IoT (Internet of Things) & Security

AhnLab
Ingoo Bang
Contents

01  Recent Trends on Cyber Threat

02  Security Paradigm Shift

03  Evolution of Computing Environment

04  IoT and Security
01

Recent Trends on Cyber Threat
Steady Spread of new cyber threat

- Spear Phishing
- Ransomware
- Point of Sales Hacking
- Wireless Malware
2015 top prospect security issues by security vendors

AhnLab: Mobile/PC security threats on banking

Estsoft: Victim/technique diversification as IoT business grows

Egloo Security: Increased damage due to advanced ransomware

McAfee: Increasing mobile threats

Symantec: Increasing mobile threats

Kaspersky: Increasing mobile threats

Websense: Increasing mobile threats

McAfee: Combination of cryptographic + traditional attack increasing

Symantec: Increased threat on mobile/POS attack

Kaspersky: Targeted on smart home

Websense: Threats on IoT (Industrial Sensors)

AhnLab: Victim/technique diversification as IoT business grows

Estsoft: Increased damage due to advanced ransomware

Egloo Security: Increased security threats against Linux/MacOS

McAfee: New threats on mobile payment

Symantec: Mobile threats

Kaspersky: Mobile threats

Websense: Mobile threats

McAfee: Security perspective from perimeter to data

Symantec: Increasing mobile threats

Kaspersky: Ransomware

Websense: Ransomware

AhnLab: Threats on data stored and transmitted by IoT

Estsoft: Threats on data stored and transmitted by IoT

Egloo Security: Threats on data stored and transmitted by IoT

McAfee: Threats on data stored and transmitted by IoT

Symantec: Threats on data stored and transmitted by IoT

Kaspersky: Threats on data stored and transmitted by IoT

Websense: Threats on data stored and transmitted by IoT

McAfee: Advanced threat via browser extension

Symantec: Increasing non-windows target attacks

Kaspersky: Personal information

Websense: Email Threat

McAfee: Increasing unknown vulnerability

Symantec: DDoS

Kaspersky: Small groups of cyber criminals

Websense: New cyber war

McAfee: Sandbox-detour attacks

Symantec: Importance on user behavior

Kaspersky: Targeted on Mac OS with illegal SW/Torrent

Websense: Data management / cloud computing

McAfee: BERserk attack

Symantec: Data management / cloud computing

Kaspersky: Data management / cloud computing

Websense: Data management / cloud computing

McAfee: Reliability abuse attacks

Symantec: Strong cooperation cyber security

Kaspersky: Strong cooperation cyber security

Websense: Strong cooperation cyber security

Privacy violation via mobile app
Household Items

South Korean woman's hair 'eaten' by robot vacuum cleaner as she slept

- Built-in Camera enables remote access via PC or Smartphones
- Easy to control through remote access

From 2002, Over 10 millions of copies of Roomba, iRobot have been sold

Remote Monitoring Controlling Device

http://www.samsung.com/sec/consumer/living-appliances/vacuumcleaners/robottango/VC-RM96WN
Within two years, 90% of all IT networks will have an IoT-based security breach

‘IDC FutureScape’ provided organizations with insight and perspective on long-term industry trends along with new themes that may be on the horizon. The Predictions Web conference series and accompanying IDC FutureScape reports are designed to help company leaders capitalize on emerging market opportunities and plan for future growth.

1. **IoT and the Cloud.** Within the next five years, more than 90% of all IoT data will be hosted on service provider platforms as cloud computing reduces the complexity of supporting IoT "Data Blending".

2. **IoT and security.** Within two years, 90% of all IT networks will have an IoT-based security breach, although many will be considered "inconveniences." Chief Information Security Officers (CISOs) will be forced to adopt new IoT policies.

3. **IoT at the edge.** By 2018, 40% of IoT-created data will be stored, processed, analyzed, and acted upon close to, or at the edge, of the network.

4. **IoT and network capacity.** Within three years, 50% of all networks will transition from having excess capacity to handle the additional IoT devices to being network constrained with nearly 10% of sites being overwhelmed.

5. **IoT and non-traditional infrastructure.** By 2017, 90% of datacenter and enterprise systems management will rapidly adopt new business models to manage non-traditional infrastructure and BYOD device categories.

