TOKYO, JAPAN

12th IDF Annual Conference

ST. PAUL, MN, USA

# IoT Forensics

## Issues, Strategies, and Challenges

*Jigang Liu*

Metropolitan State University
St. Paul, Minnesota
U.S.A.

`Jigang.Liu@metrostate.edu`

TOKYO, JAPAN

# Outline

ST. PAUL, MN, USA

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

# Introduction (1)

- Many questions to ask:
  - What is IoT?
  - What is Forensics?
  - What is IoT Forensics?
  - What is the difference between IoT Forensics and IoT Security?
  - What is the difference between IoT Forensics and Digital Forensics?
  - … …
  - ***What is the problem we try to deal with anyway?***

# Introduction (2)

- Case 1: The TRENDnet incident, 2013
  - TRENDnet, Inc. : a producer of wireless cameras (IP cameras), located in California, USA;
  - Cameras can be installed wherever you need for a video feed to your electronic devices, such as a computer or a smart phone;
  - In 2012, the company had approximately $62 million in total revenue and approximately 80 employees.

TRENDnet
TRENDnet TV-IP110W
SecurView™ Management Software Included
•Motion detection
•Email alerts
•Program recordings
•Manage 16 cameras
Wireless Internet Camera Server
▪Secure your home or office with wireless streaming video
▪Mount this compact stylish Internet camera on most surface areas
▪Advanced complimentary software supports up to 16 Internet cameras
▪Optimal wireless encryption for secure wireless transmissions
INTERNET CAMERAS
TV-IP110W

# Introduction (3)

- Overview of The TRENDnet incident

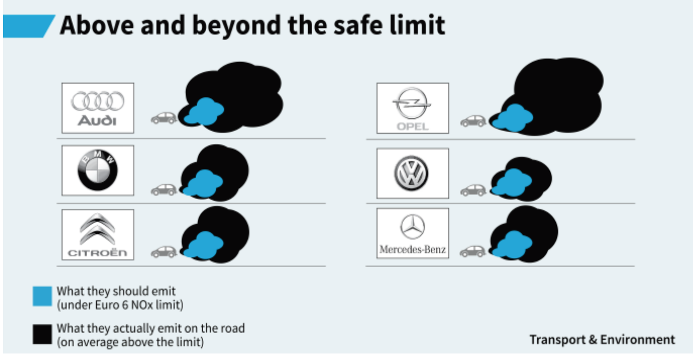
  *https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter*

  - in 2013, the Federal Trade Commission (FTC) filed a complaint against TRENDnet Inc. stated that TRENDnet failed to provide reasonable and appropriate security for the wireless cameras, which resulted in hacking attacks;
  - The hackers posted Internet links to compromised feeds for nearly 700 wireless cameras;
  - These compromised live feeds displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities;
  - The problem was that The DVSA (Direct Video Stream Authentication) setting, provided by the TRENDnet IP cameras, allows users to turn off the login credentials requirement for their cameras, so that they can make their live feeds public;
  - The final settlement: as a first-time offender, TRENDnet was not sanctioned with any financial penalties by the FTC, which otherwise could amount to $16,000 per violation, or more than 11 million dollars for 700 IP cameras.

# Introduction (4)

Case 2: The Volkswagen Scandal, 2015

- Sept. 18, 2015, the U.S. Environmental Protection Agency (EPA) issued a "Notice of Violation" to the Volkswagen accusing the automaker of cheating on emissions tests;
- The violation caused by the cheating software is related to the compliance with the Clean Air Act (CAA);
- This scandal affects 482,000 VW diesels vehicles sold in the U.S. and more than 11 million cars worldwide.



# Introduction (5)

- Overview of the VW scandal:
  - It began with a $50,000 grant obtained by the faculty at West Virginia University to evaluate a group of cars for their compliance with the CAA; (there was no former knowledge of any suspicion);
  - After all the cars passed their in-house testing, they were taken on the road-test between Los Angeles and San Francisco and it was observed that the results were significantly different from the results from their in-house testing;
  - The cheating software was written to detect when the vehicles were being emissions tested and then turned down pollution control devices when not undergoing tests;
  - As a result, these cars passed emissions tests, but emitted up to 40 times more nitrogen oxides (NOx) than allowed by law when driven on the road;
  - For those 482,000 VW vehicles sold in the U.S., the fine from the EPA could be multi-billion dollars;
  - The cheating software is protected by the law from being openly reviewed and tested by a third party in the U.S.;
  - What is the bottom line for us to investigate this sort of scandals as more and more IoTs built into our life? (smart home, smart car, smart city, smart everything, etc.)

