Security Issues on Internet of Things

Theodoros Mavroeidakos and Dimitrios D. Vergados

[1]Department of Informatics, University of Piraeus
80, Karaoli and Dimitriou St., GR-185 34, Piraeus, Greece
Email: {mavroeidakos,vergados}@unipi.gr

Outline

Introduction

What's the situation with security on Internet of Things?

- According to a contributor for TechCrunch, the software engineer Ben Dickson:
  - *"More connected devices mean more attack vectors and more possibilities for hackers to target us; unless we move fast to address this rising security concern, we'll soon be facing an inevitable disaster."*
- As stated by the MeshDynamics founder and CTO, Francis daCosta:
  - *"Billions of IoT devices cannot be individually managed; they can only be accommodated."*
  - *"Just imagine the possibilities for mischief and other IoT security issues when most of what happens on the world's networks not only isn't monitored but quite possibly cannot be."*

Motivation

The security issues and concerns surrounding the Internet of Things (IoT), occur as the consequence of:

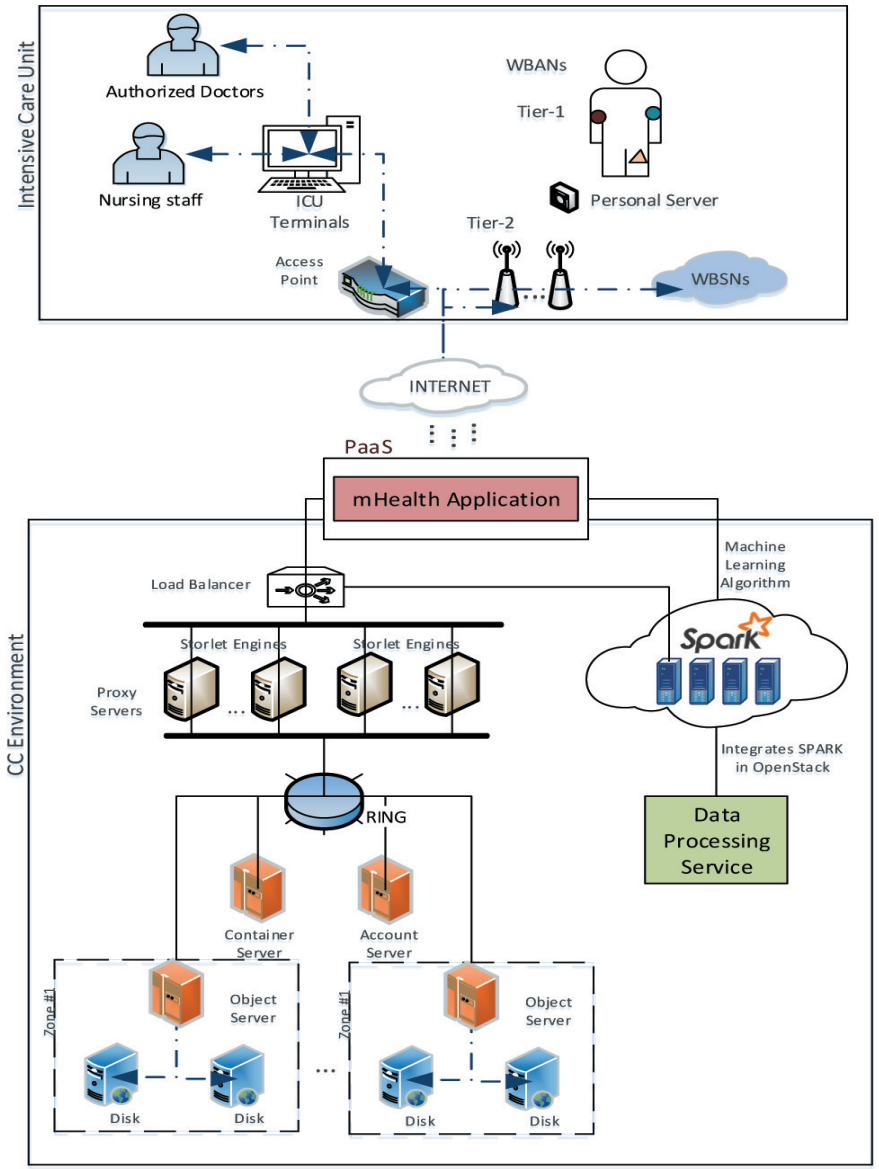
- **insufficiencies** residing on previous conventional security models utilized on wireless networks and mobile telecommunications,
- **threats** emerging due to unaccounted vulnerabilities and zero-day exploits extended both on hardware and software,
- **sensitive data** circulating the IoT infrastructure (i.e. clinical health data, spatial data), and
- **communication paths** facilitating interconnection of sensors and devices through a diversity of protocols and standards

IoT Infrastructure

The IoT Infrastructure can be divided into four layers:

- **Perception layer**: This layer consists of IoT devices such as Zigbee, RFID, GPS, but also sensors measuring Temperature, Humidity, Gas, Hydrogen, Air Pressure, etc.
- **Network Layer**: This layer supports the transmission of information and extends from the mesh construction of sensors to the backend APIs.
- **Processing Layer**: This layer provides the backend facilities (i.e. storage, compute services) where the processing logic (i.e. data mining, data transformations) is implemented.
- **Application Layer**: This layer enables outsourcing of already processed information to the users through IoT applications.