6. **IoT and vertical diversification.** Today, over 50% of IoT activity is centered in manufacturing, transportation, smart city, and consumer applications, but within five years all industries will have rolled out IoT initiatives.

7. **IoT and the Smart City.** Competing to build innovative and sustainable smart cities, local government will represent more than 25% of all government external spending to deploy, manage, and realize the business value of the IoT by 2018.

8. **IoT and embedded systems.** By 2018, 60% of IT solutions originally developed as proprietary, closed-industry solutions will become open-sourced allowing a rash of vertical-driven IoT markets to form.

9. **IoT and wearables.** Within five years, 40% of wearables will have evolved into a viable consumer mass market alternative to smartphones.

10. **IoT and millennials.** By 2018, 16% of the population will be Millennials and will be accelerating IoT adoption due to their reality of living in a connected world.

"The Internet of Things will give IT managers a lot to think about," said Vernon Turner, Senior Vice President of Research. "Enterprises will have to address every IT discipline to effectively balance the deluge of data from devices that are connected to the corporate network. In addition, IoT will drive tough organizational structure changes in companies to allow innovation to be transparent to everyone."
02

Security Paradigm Shift
Development of Computing Environment and Security

1980
- Mainframe
- PC

1990
- Web
- Internet

2000
- Browser
- SNS
- Smart Phone
- Tablet

2010
- Cloud
- Big Data
- IoT

SECURITY THREAT
- Virus
- Trojan
- Worm
- Spyware
- Hoax
- Phishing
- Social Engineering
- Smishing
- Game Hack
- APT (Advanced Persistent Threat)
- Hacktivism

SECURITY SOLUTION
- Anti-Virus
- Firewall
- E-mail SPAM Filter
- IDS (Intrusion Detection System)
- IPS (Intrusion Prevention System)
- Anti-DDoS
- Anti-spyware
- MDM (Mobile Device Management)
- MAM (Mobile Application Management)
- MCM (Mobile Content Management)
- Web Firewall
- Virtualization
- ATD (Advanced Threat Defense)
- Forensics
Cyber Security

Signature Based

Vulnerability Context Analysis

Secure Contents Management

Identity and Access Management

MSS

Managed Security Service

Threat Intelligence

SCM

IAM
03

Evolution of Computing Environment
New Emerging Computing Environment every 5 years

1984: Personal Computer
1989: Dial-up Text Computing
1994: Desktop PC
1999: Portable PC
2004: Notebook Netbook
2009: iPhone Android
2014: Internet of Things
2019: Smart CAR

Paradigm Shift through time

PC

Post PC

Homogeneity

Heterogeneity

Program

Application

Rapid Environmental Changes
The Evolution of the Desk

The evolution of the desk by the Harvard Innovation Lab
http://imgur.com/tWvyfya
The Evolution of the Desk

The evolution of the desk by the Harvard Innovation Lab

http://imgur.com/tWvyfya
04

IoT and Security
Top 10 Strategic Technologies 2011 ~ 2015 by Gartner

2011
- Cloud Computing
- Mobile Applications / Media Tablets
- Social Communications / Collaboration
- Video
- Next-Generation Analytics
- Social Analytics
- Context-Aware Computing
- Storage Class Memory
- Ubiquitous Computing
- Fabric-based Infrastructure/Computer

Internet of Things

2012
- Media Tablets and Beyond
- Mobile-Centric Applications / interfaces
- Contextual and Social User Experience
- App Stores and Marketplaces
- Next-Generation Analytics
- Big Data
- In-Memory Computing
- Extreme Low-Energy Servers
- Cloud Computing

Internet of Things

2013
- Mobile Device Battles
- Mobile Applications and HTML5
- Personal Cloud
- Hybrid IT and Cloud Computing
- Strategic Big Data
- Actionable Analytics
- In Memory Computing
- Integrated Ecosystems
- Enterprise App Stores

Internet of Things

2014
- Mobile Device Diversity and Management
- Mobile Apps and Applications
- Hybrid Cloud and IT as Service Broker
- Cloud/Client Architecture
- The Era of Personal Cloud
- Software Defined Anything
- Web-Scale IT
- Smart Machines
- 3-D Printing

