Malware Infection to Vehicle ECUs follows the infection to IoT Devices

Koji Nakao

Distinguished Researcher,

Network Security Research Institute, NICT &

Visiting Professor, Yokohama National University

Darknet Monitoring

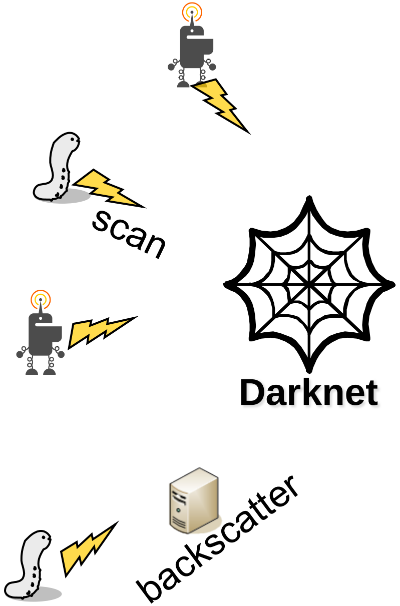
- **Darknet**: Unused IP addresses space

- **In theory**: any packets should **NOT** arrive at the darknet because they are not connected to any hosts.

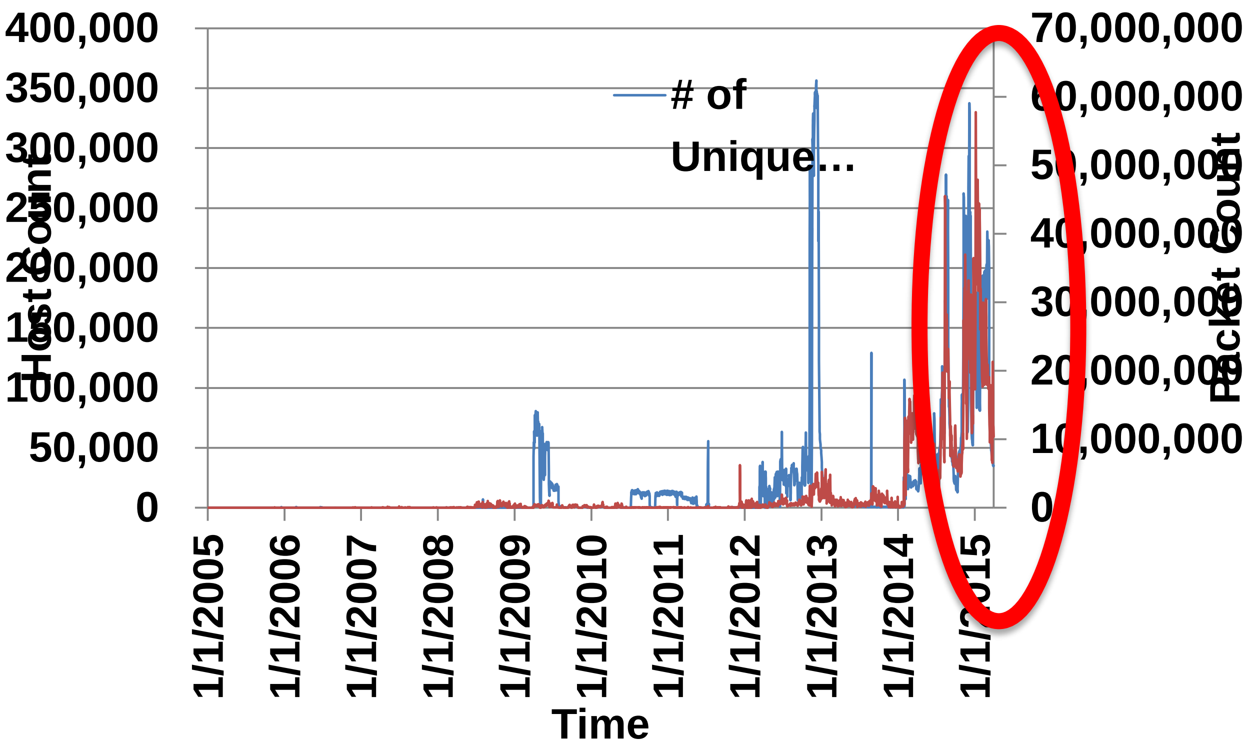
- **In fact**: quite a few packets **DO** arrive!

