Internet of Things Security: Challenges and Issues

RAJ JAIN
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Keynote at 9th Central Area Networking and Security Workshop (CANSec), University of Central Missouri, Warrensburg, MO, April 16, 2016

These slides are available on-line at:
http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm
Overview

1. IoT Hype
2. A Layered Model of IoT and Smart Cities
3. Areas of Research for IoT
4. IoT Security
5. Software Defined Secure Multi-Cloud Application Management for IoT
## Trend 1: Smart Everything

<table>
<thead>
<tr>
<th>Smart Watch</th>
<th>Smart TV</th>
<th>Smart Car</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Health</td>
<td>Smart Home</td>
<td>Smart Kegs</td>
</tr>
<tr>
<td>Smart Space</td>
<td>Smart Industries</td>
<td>Smart Cities</td>
</tr>
</tbody>
</table>

Washington University in St. Louis  
http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm  
©2016 Raj Jain
What’s Smart?

- Old: Smart = Can think → Computation
  = Can Recall → Storage
- Now: Smart = Can find quickly, Can Delegate
  → Communicate = Networking
- Smart Grid, Smart Meters, Smart Cars, Smart homes, Smart Cities, Smart Factories, Smart Smoke Detectors, …
Gartner Hype Cycle 2015


VC investment
Acquisitions
By large corporations
Mass Production

Washington University in St. Louis
http://www.cse.wustl.edu/~jain/talks/iots_uem.htm
©2016 Raj Jain
Gartner’s Hype Cycle For IoT 2015

Washington University in St. Louis  
http://www.cse.wustl.edu/~jain/talks/iots_uem.htm
Google Trends

- Around for 10 years
- IERC-European Research Cluster on the Internet of Things funded under 7th Framework in 2009
  ⇒ “Internet of European Things”
- US interest started in 2009 w $3.4B funding for **smart grid** in American Recovery and Reinvestment Act of 2009

Obama invests $3.4B in Smart Grid
Oct 27, 2009

Google buys Nest for $3.2B
Jan 13, 2014

---

Washington University in St. Louis  http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm  ©2016 Raj Jain
Computing vs. IoT

- 21 Billion devices by 2020

Ref: M. Moran, "Why the Internet of Things Will Dwarf Social (Big Data)," Gartner Report #G00289622, February 2016
Washington University in St. Louis [http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm](http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm) ©2016 Raj Jain
IoT Business Opportunity

- $1.7 Trillion by 2020 - IDC
- $7.1 Trillion - Gartner
- $10-15 Trillion just for Industrial Internet – GE
- $19 Trillion – Internet of Everything - Cisco


Washington University in St. Louis
A 7-Layer Model of IoT

**Services**
- Energy, Entertainment, Health, Education, Transportation, …

**Apps and SW**
- SDN, SOA, Collaboration, Apps, **Clouds**

**Analytics**
- Machine learning, predictive analytics, Data mining, …

**Integration**
- Sensor data, Economic, Population, GIS, …

**Interconnection**
- DECT/ULE, WiFi, Bluetooth, ZigBee, NFC, …

**Acquisition**
- Sensors, Cameras, GPS, Meters, Smart phones, …

**Market**
- Smart Grid, Connected home, Smart Health, Smart Cities, …
# A 7-Layer Model of Smart Cities

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>Roads, Trains, Buses, Buildings, Parks, …</td>
</tr>
<tr>
<td>Acquisition</td>
<td>Sensors, Cameras, GPS, Meters, Smart phones, …</td>
</tr>
<tr>
<td>Interconnection</td>
<td>DECT/ULE, WiFi, Bluetooth, ZigBee, NFC, …</td>
</tr>
<tr>
<td>Integration</td>
<td>Sensor data, Economic, Population, GIS, …</td>
</tr>
<tr>
<td>Analytics</td>
<td>Machine learning, predictive analytics, Data mining, …</td>
</tr>
<tr>
<td>Apps and SW</td>
<td>SDN, SOA, Collaboration, Apps, Clouds</td>
</tr>
<tr>
<td>Services</td>
<td>Energy, Entertainment, Health, Education, Transportation, water, …</td>
</tr>
</tbody>
</table>

**ICT**

**Management**

**Security**

---

Washington University in St. Louis  
[http://www.cse.wustl.edu/~jain/talks/iots_uem.htm](http://www.cse.wustl.edu/~jain/talks/iots_uem.htm)

©2016 Raj Jain
IoT is a Data ($) Mine

I THINK MY NEST SMOKE ALARM IS GOING OFF. GOOGLE ADWORDS JUST PITCHED ME A FIRE EXTINGUISHER AND AN OFFER FOR TEMPORARY HOUSING.
Areas of Research for IoT