Internet of Things

2015
- Computing Everywhere
- 3D Printing
- Advanced, Pervasive and Invisible Analytics
- Context-Rich Systems
- Smart Machines
- Cloud/Client Computing
- Software-Defined Apps/Infrastructures
- Web-Scale IT
- Risk-Based Security and Self-Protection
Top 10 Strategic Technologies 2011 ~ 2015 by Gartner

- **2011**: Mobile
- **2012**: Tablet
- **2013**: Big Data
- **2014**: Cloud
- **2015**: Internet of Things
Gartner’s view on IoT (2011 vs 2014)

Hype cycle 2011 - http://www.gartner.com/newsroom/id/1763814
Hype cycle 2014 - http://www.gartner.com/newsroom/id/2819918
Internet of Things, IoT

- Technology connecting physical objects with embedded computing system and communication ability
- **Share information of the objects which can be uniquely identified**
- A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies.
  – ITU: International Telecommunication Union
- A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols
  – IETF: Internet Engineering Task Force
- Exchange of measurable data such as a temperature, humidity, angle, weight, and location based on standard communication protocols

Source: Cisco IBSG, April 2011

http://www.kisa.or.kr/uploadfile/201306/201306101746357807.pdf
In CES 2015 (Consumer Electronics Show)

- Individual broadcasting via smartphones, selfie stick, microphones
- No camera operator, lighting, broadcasting equipment necessary
- Effective on cases such as on-the-spot live broadcast for large-scale event or immediacy of the news is required
- Self covering, editing, broadcasting reporter shown in CES 2015

http://imgur.com/tWvyfya
IoT Extends its capability

How Smart, Connected Products Are Transforming Competition, Michael E. Porter and James E. Heppelmann

Comprehensive monitoring and alerts via sensors and external information

These features are available via built-in product or cloud software

Monitoring

Control

Optimization

Autonomy

• Improve performance
• Preventive treatment, service
• Improve and customize personalized product
• Self treatment and service

Harvard Business Review Korea, How Smart, Connected Products Are Transforming Competition, Michael E. Porter and James E. Heppelmann, p. 64, November 2014
# The IoT Services

## Service Examples of IoT

<table>
<thead>
<tr>
<th>Vehicle</th>
<th>Meter</th>
<th>Remote Maintenance</th>
<th>Environment Monitoring</th>
<th>Security</th>
<th>Industrial Computing</th>
</tr>
</thead>
</table>
| • Vehicle information  
• Notify emergency  
• Detect stolen vehicle  
• Navigation  
• Toll auto payment | • Electricity Smart-Meter  
• Gas Smart-Meter  
• Water Smart-Meter  
• Control Multi Utility | • Remote Service  
• Preventive Maintenance  
• Remote Control | • Air pollution monitoring  
• Water pollution monitoring  
• Remote measure and analysis | • Control CCTV | • Logistics scanner  
• Industrial PDA  
• On-site assessment terminal |
| Medical Treatment | Path Trace | Payment | Environment Monitoring | Security | Industrial Computing |
| • Remote monitoring  
• Remote treatment  
• Disease control | | • POS terminal  
• Vending machine  
• ATM | | • Air pollution monitoring  
• Water pollution monitoring  
• Remote measure and analysis | | • Logistics scanner  
• Industrial PDA  
• On-site assessment terminal |

Korea Telecommunications Technology Association (2011)

http://www.kisa.or.kr/uploadfile/201306/201306101746357807.pdf
The Internet of Everything 2015

- Devices surrounding us will grow rapidly until 2019

- Majority will be tiny things that consists of Internet of Things

- PC, Smartphone, Tablet will grow but the market share will not likely be big

- Five or more years to prepare for Smart TV, Wearable, Connected Car

The Internet of Things Will Be The World’s Most Massive Device Market

- The IoT will result in $1.7 trillion in value added to the global economy in 2019

- Device shipments will reach 6.7 billion in 2019 for a five-year CAGR of 61%

- The main benefit of growth in the IoT will be increased efficiency and lower costs.