- Packets arriving at the darknet are…
  - Scans by malwares
  - Backscatter (reflection of DDoS attack)
  - Miss configurations etc.

- Darknet traffic reflects **global trend in malicious activities** on the Internet.



Telnet (23) attacks on Darknet have rocketed



Challenges

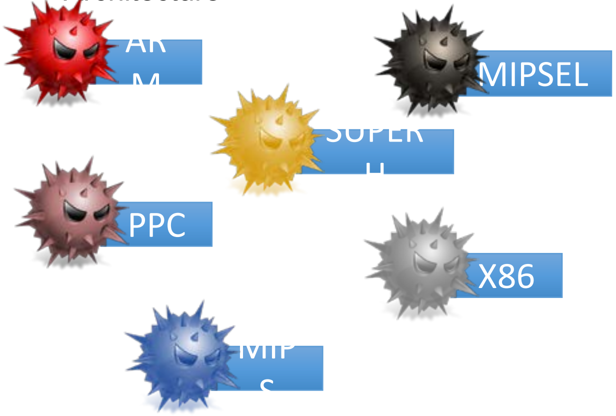
Honeypot

IoT devices listening on Telnet

- Emulating diverse IoT devices
- Handling to capture malware of different CPU architectures

Sandbox: IoTBOX

IoT malware of different CPU Architecture



- Handle to run malware of different CPU architectures

Attacking hosts are IoT devices (2016, January-June)

