IEEE Advancing Technology for Humanity
CYBER SECURITY 2018
Scotland
JUNE 11-12, 2018

infotecs

Lightweight Distributed Attack Detection and Prevention for the Safe Internet of Things

Vladimir Eliseev, JSC InfoTeCS; Olga Eliseeva, MSTU

IoT Security Facts

infotecs

Incidents with IoT:

- More than 73000 Internet-connected cameras with default password (Nov 2014)
- Mirai botnet (Sep 2016 and later)
- Leet botnet (Dec 2016)
- Amnesia botnet (Apr 2017)
- Brickerbot botnet (Apr 2017)
- Millions of CPE with known vulnerabilities (2017-2018)

Botnet features:

- Contains of many typically infected similar devices
- Coexist with normal functions of infected devices (except for Brickerbot)
- Traffic up to **1.1Tbps** and more than **100Mpps**
- Both amplification and flood attack techniques
- Both runtime and persistent presence in infected system
- Cheap Attack-as-a-Service: **$20** per target (**290-300Gbps**)

How to infect a Smart Thing? How to protect it?

Infection/illegal use:

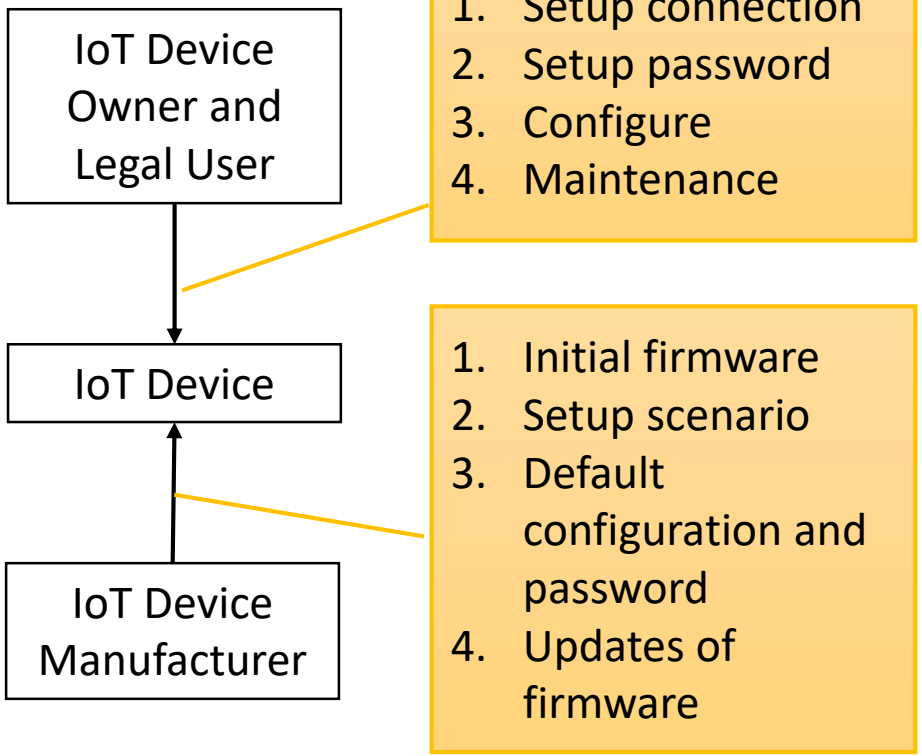
- Weak and default passwords
- Exploits to unpatched firmware
- Well-known weakness of popular protocols (UPnP, SSDP, DNS etc)

Protection by a manufacturer:

- Less bugs and frequent firmware updates
- Force user to be accurate with security settings

Protection by an owner:

- Be professional and care of security



The roots of IoT security problems

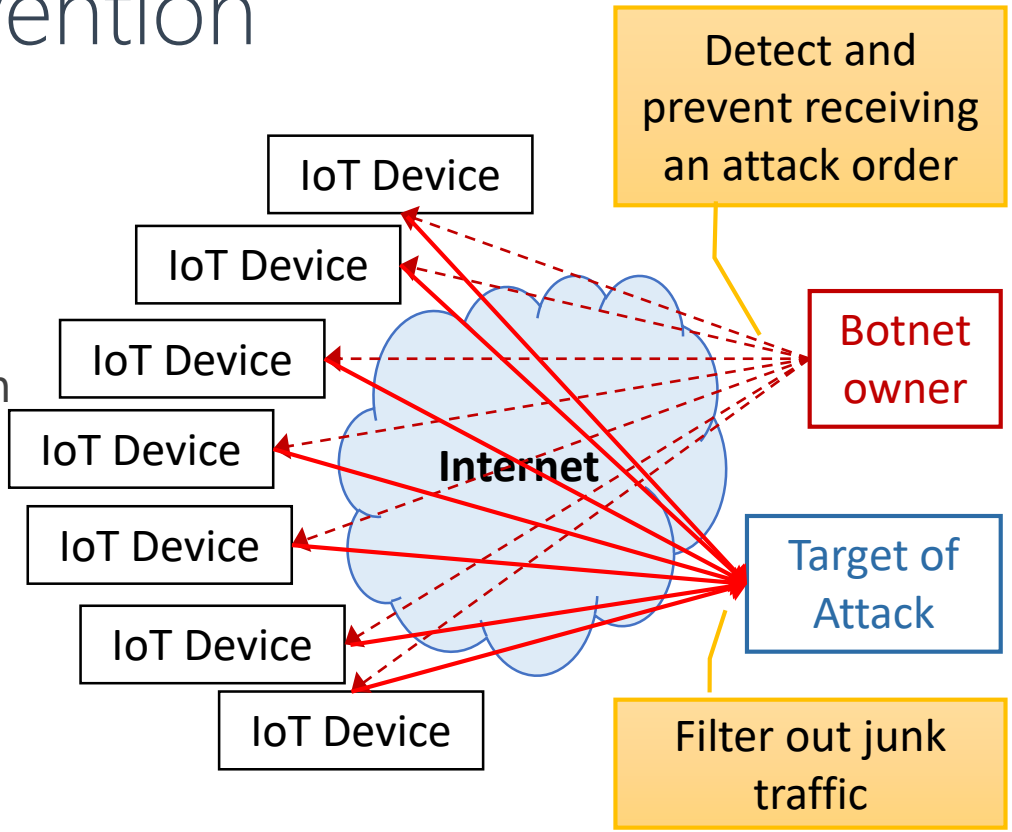
infotecs

Characteristics:

- Target user for IoT devices is a customer without IT knowledge. The more simple the better!
- Firmware security updates are usually not supplied by a vendor after the model got off the market
- Security is not an important function for IoT. All security features are too deep inside and no one knows are they really present or not
- The basis of any IoT device is a typical computer architecture with well known OS, software, bugs and vulnerabilities – familiar for hackers
- There is no capability to install addon protection software like on PC or Mobile

Anatomy of the IoT botnet attack and its prevention

- After infection and loading malicious modules all devices which belong to the botnet are ready to execute attacking actions: flood or amplify
- Attack starts with an order from botnet C&C center, controlled by the botnet owner
- Channel to the C&C center is often encrypted by TLS/SSL
- Numerous IoT devices begin to generate junk traffic, targeted to the victim Internet resource



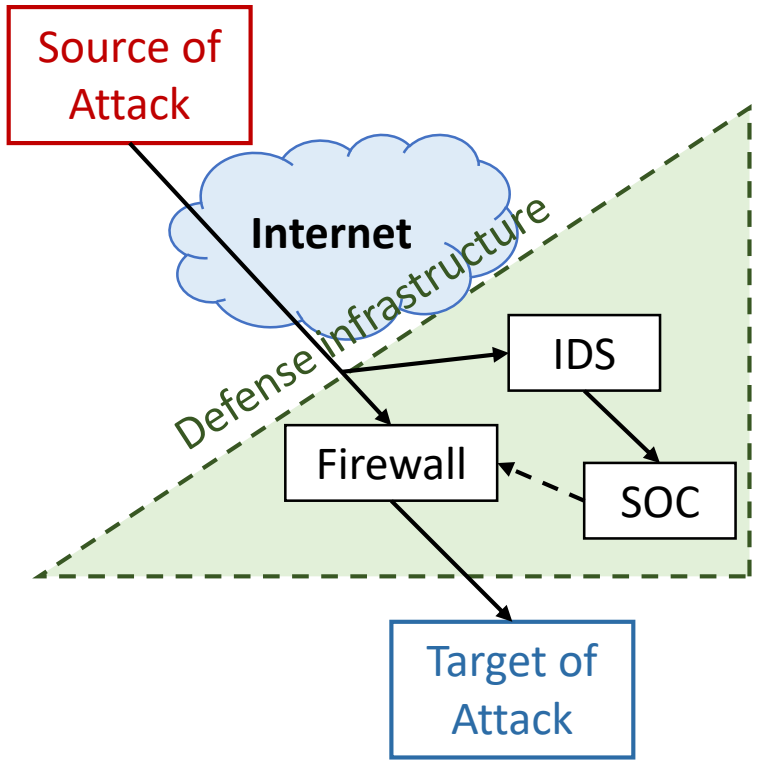
IoT: Intrusion detection and prevention considerations

Why not to use IDPS to protect IoT device from infection?

- No defense infrastructure in place of typical IoT device Internet connection
- Defense infrastructure is too expensive to be used for numerous and cheap IoT devices in every place of their connection

Why not to integrate IDPS into the IoT device?