- The IoT lacks a common set of standards and technologies that would allow for compatibility and ease-of-use
Elements and major assignment of IoT by Gartner

**The IoT is About Business Models**

- Service
- Gateway
- Thing

**Implementation Challenges**

- Security: Diversified Threats
- Standards: Required for scale
- Value: System Reliability QoS

http://www.gartner.com/it/page.jsp?id=2833417
Increasing population and expanding things

- Year 2003 – 6.3 Billions world population, 500 Millions connected devices (0.08 connected devices per person)
- Year 2008~2009 connected devices per person exceeds 1
- Year 2010 – 6.8 Billions world population, 12.5 Billions connected devices (1.84)
- Year 2015 – 7.2 Billions world population, 25 Billions connected devices (3.47)
- Year 2020 – 7.6 Billions world population, 50 Billions connected device(6.58)

Source: Cisco IBSG, April 2011

Expansion of things and connection to the Internet

“Things” refer to any physical object with a device that has its own IP address and can connect & send/receive data via a network.

- Dog: 0.5 Billion
- Cat: 0.5 Billion
- Cow: 1.5 Billion
- Pig: 1 Billion
- Chicken: 20 Billion

23.5 Billion

* Monitoring path and health of cows with sensors on ears: 200MB per year
Expansion of things and connection to the Internet

- **IPv4**: 4.3 Billion
- **IPv6**: 281 Trillion
Twenty Internet of Things trends to watch in 2015

IBM Center for Applied Insights, 2015.1.27.

1. Security & Privacy
2. Standards
3. Hardware
4. Software
5. Edge Analytics
6. Machine-to-Machine (M2M) automation
7. Platform-to-Platform integration
8. Wearables
9. Sensor fusion
10. Sensor hubs
11. Big data
12. Blockchain
13. Success stories
14. Chief IoT Officer
15. Business process transformation
16. Education needed
17. Product design
18. Network bandwidth
19. Vertical clouds
20. Industry partnerships

Twenty Internet of Things trends to watch in 2015

1. **Security & privacy:** Trust and authentication become critical across all elements of the IoT, including devices, the networks, the cloud and software apps.

2. Standards: Competing proprietary and open source standards efforts have continued to struggle to come together for common good, but perhaps we will see breakthroughs in 2015.

3. Hardware: Advanced microcontrollers, systems on chips, and sensor technologies are enabling new types of IoT devices. These devices are also getting smaller, smarter and cheaper.

4. Software: A huge rush of activity is expected as developers increase their focus on developing IoT platforms and solutions that upload data from sensors and perform the analytics necessary to deliver the insights required for business decision.

5. Edge analytics: Increasingly, analytics capabilities will be pushed to the edge of networks. Advanced analytics and dashboards will be needed to provide insights from all the “things.”

6. Machine-to-machine (M2M) automation: In the future, sensors, devices and whole IoT systems will be talking to each other, providing insights and making decisions without human intervention.

7. Platform-to-platform integration: Expect movement from closed platforms toward open IoT platforms that support multiple applications, devices, and networks.

8. Wearables: As the market matures, watch this category closely as sensor hubs and software platforms to support wearables evolve.

9. Sensor fusion: Combining data from different sources can improve accuracy. Data from two sensors is better than data from one. Data from lots of sensors is even better.

10. Sensor hubs: Developers will increasingly experiment with sensor hubs for IoT devices, which will be used to offload tasks from the application processor, saving power and improving battery life in the devices.

11. Big data: “Things” (sensors, chips, computers) will produce even more data than we have now, taxing our already complex enterprise information management systems.

12. Blockchain: Using blockchain technology, developers can set up a distributed model that doesn’t require trusting every node in the network.

13. Success stories: To move from hype to real mass adoption, vendors need to provide customer case studies that prove the benefits that await enterprises.

14. Chief IoT Officer: Expect more senior level execs to be put in place to build the enterprise-wide IoT strategy.


16. Education needed: Demand will rise for education and skills training related to IoT systems, how to develop applications, implement them and what to do with the data collected.

17. Product design: Consumers and customers will increasingly expect products to come with embedded sensors that can connect to mobile devices and IoT systems.

18. Network bandwidth: As more devices come online, networks will clog and service providers will be in a never-ending battle to increase network capacity.

19. Vertical clouds: Aggregating all this big data and acting on its findings will best be achieved by capturing, analyzing and responding from the cloud. In 2015, expect specialized and vertical IoT cloud services.