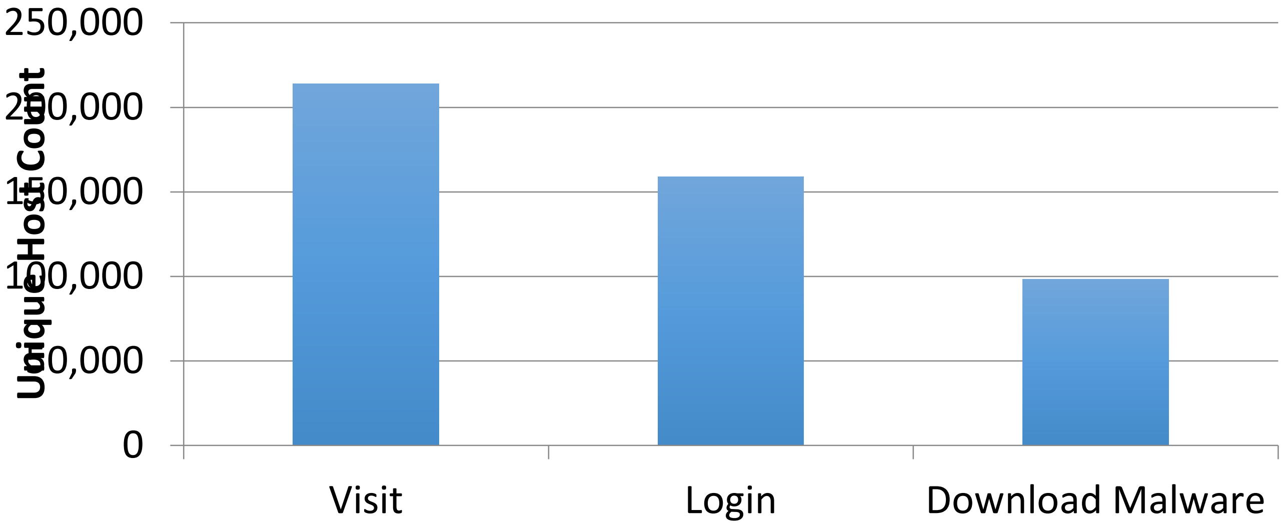
600,000 attacking IPs

500models observed in 6 months

National Institute of
Information and
Communications
Technology

IoTPOT results

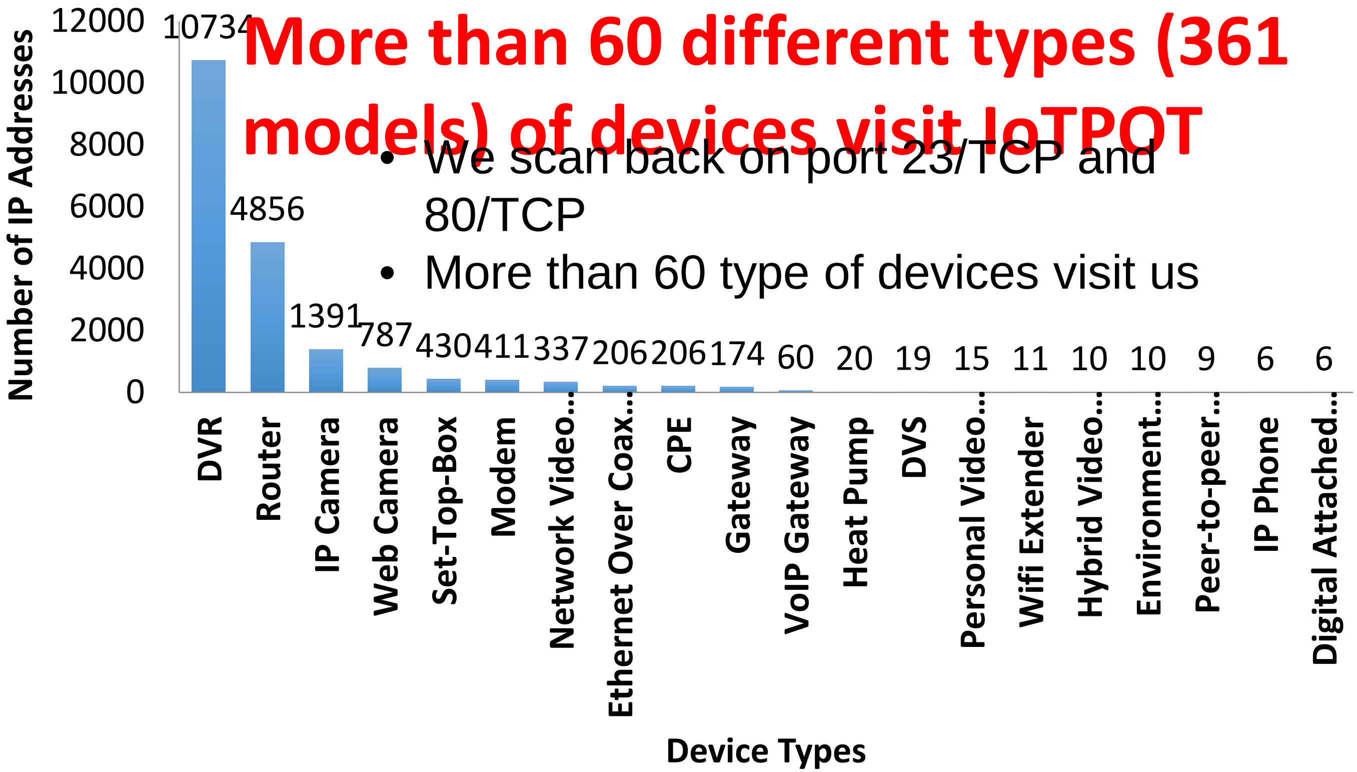
- During 122 days of operations [April 01 to July 31 - 2015]



- **90,394 Malware Download Attempts**
- **Malware of 11 different CPU architectures**
- **93% of downloaded binaries are new to Virus Total (2015/09)**