IoT Infrastructure: Health Care Use Case



IoT healthcare plans are implemented with Wireless Body Area Networks (WBAN) through the deployment of body sensors on patients.

T. Mavroeidakos, N. Tsolis and D. D. Vergados. Machine Learning Methodology boosts Intensive Care through Cloud-oriented WBAN Infrastructure. Submitted to IEEE International Conference on Communications (ICC), 2018.

Threats Landscape

Cyber-threats that target the IoT Infrastructure aim at harming its:

- **Consistency**
- **Confidentiality**
- **Integrity**
- **Availability**
- **Trust & Privacy**

The most harmful cyber-threats against the IoT are classified as:

- **Malware**
- **Denial of Service**
- **Botnets**
- **Physical Manipulation**
- **Information Leakage**
- **Remote Access Tools**
- **Ransomware**

Threats Landscape: Malware

Malware: is malicious software that hijacks the sensor's functions and spreads in the IoT infrastructure in order to gather operational intelligence.

Top IoT Malware:

- *BASHLITE*: infects embedded systems running BusyBox by initially exploiting the Shellshock software bug and then commences a DDoS attack. It propagates in the local network through brute forcing.
- *Linux.Darlloz*: is a worm that affects Linux based embedded systems such as Closed-circuit television (CCTV) and set-top-boxes used in cable, satellite and terrestrial television.
- *MrBlack*: targets networking devices with default credentials and their remote administration option left enabled. It is coupled with MITM attacks, cookie hijacking and other attacks.

Threats Landscape: Botnet

Botnet: is a network of infected devices spread across the world and controled remotely from a *master* following the client-server architecture.

Top IoT Botnet:

- *Remaiten*: is based on telnet scanning and logs in the victim system through username/password combinations which are tested recursively. Upon connection, it transfers the bot executable and establishes connection with the *master*. There are three strains of *Remaiten*, versions 2.0, 2.1 and 2.2
- *Mirai*: is a worm based on telnet scanning, launches DDoS attacks and targets Linux based embedded systems such as IP cameras and home routers. Since its source code publication, many blackhat groups utilize it in the midst of malware development.

Threats Landscape: Imminent Threat 'IoT_reaper'

IoT_reaper: is a malware botnet that gathers and assesses information in order to use ideal exploits with regard to the discovered vulnerabilities. Already infected two million devices and growing at rate of 10,000 new devices per day.

Vulnerable IoT devices:

- D-Link, Netgear, TP-Link and Linksys Router
- CCTV and Wireless IP Cameras

Reaper attack is based on the weaponization of Proof of Concepts (PoC) exploits with malicious payloads against known vulnerabilities:

- *CVE-2017-8222 - RSA key and certificates*
- *CVE-2017-8225 - Pre-Auth Info Leak (credentials) within the GoAhead http server*
- *CVE-2017-8223 - Misc - Streaming without authentication*
- *CVE-2017-8221 - Misc - "Cloud" (Aka Botnet)*

Threats Landscape: Botnets in Defense

Top IoT Defensive Botnets:

- *Hajime*: is an IoT worm and adversary of *Mirai* botnet. It breaks into unsecured devices through Telnet and blocks access to ports 23, 7547, 5555, and 5358, common entry points for Mirai worm and other threats. This worm indicates a whitehat signature, due to the lack of malicious objectives so far (*it has a master*).
- *Linux.Wifatch*: is based on Telnet connections using weak credentials. Upon its installation on IoT devices, removes malware of known families and connects the infected device to a peer-to-peer (P2P) network for the purpose of receiving threats' updates.

