DATA STORAGE SECURITY SUMMIT

IoT Security: Problems, Challenges and Solutions

LIWEI REN, PH.D
Trend Micro

DATA STORAGE SECURITY SUMMIT

01010011 01001110 01001001 01000001

SEPTEMBER 24, 2015
SANTA CLARA, CA

SNIA

Background

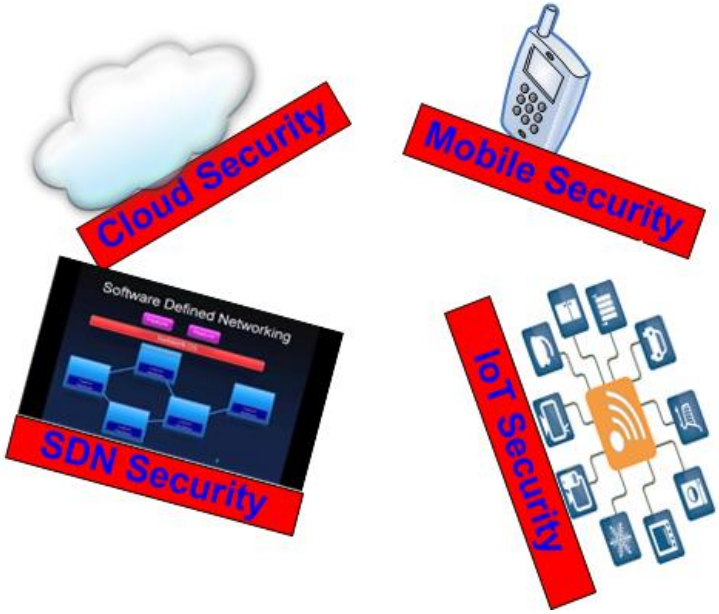
- **Liwei Ren**
  - Research interests
    - Data security & privacy, network security analysis
    - Data compression, math modeling & algorithms
  - Measurable contributions:
    - 10+ academic publications
    - 20+ US patents granted
    - 1 security software company in Silicon Valley with successful exit.
  - Education
    - MS/BS in mathematics, Tsinghua University, Beijing
    - Ph.D in mathematics, MS in information science, University of Pittsburgh
- **Trend Micro™**
  - Global security software vendor with headquarter in Tokyo, and R&D centers in Silicon Valley, Nanjing and Taipei.
  - A leader in cloud security.

Agenda

- Why do I have this sharing?
- IoT security: trends, problems and challenges
- A few security technologies & IoT
- Standard security protocols
- Summary

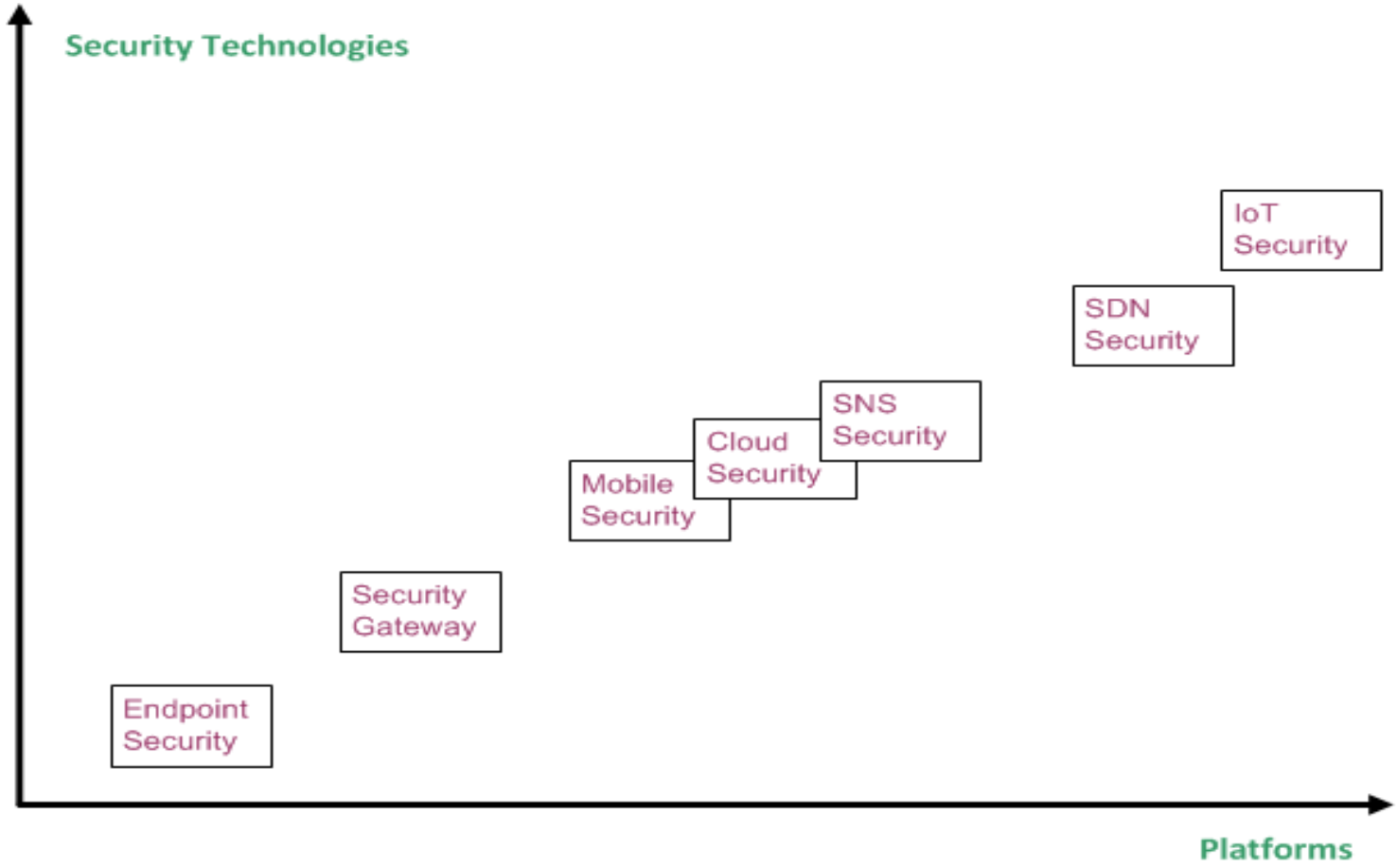
Why do I have this sharing?