NICT National Institute of Information and Communications Technology

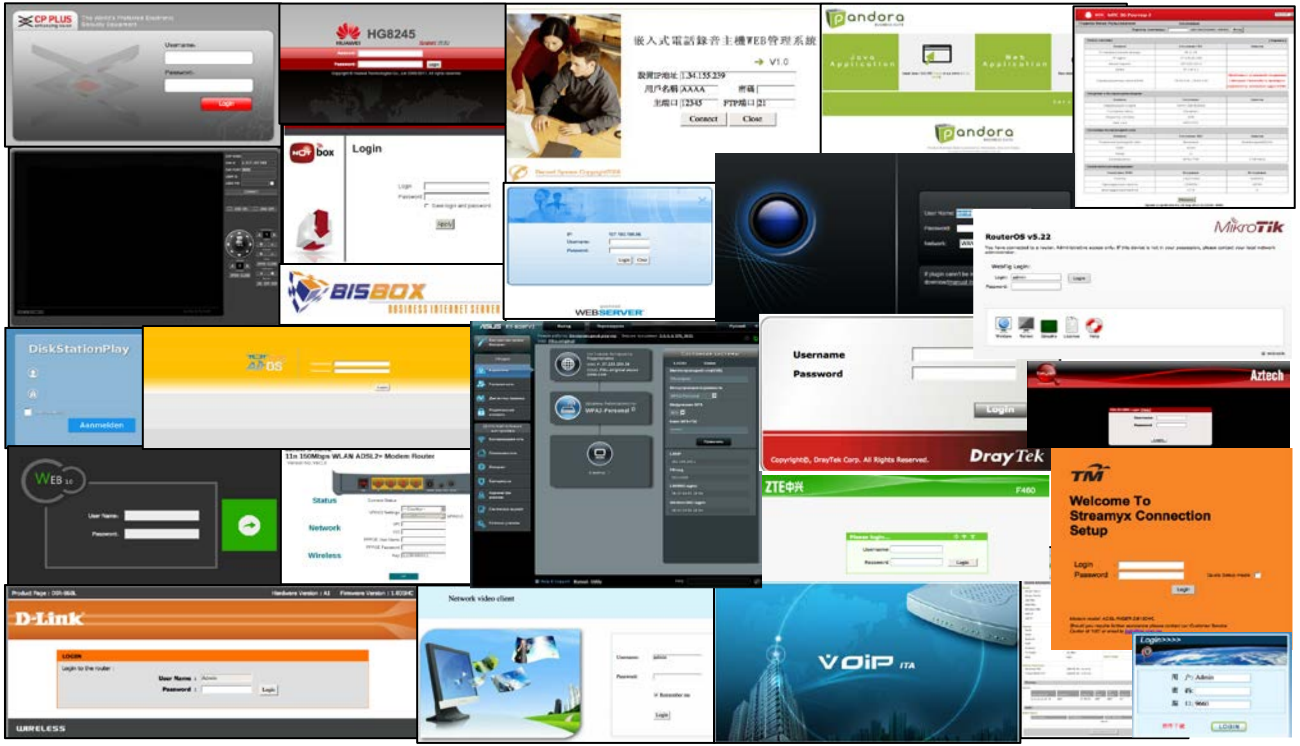
Looking back on devices visiting IoTPOT



More than 60 different types (361 models) of devices visit IoTPOT

- We scan back on port 23/TCP and 80/TCP
- More than 60 type of devices visit us

Web interfaces of devices attacking us

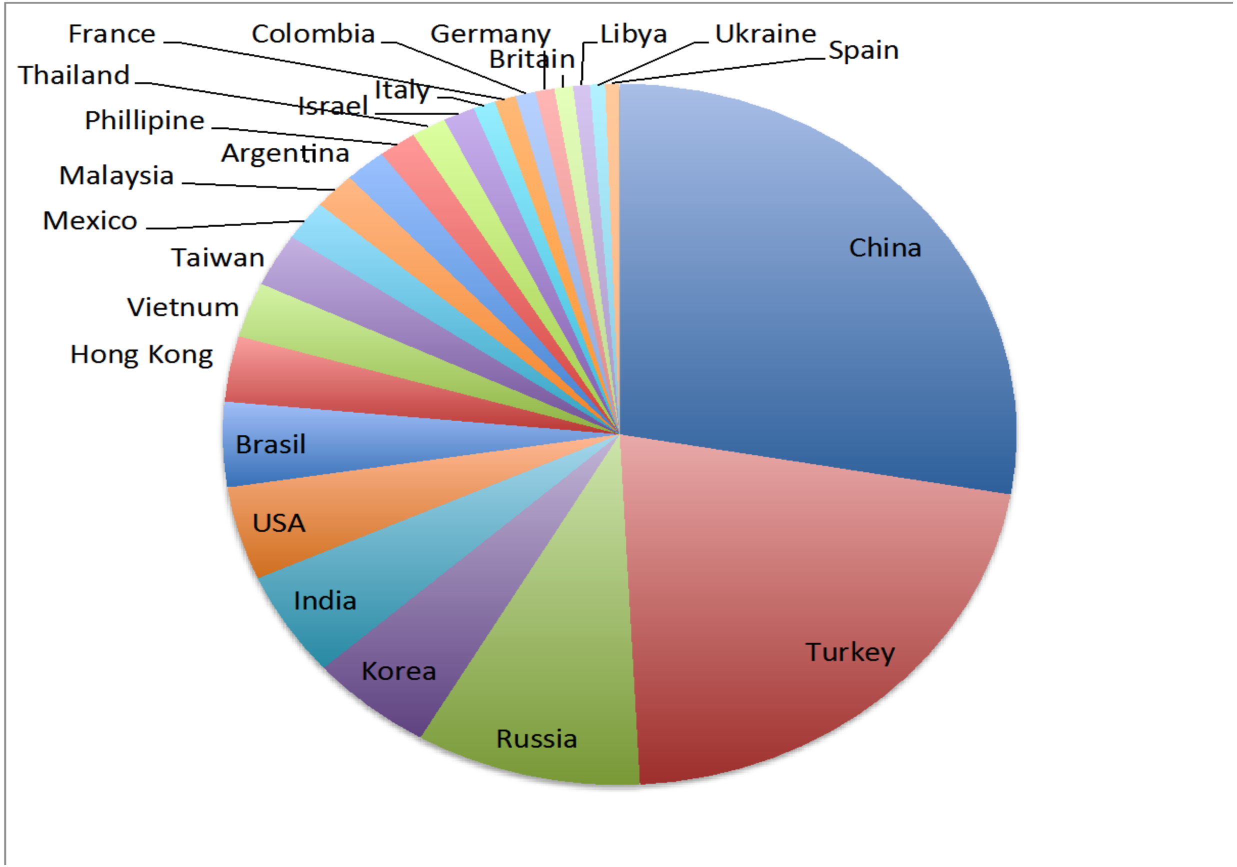


Categorizing IoT device types infected by Malwares

- Surveillance Group
  - IP Camera
  - DVR
- Networking Related Devices
  - Router
  - Gateway
  - Modem
  - Bridge
  - Security Appliance
- Telephone System
  - VoIP Gateway
  - IP Phone
  - GSM Router
  - Analog Phone Adapter
- Infrastructure
  - **Parking Management System**
  - LED display control system