# Introduction (6)

- **The reality**:
  - The problems to deal with are legal dispute, civil or criminal cases, cyber attacks, and data breach, etc.;
  - As reported "you might remain silent, but anything your computer says will be held against you" especially when everything is moving to the cloud and everything around us is going to be one of the Internet of Things;
  - What has changed in this cyberphysical environment?
    - no longer controlled by us
    - mixed with others;
    - shared with others;
    - might be located in a different country;
    - no longer static; it is dynamic; for instance, the critical signals from the sensors at the crime scene might have been recorded by the sensors on the car that passed by the scene when the crime took place.

# Introduction (7)

- Everyone is going to leave some digital traces behind them in this cyberphysical world no matter you like/notice it or not;
  - As we try to control everything electronically, we put ourselves under the control of this cyberphysical world inevitably;
- "Crime scene" has become "crime universe" in terms of the size of the Internet, heterogeneous nature of IoTs, and the volume of data involved
  - malicious incidents can occur in any places at anytime with or without any interaction with us;
- It is not necessary to take all the available evidence from an IoT cyberphysical environment to win the case;
  - There could have many different ways in collecting evidence from an IoT cyberphysical environment to determine whether a suspect was on the crime scene. For instance, cell phone records, CCTV tapes, parking meter records, or car navigation logs.
- Digital/IoT forensics is looking for the fact or evidence, not for reasons that cause the problems or for solutions that solve the problems

# Introduction (8)

Fundamental concepts about the U.S. legal system:

- "You have to prove me wrong"
  - Defendants hold an upper hand in defending their wrong doing. The burden of proof is often on the plaintiff side.
- "Procedure is somehow more important than the fact"
  - You have to prove that nothing has been changed after the seizure of the evidence (chain of the custody)
- "It must be a real person with a resolved identity"
  - For a child pornography image, you have to provide the identifications of the children who appear on the image
- "Federal laws are usually tougher than state laws with the respect to the cases involving digital evidence"
  - There is no central police office in the U.S. The federal cases are handled by FBI
- "For a criminal case, the decision by the jurors must be unanimous"
  - Anyone can influence an outcome of a criminal case by being a juror

# Outline

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

# Scope of the Problem

- IDC (International Data Corporation) forecasts that the IoT market will reach $3.04 trillion and there will be 30 billion connected things in 2020. (*5 per person on the Earth*).

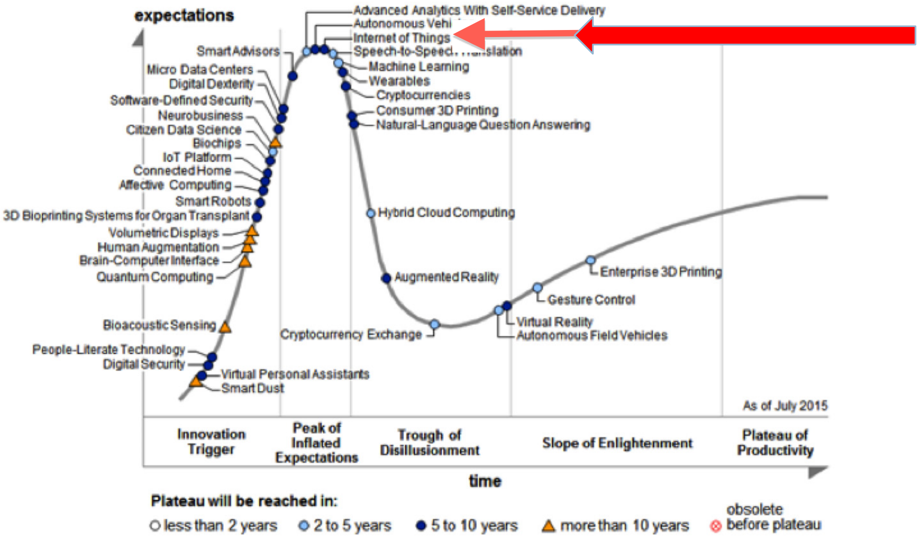


Figure: Hype Cycle for Emerging Technologies (Gartner, August 2015)