- **I am not an expert in IoT security yet☺**
  - What ?
  - Why do you share?
- **A new computing platform leads to new security problems & challenges…**
  - and new opportunities as well!
- **I started to investigate IoT security after RSA conference in April:**
  - Too many questions (???)
  - I like to invite experts to discuss via this sharing



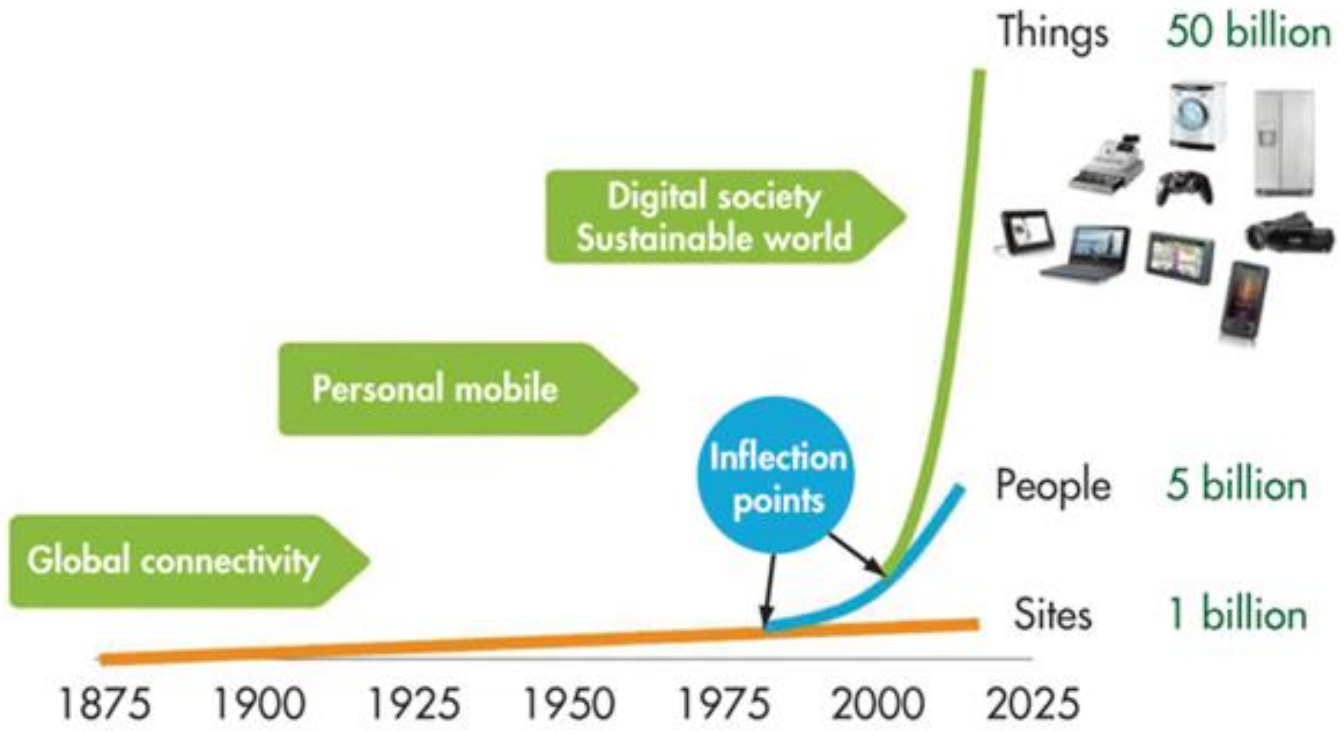
Why do I have this sharing?

- IoT security means new opportunities for a security professional (like myself) to develop novel security solutions!