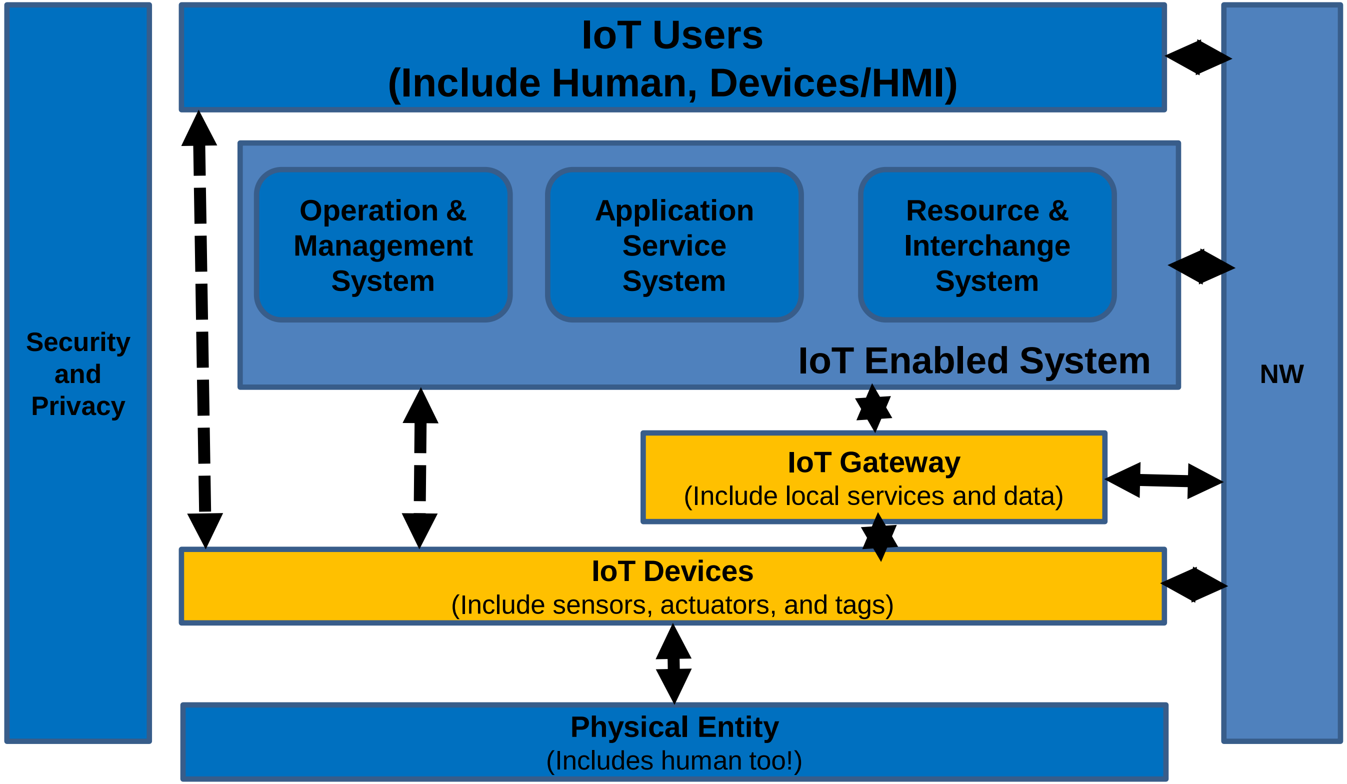
- Industrial Control System
  - Solid State Recorder
  - Internet Communication Module
  - Data Acquisition Server
  - BACnet I/O Module
- Personal
  - Web Camera
  - Personal Video Recorder
  - Home Automation Gateway
- Broadcasting Facility
  - Digital Video Broadcaster
  - Digital Video Scaler
  - Video Encoder/Decoder
  - Set Top Box
- Other
  - Heat Pump
  - Fire Alarm System
  - Disk Recording System
  - Optical Imaging Facility
  - Fingerprint Scanner

AS with more than 1,000 infected IoT Devices



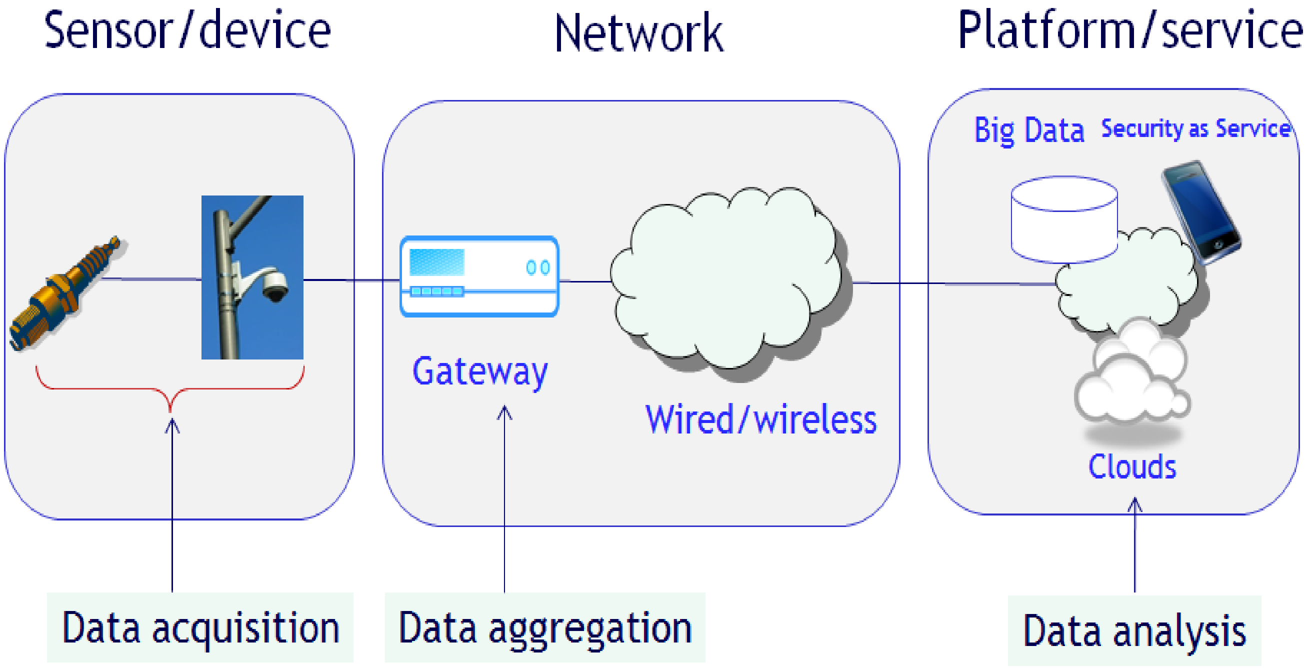
National Institute of Information and Communications Technology