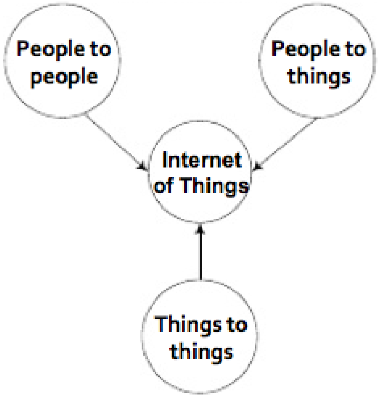
# Scope of the Problem

- Internet of Things (IoT)
  - The network of physical objects accessed through the Internet... These objects contain embedded technology to interact with internal states or the external environment.” (by CISCO)

    *http://www.cisco.com/web/solutions/trends/iot/overview.html*
  - Six Pillars of the Cisco IoT System
    1) Network connectivity
    2) Fog computing
    3) Data analytics
    4) Security - cyber and physical
    5) Management and automation
    6) Application platform

# Scope of the Problem

- Internet of Things (IoT)
  - It is an extension of traditional networks for the interconnection of every object/thing to every other object/thing with all the underlying processes and protocols that enable and support these interconnections.



-- Edewede Oriwoh, “Internet Of Things – the argument for Smart Forensics”

# Scope of the Problem

- IoT technology includes but not limited to the following components:
  - M2M: Machine to machine communications
  - RFID: Radio Frequency Identification
  - CAC: Context-aware computing
  - WUC: Wearable and Ubiquitous computing
- Other IoT related terms:
  - IoE: Internet of Everything
  - IoO: Internet of Objects
  - M2M: Machine to Machine communications
  - FI: Future Internet

# Scope of the Problem

- Forensics
  - *The use of science and technology to investigate and establish facts in criminal or civil courts of law.*

*www.thefreedictionary.com*

- Computer/Digital Forensics
  - *We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*

*www.us-cert.gov/reading_room/forensics.pdf*

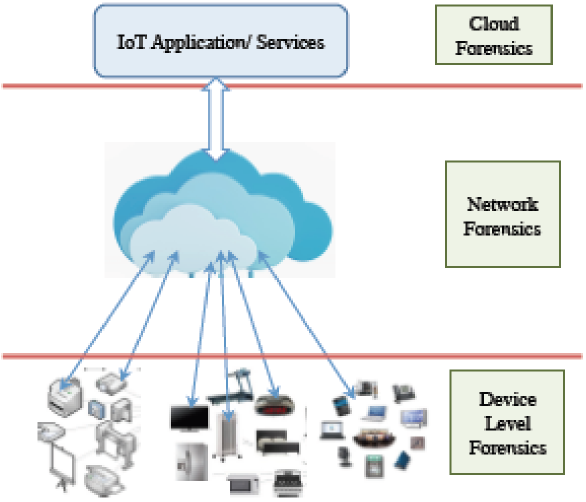
- Forensic Computing
  - *the process of* ***identifying***, ***preserving***, ***analyzing*** *and* ***presenting*** *digital evidence in a manner that is legally acceptable.*

*http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf*

# Scope of the Problem

- IoT Forensics:

  “Execute digital forensics procedures in the IoT paradigm”



IoT Application/ Services

Cloud Forensics

Network Forensics

Device Level Forensics

*by Zawoad, S. and Hasan, R.*

- Other related terms: Forensics of Things and Smart Forensics.

# Scope of the Problem

- Differences between IoT Forensics and IoT Security?
  - IoT Security:
    - Prevent malicious access to and activities on IoT devices and networks;
    - Prevent bad things from happening;
  - IoT Forensics:
    - Obtain digital evidence from IoT devices for a legal purpose;
    - Find who did the bad thing or prove you did not do the bad thing.