IoT security: trends, problems and challenges

- **Trends (Stan Schneider | *Electronic Design*)**



IoT security: trends, problems and challenges

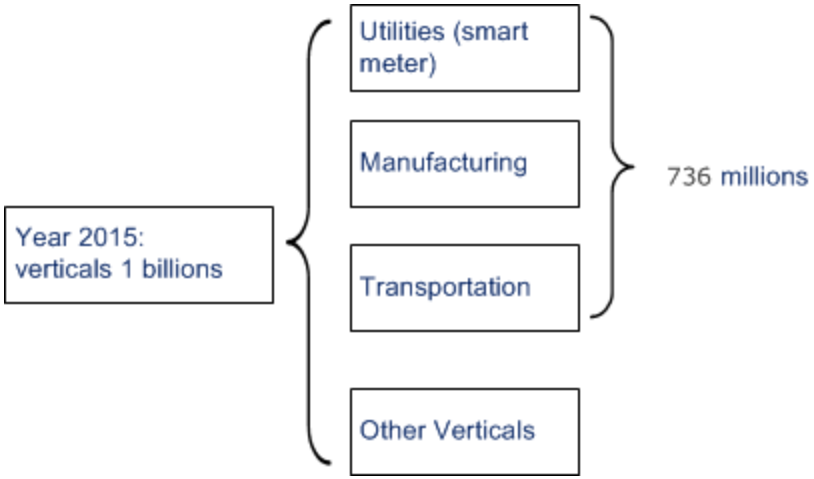
DATA STORAGE SECURITY SUMMIT

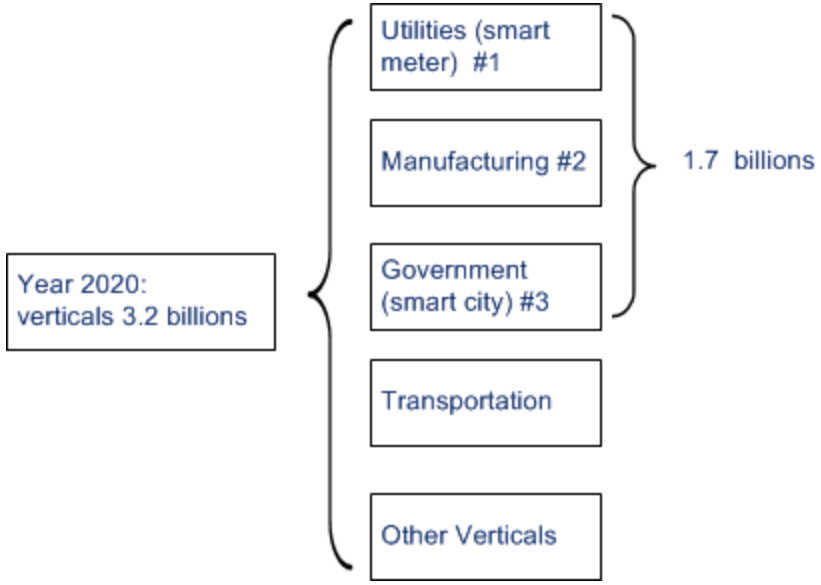
- **Categories & Numbers:**
  - Source: Gartner Nov,2014)
  - Internet of Things Units Installed Base by Category in Million

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	3,032.0	3,750.0	4,880.6	25,006.6

IoT security: trends, problems and challenges

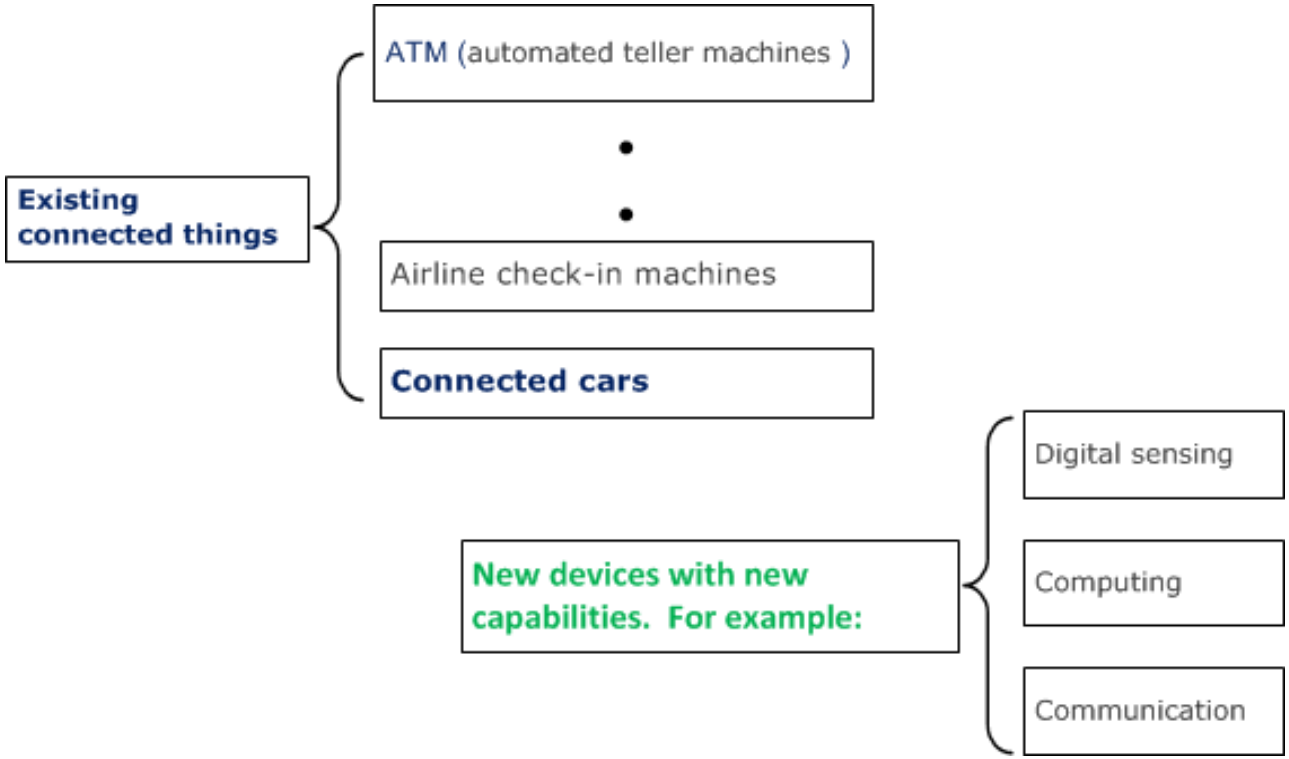
- **Categories & Numbers** :





IoT security: trends, problems and challenges

- **What's new?**



IoT security: trends, problems and challenges

DATA STORAGE SECURITY SUMMIT

Security cases

Attack Name	Story	Resource	Date
Car recall	Chrysler recalled 1.4 million hackable cars in July, 2015	CNN News	July 24, 2015
Lizard Stressor	An attack online service hosted in Bosnia. It can convert homes and commercial routers into a zombie horde.	An online article	Jan 2015
	First wide-scale hack involving television sets and at least one refrigerator ☺. 750,000 spams were sent.	Proofpoint	Jan,2014
Linux.Darlloz	Discovered a worm for devices running Linux .	Symantec	Nov, 2013
Hacked Camera	A hacker was able to shout abuse at a two-year-old child by exploiting a vulnerability in a camera advertised as an ideal "baby monitor".	ABC News	Aug, 2013

IoT security: trends, problems and challenges

- **Problems and security challenges**
  - Many small devices have limited CPU power
    - Not much processing power for security
      - Need to look for new encryption scheme with less CPU power.
      - Can not install AV software☺
    - Example: IP-addressable light bulbs.
  - IoT also needs both encryption key management and identity management
    - It may scale into billions!