- High False Positive rate for fully automated IDPS solutions
- Needs frequent update of a large database with attack signatures and prevention rules
- Too modest resources of IoT's computer platform does not allow to run IDPS



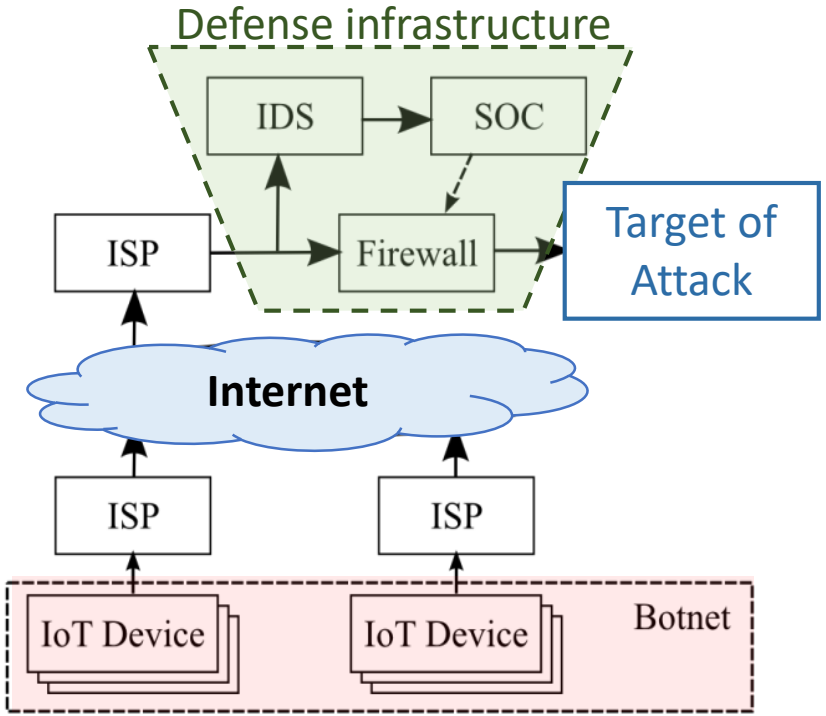
DDoS attack from the IoT botnet

Popular attacks:

- SYN, UDP, ICMP flood
- IP fragmentation
- NTP, DNS amplification
- HTTP flood (application layer attack)

Difficulties to filter junk traffic:

- Botnet member IoT devices are behind DNAT
- Application layer attack looks like normal traffic
- Power of an attack is very high due to large number of IoT devices in a botnet



The background of an idea

Nobody cares about IoT device's security:

- The device works good most of the time even if it belongs to some botnet
- An user is a dummy (to configure and to service the device properly)
- A vendor is greedy (to release security updates and to develop security proven firmware)

Main problems:

- IoT devices become very dangerous when they are captured into a botnet
- To fight with IoT botnet attacks is much more expensive than to conduct them
- Junk traffic from IoT botnet may flood not only customer resources, ISP infrastructure as well

…so, we need to protect the Internet from infected IoT devices

Useful considerations and an idea

IoT device specifics:

- Fixed functionality for the entire lifetime
- Identity of devices of the same model – they differ only by the serial number
- Limited and very specific functionality

Ergo:

It's possible to describe the normal behavior of the IoT device in terms of measured parameters:

- Network ports and protocols
- Network traffic statistics
- Directions of the network traffic
- CPU and memory consumption
- Etc

Malicious use of IoT device in a botnet:

- Different ports and protocols
- Different statistics of network traffic
- Different CPU and memory compuption

Application:

- The normal behavior may be recognized by one-class classifier
- This classifier should be the only for all devices with the same firmware
- The anomaly should mean the malicious use of the IoT device

