Systems and Mobile Research Lab,
Department of Computer Science and Engineering

Presenter:
Sandip Chakraborty
sandipc@cse.iitkgp.ac.in
Hacker 'made plane climb' after taking control through in-flight entertainment system

FBI affidavit says hacker removed from United Airlines flight last month managed to change flight direction from his seat.

Hackers use old SSH vulnerability to attack Internet of Things devices

By Sead Fadilpašić | Published 22 hours ago

Computing

NSA Hacking Chief: Internet of Things Security Keeps Me Up at Night

The leader of the National Security Agency's hackers says that putting industrial control systems online has made America less secure.
IoT SECURITY: WHERE ARE WE TODAY?

90% of the devices collected at least one piece of personal information via the device, the cloud or its mobile application.

70% of the devices used unencrypted network services.

70% of the devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

80% of the devices along with their cloud and mobile application failed to support passwords of a sufficient complexity and length.

Our focus of this talk would be on IoT network security!
NATURE OF IoT COMMUNICATION NETWORKS – DATA PATH

Source: http://wwwrtcsmagazine.com/articles/view/105734
IoT NETWORKS – SENSING + PROCESSING + COMMUNICATION

Source: https://www.micrium.com/iot/devices/
SECURITY LAYER IN THE IoT PROTOCOL STACK

Source: http://www.computaholics.in/2016/01/internet-of-things.html
• Primarily wireless communication, however wired communication are also widely used in automobile/industrial IoT applications

• Wired communication for IoT
  • Vehicle bus, Train bus – for connecting IoT sensors at vehicles, trains
  • Communication technologies – CAN, FlexRay, Ethernet – connect the IoT sensors with vehicle/train control box

• Wireless communication for IoT
  • IEEE 802.11 or Wi-Fi
    • Low power Wi-Fi devices are used for sensor communication
    • Primarily used at the IoT gateway
    • Can be used for data offloading, Ex. use your smart-phone as personal IoT hub, tether the cellular connection via Wi-Fi tethering
COMMUNICATION TECHNOLOGIES FOR IoT

• Wireless communication for IoT
  • Low Power Solutions
    • Low-power and efficient radios, allowing several years of battery life
  • Energy harvesting as a power source for wireless radios – Ex. EnOcean’s wireless transmitter works in the frequencies of 868 MHz (for Europe) or 315 MHz (for North America) – ranges up to 30 meters inside building and 300 meters in open space
  • Mesh networking – multi-hop communication (Zigbee Alliance and Google-backed Thread group are working on low power mesh networking standard for IoT communication) – Tmesh from Filament
• Wireless communication for IoT
  • IEEE 802.15.4 – low rate wireless personal area networks (LR-WPAN)
    • works in the frequency range 868/915 MHZ, 2.4 GHZ
    • Low power communication protocol

• 6LoWPAN – the upcoming standard for IoT communication
  • IPv6 over Low power Wireless Personal Area Networks – adopted by ARM and Cisco
  • Provides encapsulation and header compression mechanisms that allow for briefer transmission times
  • Common topologies include – star, mesh, and combinations of star and mesh
  • The Phy and MAC layers conform to IEEE 802.15.4-2003 standard
HOW 6LoWPAN WORKS IN A IoT NETWORK?

Source: http://www.slideshare.net/waltercolitti/iotgent-presentation-walter
IoT NETWORK SECURITY: ISSUES AND CHALLENGES

- Ubiquitous Network Encryption
- Identity and Trust
- Access Policies with Real Time Enforcements
- Dynamic Traffic Shaping and Network Segmentation
- Network Intelligence and Data Sharing
- Automated Remediation
Security professionals will have to provide network access to a large pool of unmanaged heterogeneous devices.

IoT and mobile devices (BYOD) are different use cases -
  - BYOD carries some additional requirements for user/device authentication, data/device security, and network access controls, but is simply a mobile adaptation of well-understood PC security best practices.
  - Alternatively, IoT devices will come in all shapes and sizes, reside outside the network, and readily exchange data with corporate applications.

Given the vast differences with IoT, there is a need for strong, non-reputable device identification –
  - Each device will have to announce itself to the network with some type of authentication that can be verified by some type of authority to establish trust.
  - Enterprises will want to know details about the device type, location, activity, etc.
  - This information will have to be captured, analysed, stored, and shared among auditors, security analysts, and IoT system experts.
• Traffic is mostly tunnelled through HTTPS – how will you identify the application for traffic shaping and network segmentation?

• Understand traffic signatures for IoT application classification
CAN WE APPLY MACHINE LEARNING MECHANISMS?

Learn HTTP user agent fields for different devices and different apps – Does there exist a pattern?

Can we use a set of fields from HTTP header as a device/application fingerprint?
LOOK AT THE TRAFFIC PATTERNS FROM VARIOUS APPS

Buffered video – Bytes received per second

Interactive video – Bytes received per second

Packet size distribution for YouTube

Packet size distribution for Skype

THEY ARE LIKELY TO DIFFER

LEARN THE TRAFFIC PATTERN FOR DIFFERENT IoT APPS
We have to deal “BIG DATA” but in a distributed environment ...
<table>
<thead>
<tr>
<th>SECURITY POLICY CONTROL</th>
<th>DISTRIBUTED</th>
<th>CENTRALIZED</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTRIBUTED</td>
<td>The conventional approach – easy to implement but difficult to maintain</td>
<td></td>
</tr>
<tr>
<td>CENTRALIZED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Indian Institute of Technology Kharagpur**

- **Distributed** Network Policy, **Distributed** Security Policy
  - Implement the policies over individual routers and gateways
  - Ex. Configure IP filters over individual devices
WHAT CAN HAPPEN AS A RESULT OF POLICY INCONSISTANCY?
WHAT CAN HAPPEN AS A RESULT OF POLICY INCONSISTANCY?