IoT security: trends, problems and challenges

- **Problems and security challenges**
  - New devices for endpoint security
    - New firmware, embedded OS, new software & etc.
      - It is not possible to support AV on every device.
  - New transport protocols for making network security difficult!
  - Much more network traffic for security analysis
    - Bad news for large enterprises as network security is already complex and cumbersome

IoT security: trends, problems and challenges

DATA STORAGE SECURITY SUMMIT

- **Seven IoT security risks***:
  1. Disruption and denial-of-service attacks
  2. Understanding the complexity of vulnerabilities
  3. IoT vulnerability management
  4. Identifying, implementing security controls
  5. Fulfilling the need for security analytics capabilities
  6. Modular hardware and software components
  7. Rapid demand in bandwidth requirement

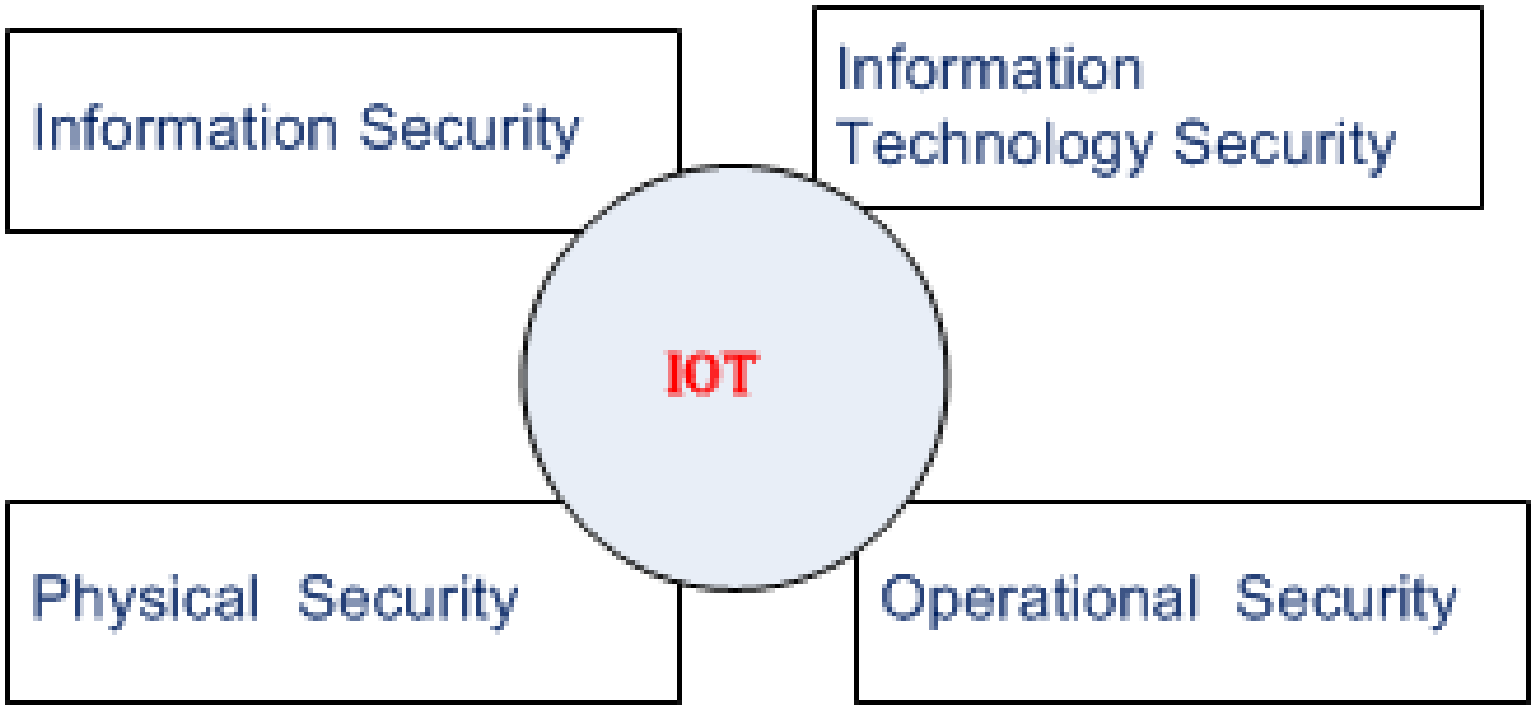
***Source:** INFORMATION SECURITY INSIDER EDITION / SECURING THE INTERNET OF THINGS, AUGUST 2014

IoT security: trends, problems and challenges

- **IoT Security Top 10 (OWASP 2014):**
  - I1 Insecure Web Interface
  - I2 Insufficient Authentication/Authorization
  - I4 Lack of Transport Encryption
  - I5 Privacy Concerns
  - I9 Insecure Software/Firmware
  - I3 Insecure Network Services
  - I6 Insecure Cloud Interface
  - I7 Insecure Mobile Interface
  - I8 Insufficient Security Configurability
  - I10 Poor Physical Security