IoT Reference Model(entity based)


Security and Privacy
IoT Users
(Include Human, Devices/HMI)
Operation & Management System
Application Service System
Resource & Interchange System
IoT Enabled System
IoT Gateway
(Include local services and data)
IoT Devices
(Include sensors, actuators, and tags)
Physical Entity
(Includes human too!)
NW

From ISO/IEC JTC1/CS27/WG10 WD 30141

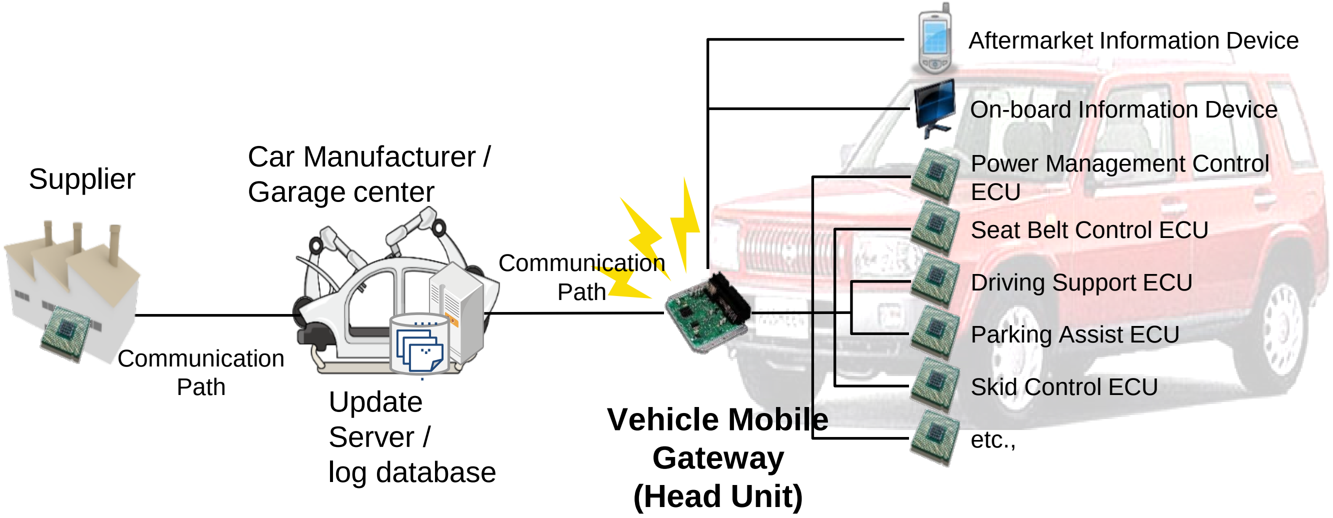
IoT Gateway Based Model in ITU-T



National Institute of Information and Communications Technology

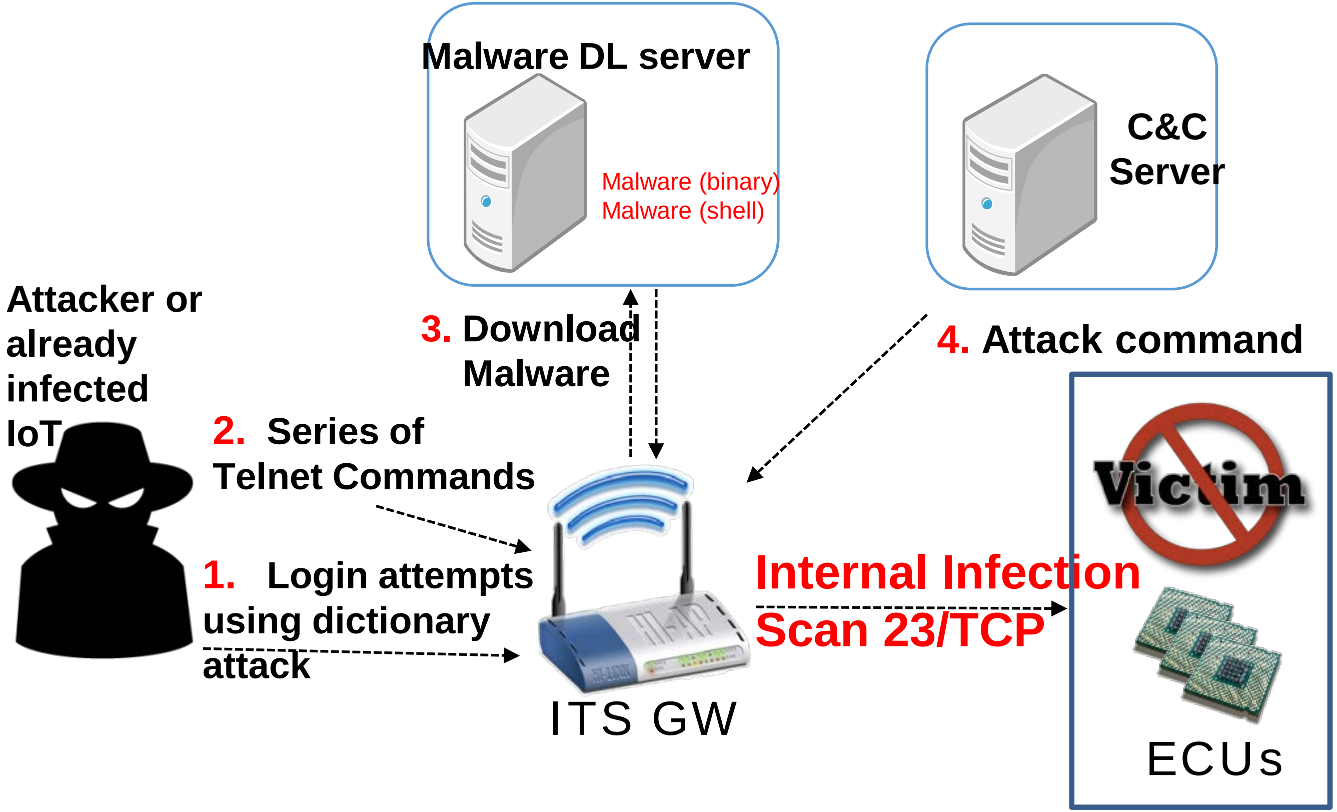
Remote Secure OTA Updates for ITS software/firmware

“ITS : General model of networked vehicle” is introduced in OTA software updates for ITS in ITU-T SG17



Aftermarket Information Device
On-board Information Device
Power Management Control ECU
Seat Belt Control ECU
Driving Support ECU
Parking Assist ECU
Skid Control ECU
etc.,
Supplier
Car Manufacturer / Garage center
Communication Path
Communication Path
Update Server / log database
Vehicle Mobile Gateway (Head Unit)

Telnet based attacks to IoT can be followed...



Conclusion

- **Malware infections of IoT devices is getting worse every year from 2014. Huge DDoS attacks were recently observed by means of infected IoT devices (botnet).**

- **There are several similar features between IoT devices and Device components located in Vehicle. For example, many IoT devices are currently operated under the Gateway (GW) function similarly with ITS environment.**

- **Malware infections to Vehicle ECUs/GW follow the infection to IoT devices.**

- **Technical process, such as "Threats Detection" → "Tracing" → "Notification" → "Response (e.g. removing malware)→ "Patching Vulnerabilities", should be applied to Vehicle systems. Most importantly, appropriate software updating function should be implemented for ECUs and Gateway.**

- **In the process of Detection of Threats/attacks, Honeypot and Anomaly (behavior) Detection Technologies for Vehicle could be worthwhile to consider to implement for secure Vehicle communications.**