile, etc. SSD, HD, RAM, etc.
• What is the processing mechanisms of the device
  – Processor, video card, SSP, co-processor
• What are the non-traditional sensors of the device
  – G-force, GPS, FM, CD player, Bluetooth, Compass, etc.
• What is the device architecture like
• Are there barriers like media transfer protocol (MTP)?

Analysis Phase

• Highly dependent on whether physical image is possible Tools: Cellebrite UFED, MPE+, FTK
• Primarily looking for system artifacts, user interaction, I/O and evidence of probative value (dependent on context)
Validate Phase

- Getting raw data off a device does not prove the provenance of the data
- Seeding a device with known data sets allows for validity and reliability of acquisition phase to be tested
- Seeding can include introduction of errant or erroneous data
- Validity and error rates are challenged by some in the digital forensic community
- Challenges can be addressed through empiricism

Reporting Phase

- What did you think you knew
- What were your assumptions
- Report the results in that context with issues and problems alliterated every time.
- **EVERY** lab and report has an abstract, steps of the process, issues and problems, and conclusions sections.
- Errors and omissions are failures and, problems and analysis are not even if acquisition or analysis fails
Applying context to the problem

- Why do we care?
- Why is this research?
- Why should we continue doing this?
- Who are the stakeholders?

Tell me about ICS/DCS/BCS

- “You guys over in IT really don’t get industrial control systems.”
- MODBUS, DNP3, other ICS protocols are found in Wireshark, Metasploit and other “hacker” tools.
- Nessus and NMAP have detection rules
- “We found your SCADA system on the Internet” – xoxo Shodan

Slides located at http://selil.com
Is there a deeper reality?

• You need motive, means AND opportunity to do something bad.
• Just because it is possible does not mean it is probable.
• **Can** does not mean **will** happen.
• At the individual, personal, family level...
  – Risk is money, privacy, and safety not incidents of national significance

Money...

• Not all Internet connected devices are for your benefit.
• Currently ATM card skimmers are a great way to steal both the card data and PIN you utilize
• Watch for the sideways attack....

Money...

- Everybody likes money
- Credit card related breaches are in the news
- Credit cards work exactly as they were designed
- As they get smarter they join the IoT category
- The issue is not with the credit card so much as it is with the system of using credit cards
- Any significantly complex system can be used exactly as designed for nefarious purposes
Former Purdue students sentenced for hacking, changing grades

The student hackers who changed their grades were sentenced this week after pleading guilty to several felonies.

From 2008-2010, three students were involved in an incident in which they hacked into Purdue’s computer system. The students reportedly stole and inserted key logging devices in professors’ keyboards, allowing them access to passwords, which were later used to enter the system.
Privacy...

December 21, 2011 “Chinese hack into US Chamber of Commerce, “.... At one point the penetration of the Chamber of Commerce was so complete that a Chamber thermostat was communicating with a computer in China.” ABC News

Safety...

• Your cell phone is a walking bundle of sensors.
• It contains radios (Cellular, Wifi, Bluetooth, Near Field Communication, GPS, FM)
• It contains sensors for light, microphone, camera, magnetism, heat, touch, shock, gyroscope.
• It knows when you are awake, eating, walking, running, sleeping, being lazy, and your most intimate secrets.
• And, you take it into your car
It’s all just stuff

Since 2004 have been looking at automobile forensics and focusing on black box and accident data recorders. Interest started in the late 1980s and mid 1990s as chipping and hotrod cars became a significant interest. We went from EFI and supercharger is bad, to EFI and supercharge is good. In the mid 1990s I chased navionics around SeaTalk and other various NEMA protocols on yachts and ships.

---

Background on where we thought we were going

- **March 29, 2007:** NHTSA opens a preliminary investigation into pedal entrapment on MY’07 Lexus ES350 models based on five consumer complaints
- **January 21, 2010:** Toyota recalls 2.3 million vehicles for the sticky pedal defect.
- **2010-2011** NHTSA outsourced source code analysis to NASA  
- NHTSA Exec Summary  
- NHTSA Report Here  
- NASA Exec Summary  
- NASA Report Here  
Famous words in politics... “Uh oh...”

- In 2011 "NASA found no evidence that a malfunction in electronics caused large unintended accelerations," said Michael Kirsch, Principal Engineer at the NASA Engineering and Safety Center (NESC).
  — This is not wrong it is just primarily short sighted
- Chris Valasek @nudiehadbeardasher and Charlie Miller @0xcharlie hack a Toyota and Ford and on Page 40 of their 2014 report talking about the Toyota "Acceleration of the automobile via the Internal Combustion Engine (ICE) could be directly linked to a single CAN ID which has the following signature: "

So my students and I rented a car...

- The car was a newish Ford Flex with infotainment system
- We forensically processed the car for evidence
- We looked at both digital and physical evidence
- What we found was interesting
- It was a learning experience...
Open research questions
Amateurs argue about crime and punishment. Experts argue about authorities and budgets.

- Balance the authorities of ADA, HIPPA, CFAA, C&A, network security. How are you going to handle all of the autonomous medical devices that are going to be required by human resources to be hooked up to your production Internet network? SCIF’s? Who is going to be educated in their investigation?
- Defense in depth is dead. It is completely possible that the edge of the network is now the frontline. Your mobile devices represent a new paradigm as they are connected to automobiles, headsets, home networks, etc. Threats vary from the Pineapple to the home system. Who is going to do incident response at this level?
- Forensics is almost never built into systems and often for the purpose of legal validity needs to be reverse engineered. This is a non-scalable problem driven by memetics and fads rather than societal goals. Process should be scientific and validated by the community.
- **Risky ideas:** Many of the "old" information assurance and security rules, doctrine, and sometimes called science is based on myths, half truths, and outdated technological concepts. Almost all of the multicians work was looking at mainframe computers or analogized from other knowledge domains. We need deep, rigorous, completely new approaches based on valid evidence based approaches. Clean paper approach to information security research is informed by the digital forensics and incident response disciplines.

Questions?