20. Industry partnerships: Traditional IT vendors will accelerate their partnerships with global telecom service providers, semiconductor vendors, and vertical IoT platform providers.
Growth in Security Solutions Shifting from Reactive to Proactive

2020
$50B

$25B

$5B

Federated Single Sign-On (FSSO)
Threat Intelligence
Cloud
Mobile
Software Defined Networks (SDN) security
IoT Security
Security as a Service
User Provisioning
Policy and Compliance
Distributed Denial of Service Security
Security Device Management
Data Loss Prevention
Server Security
Intrusion Prevention
Proactive Endpoint Risk
Management (IEM)
Security Information and Event Management (SIEM)
Specialized Threat Analysis and Protection (STAP)

Almost 50% of cloud security will be delivered by the cloud to protect applications and data in the cloud

Almost 50% of cloud security products will be 10x more valuable than traditional technologies

20% of security markets will shift protecting people and their assets to securing "things" that communicate among themselves without direct human interaction

A Revolution in the Size and Shape of Computing

Intel® Curie™ module: reimagining wearable technology solutions

The Intel® Curie™ module is a highly integrated hardware module that can power a solution the size of a button.

http://techcrunch.com/2015/01/06/intel-wearables-chip/
Tiny Things.. Chips & TrackR sticker

Key Features

- A low-power, 32-bit Intel® Quark™ SE SoC
- 384kB Flash memory, 80kB SRAM
- A low-power integrated DSP sensor hub with a proprietary pattern matching accelerator
- Bluetooth* Low Energy
- 6-axis combo sensor with accelerometer and gyroscope

- Easy to find the exact location with this attached : to prevent valuable items, bicycles, bags and even pets from loss.
  - Diameter : 25 mm
  - Thickness : 5 mm
  - Battery Life : 1 year
  - Battery Type : Replaceable CR2016 Battery
  - Bluetooth 4.0 (Bluetooth Low Energy) Built-in
  - Device Compatibility
    - iPhone 4s & Later, iPad 3rd Generation & Later
    - Android 4.4 & Later with Bluetooth Low Energy

http://techcrunch.com/2015/01/06/intel-wearables-chip/
http://hlifeinfo.tistory.com/1102
Things that are used around the work

All-in-one PC/mouse

- 1.4Ghz Coretex SoC
- 128GB NAND Memory
- 2 USB Port
- Micro HDMI

http://www.mouse-box.com/
Intel introduces compute stick to insert on monitors

- Intel introduces finger sized compute stick called PC-on-a-stick

- With connection to HDMI of a monitor enables computing devices

- Built-in Atom Quadcore CPU, USB port, Bluetooth, WIFI functions

- RAM 2GB, Built-in Storage 32GB, Storage Extension with microSD

- Ready for sale in a couple of months. $149 for Windows 8.1 version, $89 for Linux version

- Easy to organize desktop environment anywhere with I/O devices, such as monitor, keyboard, mouse

http://techneedle.com/archives/19657
They reported that electric kettle, followed by Chinese electric iron, also had malware to spread SPAM. The newspaper mentioned “spy chip” from 30 pieces of household appliances imported from China. This chip seeks unprotected WIFI network to spread malware and SPAM to the local network with sending out data to the foreign server. It is the same chip that was found in the electric iron. Someone intentionally included hacking functions in these micro appliances. Hotels that basically provide irons and kettles as basic service can be damaged the most. Not only Summits, CEOs but public can be the victim when using hotels.

- The Electronics Times 2013.10.31
Industrial Electronic Things

Any devices providing electricity can be potential threat of data leakage.
Security of Things

Linux based aircraft
Wireless Aerial Surveillance

The drone would fly around sniffing out WiFi networks and has hardware inside that allows it to spoof a cell phone tower

Issues by IoT: Violation of personal information and privacy

The Joy of Tech™

WHAT IT’S LIKE WHEN YOU READ A NEWSPAPER...

by Nitrozac & Snaggy

WHAT IT’S LIKE WHEN YOU READ NEWS ONLINE...

AD NETWORK GUY
THE NSA
ANOTHER AD NETWORK GUY
AMAZON
ANOTHER NSA GUY
FACEBOOK

© 2014 Geek Culture
joyoftech.com

http://recode.net/2014/11/03/reading-a-newspaper-vs-reading-news-on-the-web-comic/
What changes does IoT bring to public safety

Biggest issues from IoT:

Violation of personal information and privacy
Amazing Mind Reader
THANK YOU!