# Scope of the Problem

- Differences between IoT Forensics and Digital Forensics
  - Identification of the digital evidence:
    - Digital Forensics: hard drives, cell phone, network, and etc.
    - IoT Forensics: sensors, hearing aids, appliances, and etc.
  - Preservation of the digital evidence:
    - Digital Forensics: write-blocker and standard software, such as FTK, EnCase, and etc.
    - IoT Forensics: proprietary hardware and software among the IoT devices.

# Scope of the Problem

- Differences between IoT Forensics and Digital Forensics
  - Analysis of the digital evidence:
    - Digital Forensics: based on the information technology theories and principles;
    - IoT Forensics: heavily rely on the physical and mechanical nature of the things.
  - Presentation of the digital evidence:
    - Digital Forensics: demonstrations on computers or cell phones with oral presentation;
    - IoT Forensics: experimental demonstrations with the things that were involved with the oral presentation.

# Outline

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

# Issues with IoT Forensics

- Identification
  - What *are/were* available at the event/crime scene or a remote site?
    - Sensors on buildings or cars, surveillant videos, IT clouds, and etc.;
    - Who and what were there when the event/crime occurred?
  - What *is the workflow of IoT and the way the data is saved*?
    - What is the interaction between an IoT and its environment?
    - Where is the data saved and what format the data is stored and encoded?
  - What are the constraints for collecting the possible IoT evidence?
    - Jurisdiction, proprietary, standards, and etc.
  - What is the minimum set of the possible IoT evidence?
    - Is feasible or necessary to identify all possible sources for evidence?

# Issues with IoT Forensics

- Preservation
  - Is possible to collect evidence without changing the status of the evidence?
  - What are the available tools for collecting the possible IoT evidence?
  - How to preserve the IoT evidence which depends on its environment (temperature, humidity, or sound)?
  - Do we need to keep the “IoT” as part of evidence?

# Issues with IoT Forensics

- Analysis
  - IoT related knowledge in biology, physics, mechanics, and etc.;
  - Reconstruction of the IoT crime/event scene;
  - Common repository for storing IoT data;
  - Provenance of the evidence;
  - Court accepted tools for IoT data analysis.

# Issues with IoT Forensics

- Presentation
  - Can we present IoT evidence without showing IoT devices?
  - Can we present IoT evidence without demonstrating how IoT devices work?
  - Who should be the expert witnesses for presenting IoT related evidence (IoT forensic examiners, medical doctors, or mechanists)?

# Outline

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

## Strategies in Dealing with IoT Forensics

- Identification
  - Understand the case;
  - Assess the minimum set of the IoT evidence needed;
  - Estimate the cost in manpower, time, and money;
  - Start with what is or was available;
  - Consult with the legal team as often as possible;

## Strategies in Dealing with IoT Forensics

- Preservation
  - Seek the support from the manufactures, vendors, and customer services of the IoT devices;
  - Only collect the evidence that is collectable (avoid to destroying the evidence);
  - Save the data in a commonly acceptable format if possible;
  - Take pictures of IoT devices if necessary.

TOKYO, JAPAN

# Strategies in Dealing with IoT Forensics

ST. PAUL, MN, USA

- Analysis
  - Seek the professional opinions on the IoT evidence from the experts;
  - Study the interaction among IoT devices and the relationship between IoT devices and other local and remote devices;
  - Know the lifecycle of IoT devices;
  - Understand the IoT reactions to its environment.

TOKYO, JAPAN

# Strategies in Dealing with IoT Forensics

ST. PAUL, MN, USA

- Presentation
  - Expert witness can be presented by a team of the experts;
  - Use as many pictures as possible if they are sufficient to explaining the situation to the jurors;
  - A simple experiment on how an IoT device reacts to its environment is worth hundreds of pictures;
  - Only discuss the IoT devices where you are able to collect evidence.

# Outline

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

# Challenges and Future Work

- Identification
  - *Status*: the "things" often have different status according to the sensors, such as temperature of the object, speed of wind, or distance of the target;
  - *Location*s: can be anywhere, visible or invisible (behind scene, inside of human body, or too tiny to see);
  - *Relationship*: the connection between the things is critical (the sources, intermediate locations, and destinations, as well as any processing tasks in between)
  - *Timing*: the "things" might not be always on or down or in a "sleeping" stage;
  - *Data:* it could be distributed, aggregated, processed, or a by-product of human-device or device-to-device interaction, or a combination of device and data;

# Challenges and Future Work

- Preservation:
  - *Proprietary*: "open-source" standards are needed;
  - *Jurisdiction*: laws and regulations should be justified accordingly;
  - *Data Forma*t: the format stored and used by "things" should be standardized;
  - *Interface*: the interface of "things" should be standardized;
  - *Operating System*: Heterogeneous nature of the IoT cyberphysical environment presents a big challenge to have a standardized OS.