IoT security: trends, problems and challenges

- **IoT will merge the following domains:**



IoT security: trends, problems and challenges

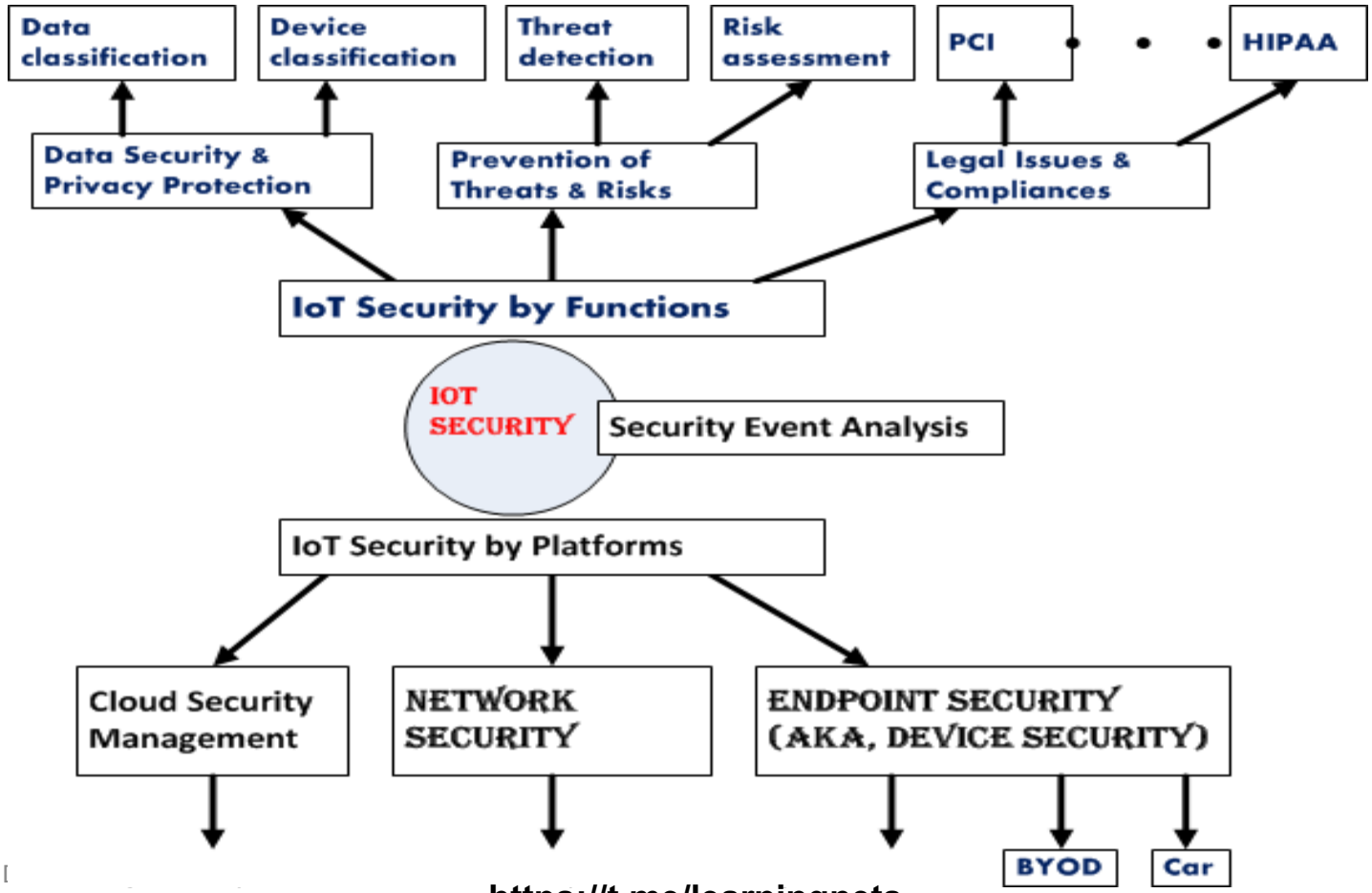
DATA STORAGE SECURITY SUMMIT

- **In the era of IoT,**
  - Do we need new concepts to describe IoT security ?
  - Do we need new security models for IoT?

- **What is the gap between IoT security and existing security solutions?**
  - When cloud arrived, what did we do for new solutions?
  - When smart phones and BYOD come, what did we do?
  - What makes IoT different from the last two major waves?

A few security technologies & IoT

- Simple taxonomy of IoT security

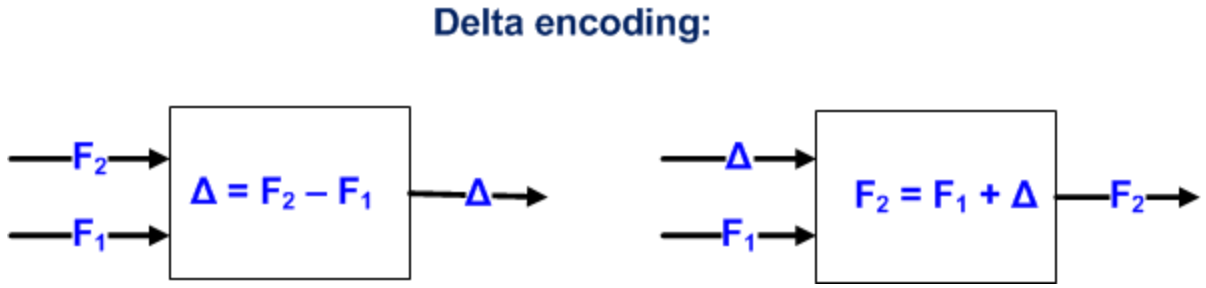


A few security technologies & IoT

- **My interests for evaluating a few solutions:**
  - Endpoint security
    - **Vulnerability and patch management**
  - Network security
    - **Network monitoring & visibility**
    - **NetFlow based security analysis**

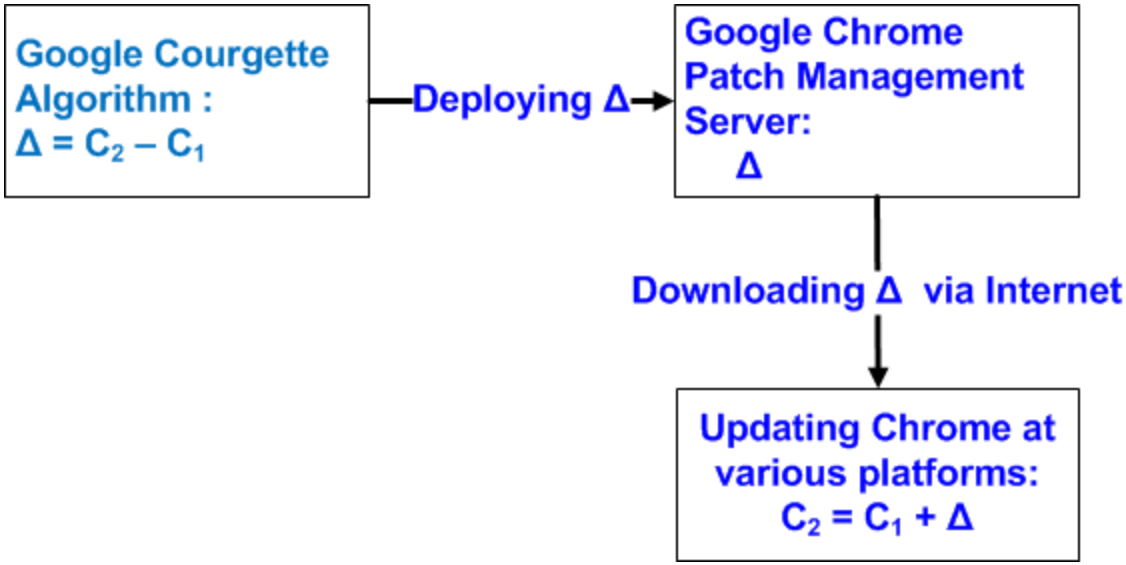
A few security technologies & IoT

- **Vulnerability and patch management with FOTA**
  - **FOTA** = ***F***irmware ***O***ver ***T***he *A*ir
  - FOTA is a technology developed for updating the firmware of mobile phones due to software bug fixes.
  - It uses delta encoding (aka, differential compression) technique to reduce the patch size.
  - Delta encoding can be shown as follows conceptually:



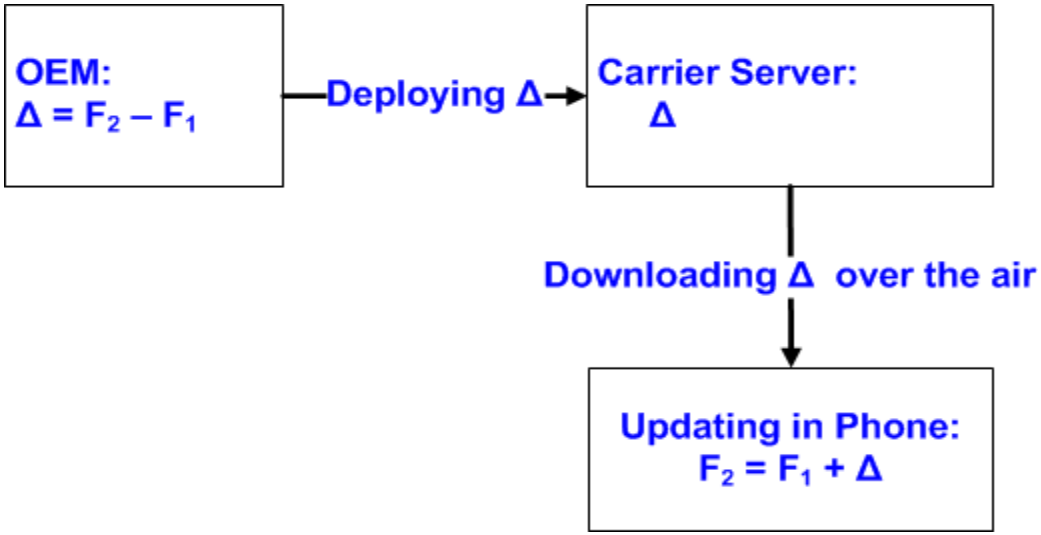
A few security technologies & IoT

- **Vulnerability and patch management with FOTA**
  - Delta encoding was used for software vulnerability management. A significant example is Google Chrome software updating powered by an very efficient delta coding algorithm *Courgette*
  - We use the same concept for IoT device security.



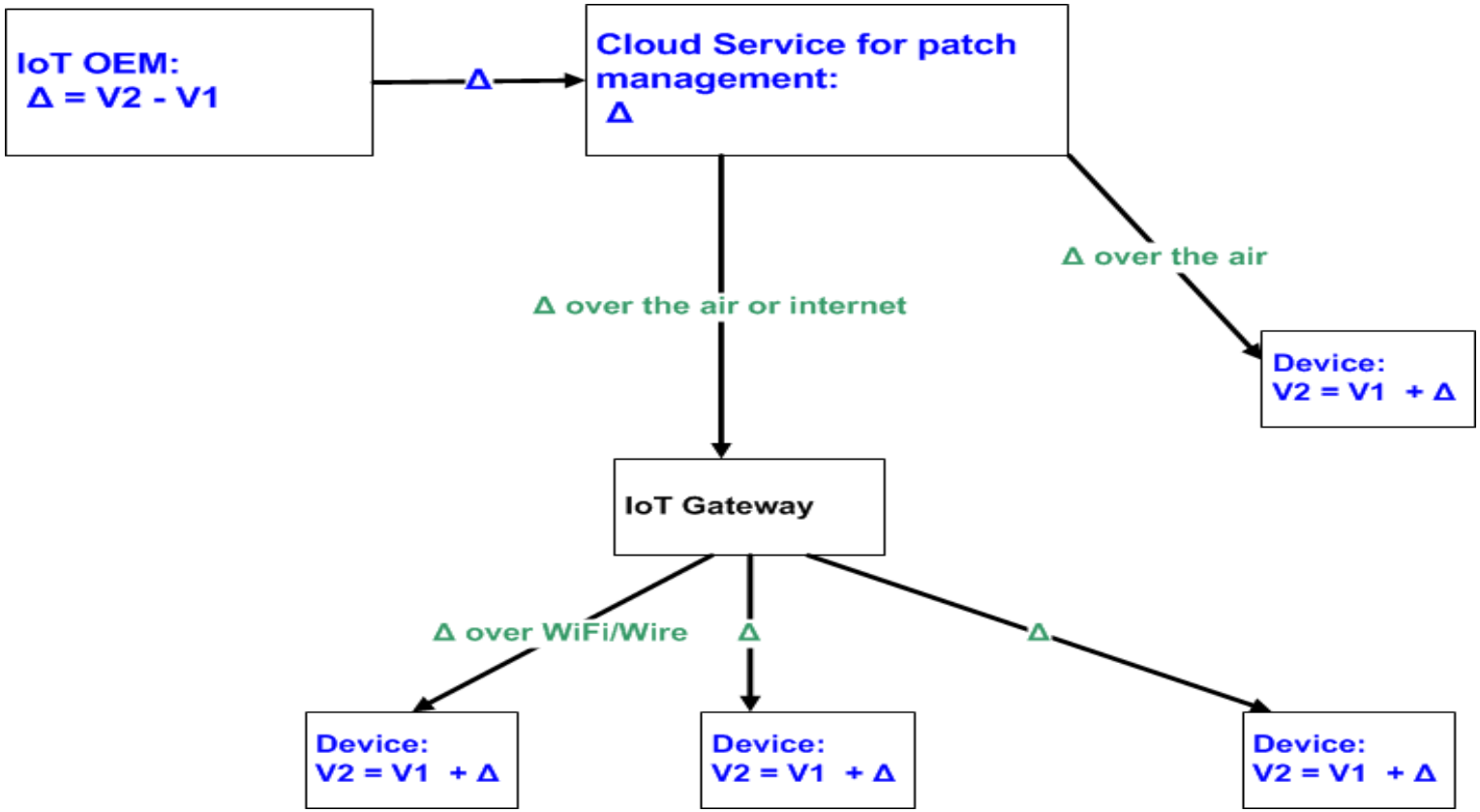
A few security technologies & IoT

- **Vulnerability and patch management with FOTA**
  - **FOTA** for bug fix of mobile phones in old days, and vulnerability management as well today.
  - **FOTA** is also under development for car ECU patch management in the field of telematics, for the security purpose.