Data from R4 and R6 should not go outside the subnets.

- What would be your access control rules?

I don’t want static IPs in my network.
WHAT CAN HAPPEN AS A RESULT OF POLICY INCONSISTANCY?

Rules:
A: INOUT R4 DROP
B: INOUT R6 DROP
A,B: ALLOW ALL
WHAT CAN HAPPEN AS A RESULT OF POLICY INCONSISTENCY?

Rules:
A: INOUT R4 DROP
B: INOUT R6 DROP
A,B: ALLOW ALL
WHAT CAN HAPPEN AS A RESULT OF POLICY INCONSISTANCY?

NETWORK PARTITIONING AND ACCESS CONTROL IS GOING TO BE EXTREMELY DIFFICULT
## SECURITY IN IoT NETWORK – DISTRIBUTED OR CENTRALIZED?

<table>
<thead>
<tr>
<th>SECURITY POLICY CONTROL</th>
<th>DISTRIBUTED</th>
<th>CENTRALIZED</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTRIBUTED</td>
<td>The conventional approach – easy to implement but difficult to maintain</td>
<td>Can be implemented over the network under common administration – NOT scalable, may be vulnerable for IoT</td>
</tr>
<tr>
<td>CENTRALIZED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Distributed** Network Policy, **Centralized** Security Policy

- Implement the network policies over individual devices, but configure the security policy at the IoT gateway.

- What happens if an internal IoT device gets compromised?
  - May not be a big problem for normal network, but can make the whole IoT network vulnerable.
## SECURITY IN IoT NETWORK – DISTRIBUTED OR CENTRALIZED?

<table>
<thead>
<tr>
<th>NETWORK POLICY CONTROL</th>
<th>SECURITY POLICY CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DISTRIBUTED</td>
</tr>
<tr>
<td>DISTRIBUTED</td>
<td>The conventional approach – easy to implement but difficult to maintain</td>
</tr>
<tr>
<td>CENTRALIZED</td>
<td>Desirable – but how to implement?</td>
</tr>
</tbody>
</table>

- Implement the network policies over individual devices, but configure the security policy at the IoT gateway

- What happens if an internal IoT device get compromised?
  - May not be a big problem for normal network, but can make the whole IoT network vulnerable
**SECURITY IN IoT NETWORK – DISTRIBUTED OR CENTRALIZED?**

<table>
<thead>
<tr>
<th>SECURITY POLICY CONTROL</th>
<th>DISTRIBUTED</th>
<th>CENTRALIZED</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTRIBUTED</td>
<td>The conventional approach – easy to implement but difficult to maintain</td>
<td>Can be implemented over the network under common administration – NOT scalable, may be vulnerable for IoT</td>
</tr>
<tr>
<td>CENTRALIZED</td>
<td>Desirable – but</td>
<td></td>
</tr>
</tbody>
</table>

DISTRIBUTED Network Policy, CENTRALIZED Security Policy

-> Implement the network policies over individual devices, but configure the security policy at the IoT gateway

What happens if an internal IoT device gets compromised?

- May not be a big problem for normal networks, but can make the whole IoT network vulnerable

Go for a SOFTWARE DEFINED APPROACH

Indian Institute of Technology Kharagpur
SOFTWARE DEFINED NETWORKING – NEW PARADIGM FOR NETWORK POLICY CONTROL

APPLICATION LAYER
- Business Applications

CONTROL LAYER
- SDN Control Software
- Network Services
- Control Data Plane interface (e.g., OpenFlow)

INFRASTRUCTURE LAYER
- Network Device
- Network Device
- Network Device
- Network Device
SDN OVER IoT – CONTROL IoT NETWORK POLICY
IoTSec: A SECURITY FRAMEWORK FOR IoT NETWORK USING SDN


• Cross-device dependencies: Implicit coupling of devices using IF-This-Then-That (IFTTT)
  • Example: Temperature sensor can control windows when it senses air-conditioner not working.
• Many vendors dealing with different parts of IoT ecosystem
• IoT devices do not run full fledged OS; resource constrained
  • Most IoT devices require <= 2MB RAM
  • Commontouch Antivirus for embedded systems requires 128 MB RAM
IoTSec: A SECURITY FRAMEWORK FOR IoT NETWORK USING SDN

- Cross-device dependencies: Implicit coupling of devices using IF-This-Then-That (IFTTT)
  - Example: Temperature sensor can control windows when it senses air-conditioner not working.
- Many vendors dealing with different parts of IoT ecosystem
- IoT devices do not run full fledged OS; resource constrained
  - Most IoT devices require $\leq 2$MB RAM
  - Commontouch Antivirus for embedded systems requires 128 MB RAM
IoTSec: A SECURITY FRAMEWORK FOR IoT NETWORK USING SDN

- Customized µmboxes (micro network security functions) – Security gateway for each IoT device

- Control Platform
  - Monitors context of different devices and applications
  - Generates global view for cross platform dependencies
  - Instantiates µmboxes based on this view
  - Configures forwarding mechanisms to forward packets to these µmboxes
WE NEED TO HANDLE A NETWORK WITH LARGE VOLUME OF DEVICES

- HOW CAN WE DESIGN A ROBUST AND SCALABLE NETWORK PARTITIONING/ACCESS CONTROL MECHANISM?

- HOW CAN WE ENFORCE GLOBAL POLICY UPDATES?

- HOW CAN WE EMBED SOFTWARE SECURITY CONTROL OVER RESOURCE-CONSTRAINT DEVICES?
Systems and Mobile Research Lab,
Department of Computer Science and Engineering, IIT Kharagpur
INDIA 721302
http://cse.iitkgp.ac.in/~sandipc/