1. **PHY**: Smart devices, sensors giving real-time information, *Energy Harvesting*
2. **Datalink**: WiFi, Bluetooth, ZigBee, 802.11ah, …
   Broadband: DSL, FTTH, Wi-Fi, 5G, …
3. **Routing**: *Multiple interfaces*, Mesh networking, …
4. **Analytics**: Big-data, data mining, Machine learning, Predictive analytics, …
5. **Apps & SW**: SDN, SOA, Cloud computing, Web-based collaboration, Social networking, HCI, Event stream processing, …
6. **Applications**: Remote health, On-line education, on-line laboratories, …
7. **Security**: Privacy, Trust, Identity, Anonymity, …
Top Inhibitors to the Adoption of the IoT


http://www.cse.wustl.edu/~jain/talks/iotics_ucm.htm
IoT Security: Popular Approach

I have finished studying other companies’ IoT Security strategies. “Close your eyes and hope for the best!” seems to be the most popular.

Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/iots_uem.htm
Current IoT Security

- **HP Study**
  - 80% had privacy concerns
  - 70% lacked encryption
  - 60% had insecure updates

- **Symantec Study:**
  - 1/5th of Apps did not use SSL (Secure transfers)
  - None of the devices provided mutual (gateway) authentication
  - No lock-out/delaying measures against repeated attacks
  - Common web application vulnerabilities
  - Firmware upgrades were not encrypted

Ref: [http://fortifyprotect.com/HP_IoT_Research_Study.pdf](http://fortifyprotect.com/HP_IoT_Research_Study.pdf)
Internet of Harmful Things

Imagine, as researchers did recently at Black Hat, someone hacking your connected toilet, making it flush incessantly and closing the lid repeatedly and unexpectedly.


Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm
Security ≠ AES-128

- CIA = Confidentiality, Integrity, Availability = Encryption + Message Authentication Code + Denial of Service Prevention
- Use of AES-128 does not guarantee security.
- Insecurity:
  - How strong is the key?
  - Where the key is stored?
  - Bugs in system code
  - Backdoors
DEFCON 2015 (Cont)

- Hacking a Linux rifle
- Hacking smart safes
- Wirelessly steal cars
- Hack a Tesla
- Hack ZigBee
- Hacking IoT baby monitors
- Hacking FitBit Aria
- Cracking crypto currency
- Hack out of home detention
- Insteon’s false security
- Hacking RFID, NFC
- DARPA Cyber Grand Challenge $2M

Ref: https://www.ethicalhacker.net/features/opinions/first-timers-experience-black-hat-defcon
http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm
Door Locks Insecurity

- **Onity Door Locks:**
  - Used on hotel doors with magnetic strips
  - Information is encrypted using a hotel-specific secret key
  - **Programming port** on the bottom
  - Security Key can be read through programming port
  - Firmware update not possible ⇒ Replace hardware

- **Sigma Design’s Z-Wave Door Locks:**
  - Z-Force tool can monitor traffic and have the lock accept an arbitrary encryption key

- **Kwikset Kevo Door Locks:**
  - **Password** can be reset by email
  - Hijacked email addresses and phishing attack

Washington University in St. Louis  [http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm](http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm) ©2016 Raj Jain
Attack Surface

1. IoT Devices
2. IoT wireless access technology: DECT, WiFi, Z-wave, ...
3. IoT Gateway: Smart Phone
4. Home LAN: WiFi, Ethernet, Powerline, ...
5. IP Network: DNS, Routers, ...
6. Higher-layer Protocols
7. Cloud
9. Life Cycle Management: Booting, Pairing, Updating, ...

Things  Access  Gateway  WAN  Cloud  Users

Washington University in St. Louis  http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm  ©2016 Raj Jain
# Recent Protocols for IoT

<table>
<thead>
<tr>
<th>Session</th>
<th>Network</th>
<th>Datalink</th>
<th>Security</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQTT, SMQTT, CoRE, DDS, AMQP, XMPP, CoAP, IEC,…</td>
<td>Encapsulation  6LowPAN, 6TiSCH, 6Lo, Thread…</td>
<td>WiFi, 802.11ah, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ISA100.11a, DigiMesh, WiMAX,…</td>
<td>IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice,…</td>
<td>IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856</td>
</tr>
</tbody>
</table>
To serve world-wide users, latency was critical and so the data was replicated and brought to edge.
Trend: Computation in the Edge

- To service mobile users/IoT, the computation needs to come to edge ⇒ Micro-cloud on the tower ⇒ Mobile-Edge Computing
Trend: Multi-Cloud

- Larger and infrequent jobs serviced by local and regional clouds ⇒ Fog Computing
Past: Software Defined Networking