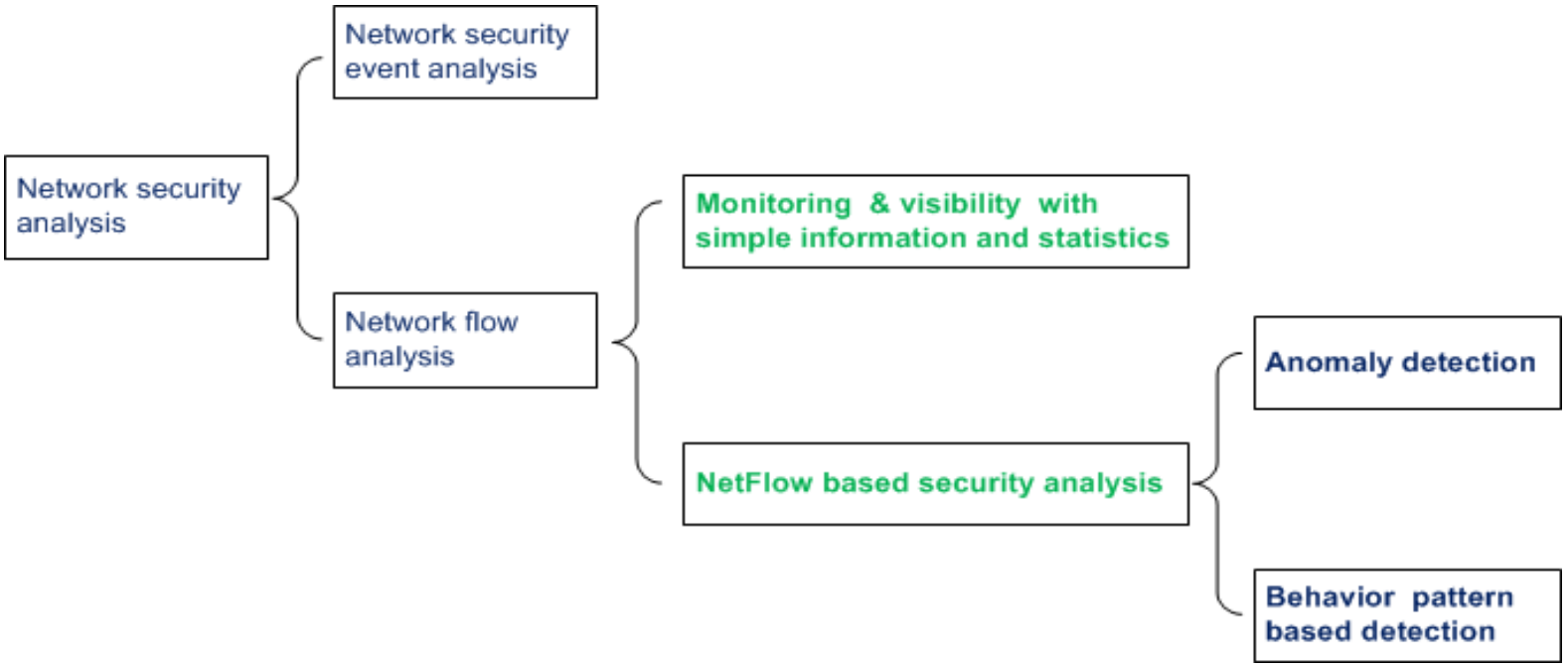
A few security technologies & IoT

- **Vulnerability and patch management with FOTA**
  - **FOTA** for IoT security for general devices:



A few security technologies & IoT

- **Network Security:**
  - Network monitoring & visibility
  - NetFlow based security analysis



A few security technologies & IoT

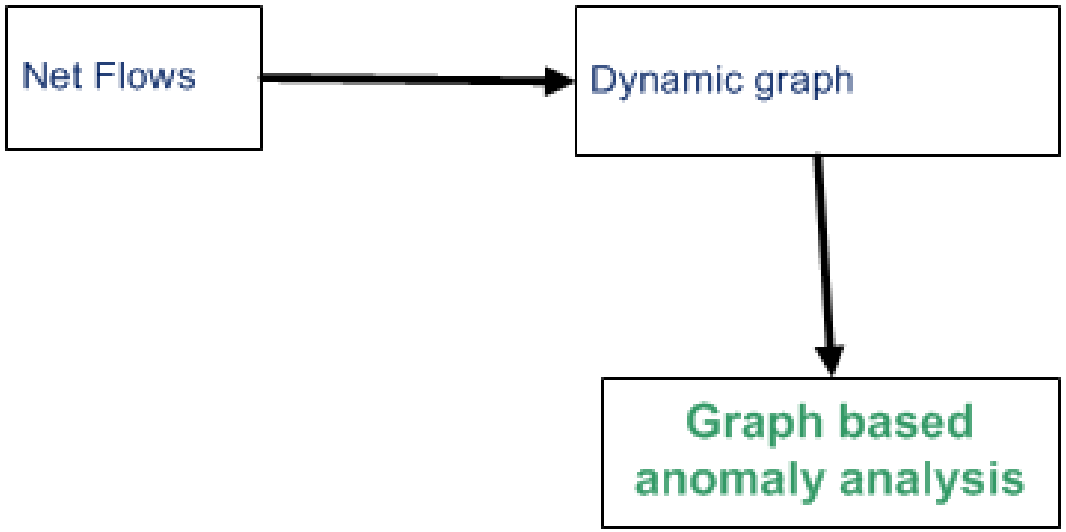
- **Network Security:** monitoring & visibility with simple information:
  - How many devices are there in this enterprise network?
  - What kind of devices are they?
  - Which devices transfer data which is not encrypted.
  - Which has heavy volume of traffic?
  - Which devices are most active ?
  - …