# Challenges and Future Work

- Analysis:
  - *What* is needed for the case?
  - *Where* are the places for finding the evidence?
  - *How* to extract the information that can be used as evidence?
  - *When* is the analysis sufficient?

# Challenges and Future Work

- Presentation:
  - *Documentation* of the trace of IoTs;
  - *Reconstruction* of the environment of IoTs;
  - *Demonstration* of the behaviors of IoTs;
  - *Education/Training* of the IoT expert witnesses.

# Challenges and Future Work

- What are the challenges for IoT forensics in the future?
  - A new branch of digital forensics or a new field
    - We even have not agreed on the definition
  - A moving target
    - Everything related to the IoT technology is changing
  - An evolutional area for the digital age
    - We don’t know what it is supposed to be
  - New cyberphysical environment
    - New hardware and software as well as new applications
  - New laws
    - More laws will be established to “civilize” the cyberphysical world
  - International cooperation
    - The concept of communities will be replaced by cyber villages or social networks

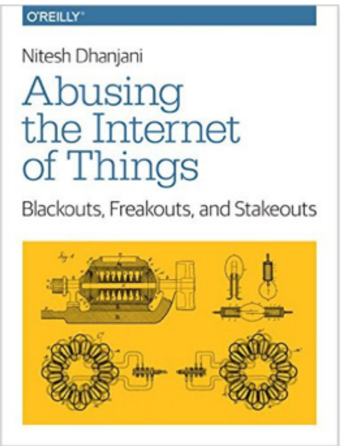
# Outline

- Introduction
- Scope of the Problem
- Issues with IoT Forensics
- Strategies in Dealing with IoT Forensics
- Challenges and Future Work
- Resources and Bibliographies

# Resources

## Nitesh Dhanjani

- Executive Director, the Americas Information Security Center of Excellence (CoE), Ernst & Young LLP, Seattle, WA, USA
- BS and MS in Computer Science, Purdue University


O'REILLY
Nitesh Dhanjani
Abusing the Internet of Things
Blackouts, Freakouts, and Stakeouts

TOKYO, JAPAN

# Bibliographies

ST. PAUL, MN, USA

- Hegarty, R. C., Lamb, D. J., and Attwood, A., *"Digital Evidence Challenges in the Internet of Things,"* the Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, Plymouth University, UK, July 8 – 9, 2014
- McKinsey & Company, *"The Internet of Things: Five Critical Questions,"* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_five_critical_questions
- Oriwoh, E., Jazani, D., Epiphaniou, G., and Sant, P., *"Internet of Things Forensics: Challenges and approaches,"* the Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, Texas, USA, October 20–23, 2013, pp 608-615
- Oriwoh, E. and Williams, G., *"Internet Of Things – the Argument for Smart Forensics,"* Chapter 26, Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, IGI Global, 2015, DOI: 10.4018/978-1-4666-6324-4.ch026, pp 407 - 423
- Zawoad, S. and Hasan, R., *"FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,"* the proceedings of the 12th IEEE International Conference on Services Computing, New York City, New York, June 27 to July 2, 2015.
- www.gartner.com, *"Gartner Says the Internet of Things Will Transform the Data Center,"* 2015, http://www.gartner.com/newsroom/id/2684616
- www.idc.com, *"Finding Success in the New IoT Ecosystem,"* 2014, http://www.idc.com/getdoc.jsp?containerId= prUS25237214.

TOKYO, JAPAN

# Thank You

ST. PAUL, MN, USA

Heartfelt appreciation goes to
***Prof. Sasaki, Prof. Uehara, and IDF members***
for their invitation and generosity!

Thank you all for attending!

**arigatoogozaimasu!**

Contact Information
*Jigang Liu* : `Jigang.Liu@metrostate.edu`