- Network can be managed w/o worrying about individual device hardware

Network Manager

Users

Network Controller

Network

http://www.cse.wustl.edu/~jain/talks/iots_uclm.htm

©2016 Raj Jain
Trend: Software Defined Multi-Cloud Application Delivery

- Cloud MOM (message oriented middleware)
Mobile Healthcare Use Case

- Home sensors for patient monitoring
- Multi-Cloud Mobile Application Deployment and Optimization Platform
- Hospital Cloud
- SDN Controller
- Insurance Co Cloud
- 5G Carrier
- Mobile Doctor
- Medical Application Service Provider

Body Area Network for mobile patient

Washington University in St. Louis
http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm

©2016 Raj Jain
Summary

1. IoT research areas are easy via the 7-layer model
2. IoT has brought in research issues in every layer: Sensors, datalink, routing, applications, analytics.
3. Security and privacy are most important issues
4. Computation is moving to the Edge ⇒ Fog Computing ⇒ Multi-Cloud/Inter-Cloud
5. Our MCAD abstracts/virtualizes the cloud interfaces and allows automated management of security and other policies of multi-cloud applications
Recent Talks on IoT

Recent Papers on Multi-Cloud


Acronyms

- **6TiSCH** IPv6 over Time Slotted Channel Hopping Mode of IEEE 802.15.4e
- **ADCOM** Advanced Computing and Communications
- **AES-128** Advanced Encryption Standard
- **AMQP** Advanced Message Queuing Protocol
- **ANT** A proprietary open access multicast wireless sensor network
- **ANT+** Interoperability Function added to ANT
- **CANSec** Central Area Networking and Security
- **CARP** Channel-Aware Routing Protocol
- **CIA** Confidentiality, Integrity, Availability
- **CoAP** Constrained Application Protocol
- **CoRE** Constrained RESTful Environment
- **CORPL** Cognitive RPL
- **CS** Computer Society
- **DARPA** Defense Advance Research Project Agency
- **DASH-7** Named after last two characters in ISO 18000-7
- **DDS** Data Distribution Service
Acronyms (Cont)

- DECT: Digital Enhanced Cordless Telephone
- DECT/ULE: Digital Enhanced Cordless Telephone with Ultra Low Energy
- DEFCON: d-e-f conference (named after alphabets d, e, f)
- DNS: Domain Name System
- DSL: Digital Subscriber Line
- DTLS: Datagram Transport Layer Security
- ECC: Error Correcting Code
- EDSA: Embedded Device Security Assurance
- FTTH: Fiber to the home
- GB: Gigabyte
- GE: General Electric
- GIS: Geographical Information Systems
- GP: Green PHY
- GPS: Global Positioning System
- HCI: Human Computer Interface
- HMAC: Keyed-Hash Message Authentication Code
Acronyms (Cont)

- HP: Hewlett Packard
- HTTP: Hyper Text Transfer Protocol
- ICS: Industrial Control Systems
- ICT: Information and Communications Technology
- IDC: International Data Corporation
- IDs: Identifiers
- IEC: International Engineering Council
- IEEE: Institution of Electrical and Electronic Engineers
- IETF: Internet Engineering Task Force
- IoT: Internet of Things
- IP: Internet Protocol
- IRTF: Internet Research Task Force
- ISA: International Society of Automation
- ITU: International Telecommunications Union
- LAN: Local Area Network
- LoRaWAN: Long Range Wide Area Network
Acronyms (Cont)

- LowPAN: Low Power Personal Area Network
- LTE: Long-Term Evolution
- MCAD: Multi-Cloud Application Delivery
- MHz: Mega Hertz
- MOM: Message Oriented Middleware
- MQTT: Message Queue Telemetry Transport
- NFC: Near Field Communication
- NSF: National Science Foundation
- OAuth: Open Protocol of Secure Authorization
- OpenADN: Open Application Delivery Networking
- PHY: Physical Layer
- PKI: Public Key Infrastructure
- RFC: Request for Comment
- RFID: Radio Frequency Identifier
- RPL: Routing Protocol for Low Power and Lossy Networks
- RSA: Rivest, Shamir, and Adleman
## Acronyms (Cont)

- SASL  Simple Authentication and Security Layer
- SDLA  Requirements for Security Development Lifecycle Assurance
- SDN   Software Defined Networking
- SDS   Software Defined Systems
- SMACK Simple Mandatory Access Control Kernel for Linux
- SOA   Service Oriented Architecture
- SSA   Software Security Assurance
- SSL   Secure Session Layer
- SW    Software
- TCG   Trusted Computing Group
- TCP   Transmission Control Protocol
- TLS   Transport Level Security
- TNC   Trusted Network Connect
- TPM   Trusted Platform Module
- TV    Television
- UDP   User Datagram Protocol
Acronyms (Cont)

- ULE  Ultra Low Energy
- US   United States
- VC   Virtual Circuit
- VM   Virtual Machine
- WAN  Wide Area Network
- WiFi Wireless Fidelity
- WiMAX Worldwide Interoperability of Microwave Access
- WirelessHART Wireless Highway Addressable Remote Transducer Protocol