A few security technologies & IoT

- **Network Security:** NetFlow based security analysis
  - NetFlow is a router feature that collects IP network traffic as it enters or exits an interface.
  - Version 5 collects the following values:
    - …
    - Timestamps for the flow start and finish time, in milliseconds since the last boot.
    - Number of bytes and packets observed in the flow
    - source & destination IP addresses
    - Source and destination port numbers for TCP, UDP, SCTP
    - ICMP Type and Code.
    - IP protocol
    - Type of Service (ToS) value
    - …

A few security technologies & IoT

- **Network Security:** NetFlow based security analysis



Standard security protocols

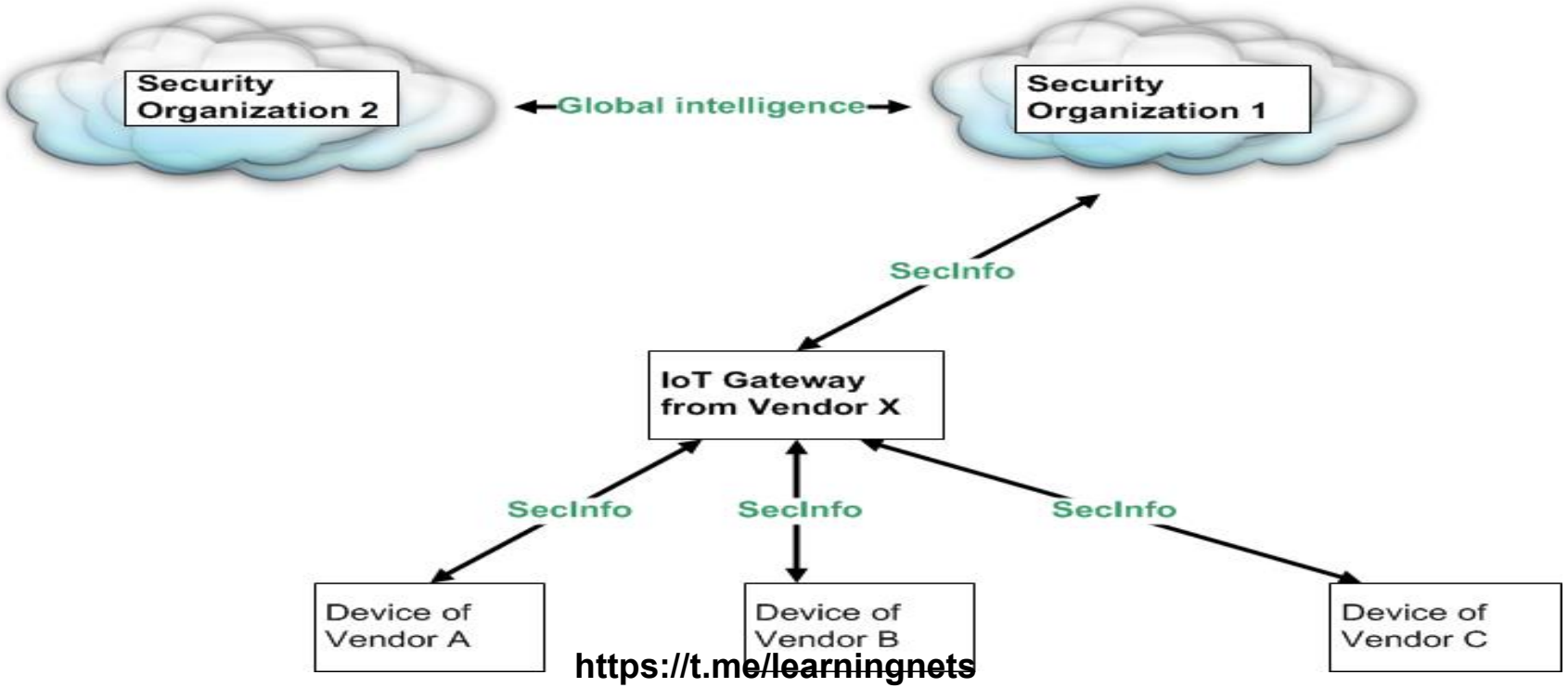
- **Why do we need a security information protocol such as OpenIOC?**
  - Describing security information
  - Retrieving actionable security information
  - Exchange security information between organizations
  - Technical support for an intelligence security model
- **How many security information protocol?**
  - OpenIOC
  - CybOX
  - IODEF

Standard security protocols

- **What is security information?**
  - A piece of information that can be used to search for or identify potentially compromised systems.
  - Example:
    - IP Address / Domain Name
    - URL
    - File Hash
    - Email Address
    - X-Mailer
    - HTTP User Agent
    - File Mutex
    - …….

Standard security protocols

- **Why do I discuss these security information protocols?**
  - There are still many security vendors not using protocols for exchanging information. A best practice is encouraged!
  - Currently, these three protocols are not unified yet. This is not good!
  - My personal opinion:
    - They will become even more important in the era of IoT security.



Summary

- IoT: trends & security challenges
- A few security technologies for IoT
- Why standard security protocols are important.

Additional Information

- **IoT Security Startups**
  - ZingBox
  - VisualThreat : car cyber security
  - Bastille Networks
  - Mocana
  - …
- **Interesting news**:
  - September 2015: McAfee created a new Automotive Security Review Board (ASRB).
  - August 2015: Symantec announced that it is securing 1 billions IoT devices.
  - July 2015: Symantec and Frost Data Capital work together to fund early-stage startups in big data and IoT security
  - May 2015: Google is offering a lightweight OS for IoT devices.

Q & A

- Thank you for your attention!
- Do you have questions?

- Email: liwei_ren@trendmicro.com
- Home page: https://pitt.academia.edu/LiweiRen