IoT device can provide information about self anomaly behavior

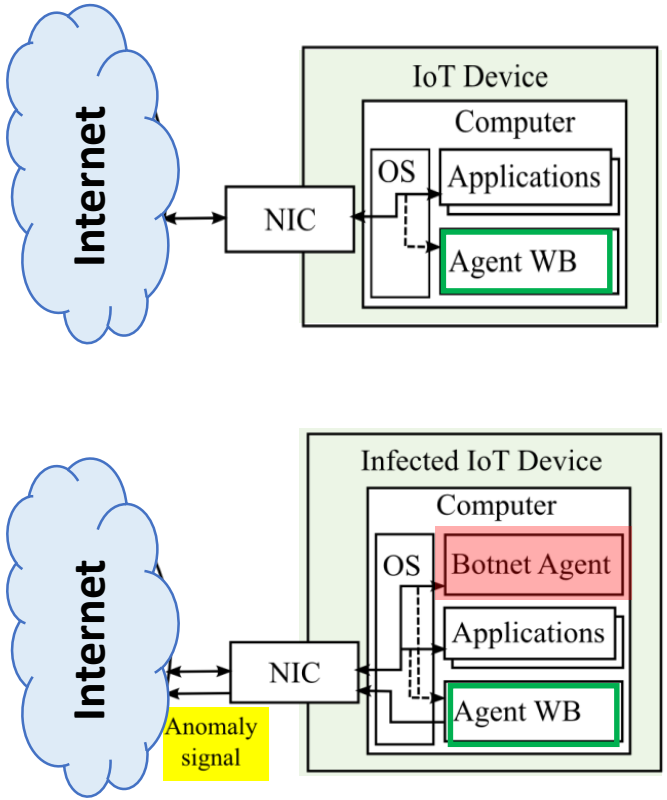
Safe IoT device architecture

The classifier should be developed together with the firmware of the IoT device

Agent-whistleblower (Agent WB) is a program which includes the classifier and the anomaly signal provider

Proposed scenario:

1. Consider the IoT device was attacked successfully (never mind which way of penetration were used – password bruteforce, code injection etc)
2. The IoT device had become infected by some Botnet Agent software, used to make DDoS attack
3. If the IoT device starts to generate some attacking and highly likely unusual traffic, Agent WB will detect the anomaly and sends a corresponding signal



Internet Service Provider (ISP) infrastructure to prevent DDoS attack

Positions:

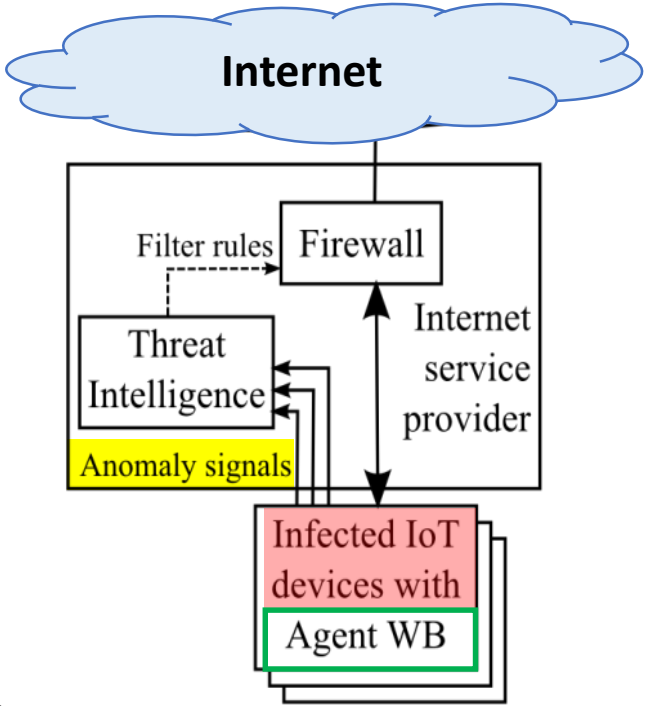
- IoT devices connects to the Internet via some ISP
- ISP can see anomaly signals (if any) from IoT devices
- Threat Intelligence modules of ISP can correlate anomaly signals
- Anomaly signal discloses the address of the IoT device from which it origins

DDoS attack case:

- Many correlated anomaly signals at the same time mean DDoS attack activity
- All source IP-addresses of attacking IoT devices are disclosed by anomaly signals
- Filter rules for the firewall can be generated automatically
- As a result, DDoS attack from this ISP will be prevents near its source

Normal case:

- No anomaly signals then firewall is open for the traffic
- Some anomaly signals appears but they are not highly correlated then firewall is open for the traffic also (False Positive case)



Discussion and conclusion

Regulation:

- IoT device vendors should be motivated to include Agent WB in their products
- ISP should have infrastructure to understand anomaly signals of any IoT device of any vendor
- An international standardization of Agent WB anomaly signal protocol should help
- National interests are taken into account because anomaly signals are processed in national borders

Discussion:

- IoT devices will become more safe for the Internet
- IoT devices will be still vulnerable and unprotected
- Zero-day vulnerability in IoT device firmware will not break the proposed technology
- But if an adversary will turn off Agent WB or will generate fake anomaly signals, it should be a problem
- Weak DDoS attacks may still appear if the threshold of the TI module is relatively high

Agent WB and classifier technology:

- The classifier may use machine learning or other techniques
- A vendor should provide classifier for the one version of firmware only once
- An authenticity of anomaly signal should be guaranteed
- Agent WB may use trusted platform mechanisms to protect itself from an adversary

Conclusion:

- An analysis of IoT secuirty problems was performed
- A novel approach of safe IoT device was represented
- An architecture of the safe IoT device and appropriate ISP infrastructure was proposed

Thank you for attention!