Both of them, compromise IoT devices to **secure** them:

- without hazardous payloads (i.e. bind and reverse shell) leading to attacks such as DDoS, but also
- without administration consent. **Violation or not?**

Threats Landscape: Ransomware

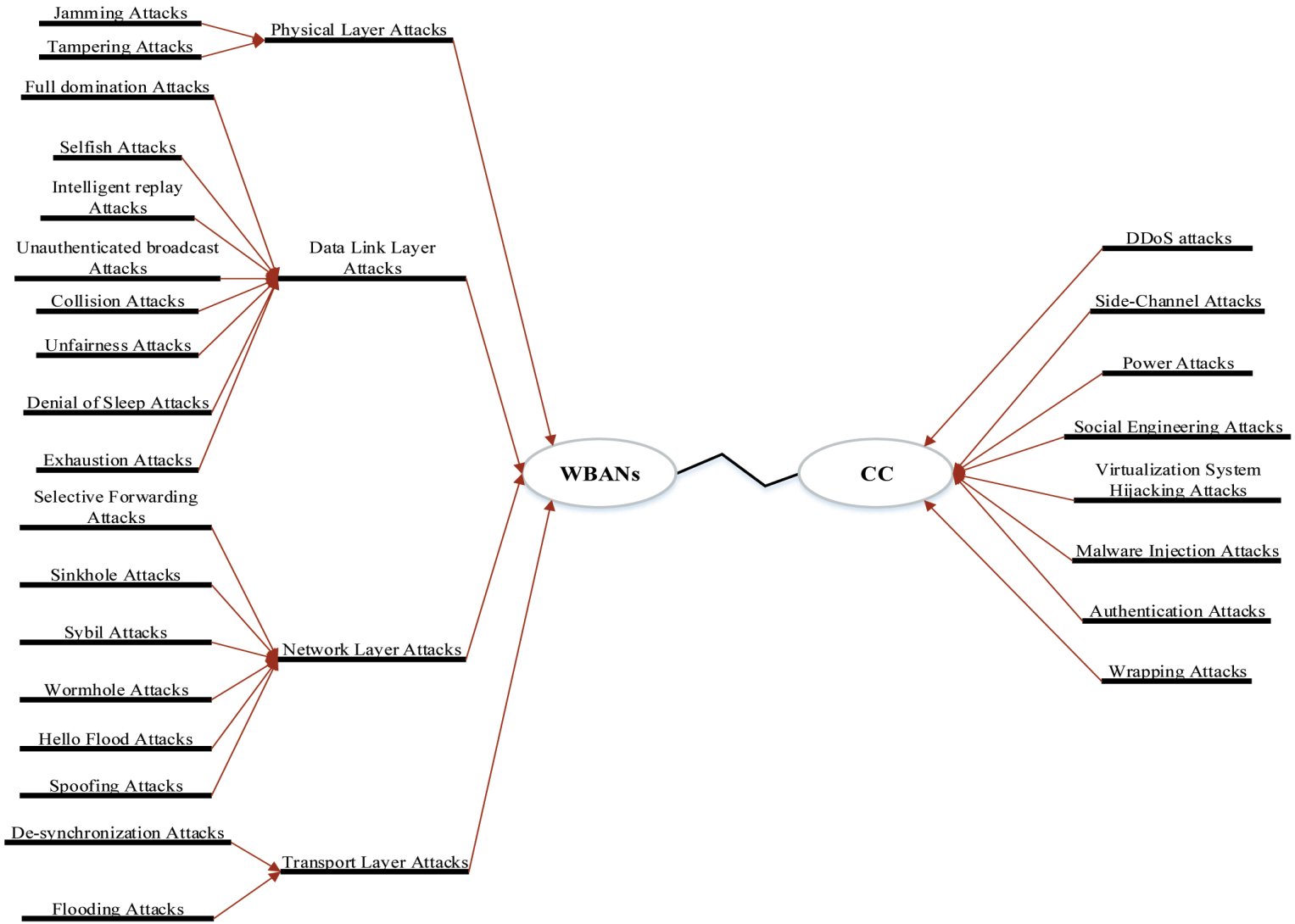
Ransomware: targets data storage facilities and blocks access to the collected data by encrypting them. A ransom should be paid in order to decrypt them.

- Ransomware attacks disrupt business continuity of the IoT infrastructure with few ways out except the ransom's payment.
- Ransomware attacks against IoT healthcare infrastructures in 2016, had been costed over $10,000 each.

Top Ransomware against IoT:

- *CryptoWall*: generates and stores a key on backend IoT infrastructure and then sends the key to command and control (C&C) server which is behind a proxy chain and controlled by the attacker.
- *Curve-Tor-bitcoin Locker (CTB-Locker)*: uses AES encryption by compression step using ZLib and communicates with the C&C server through proxy websites (Tor2web).

Threats Landscape: Health Care Use Case



Working Paper: T. Mavroeidakos, N. Tsolis and D. D. Vergados. Security Model employing Attack-Tree based Risk Assessment on Cloud-oriented WBAN Health Care Infrastructure.

Security Model: Countermeasures

Countermeasures should be orchestrated with regard to:

- the threat spectrum targeting IoT devices,
- known vulnerabilities lying on the backend Cloud APIs and
- the **intrusion kill chain** utilized by the attackers.

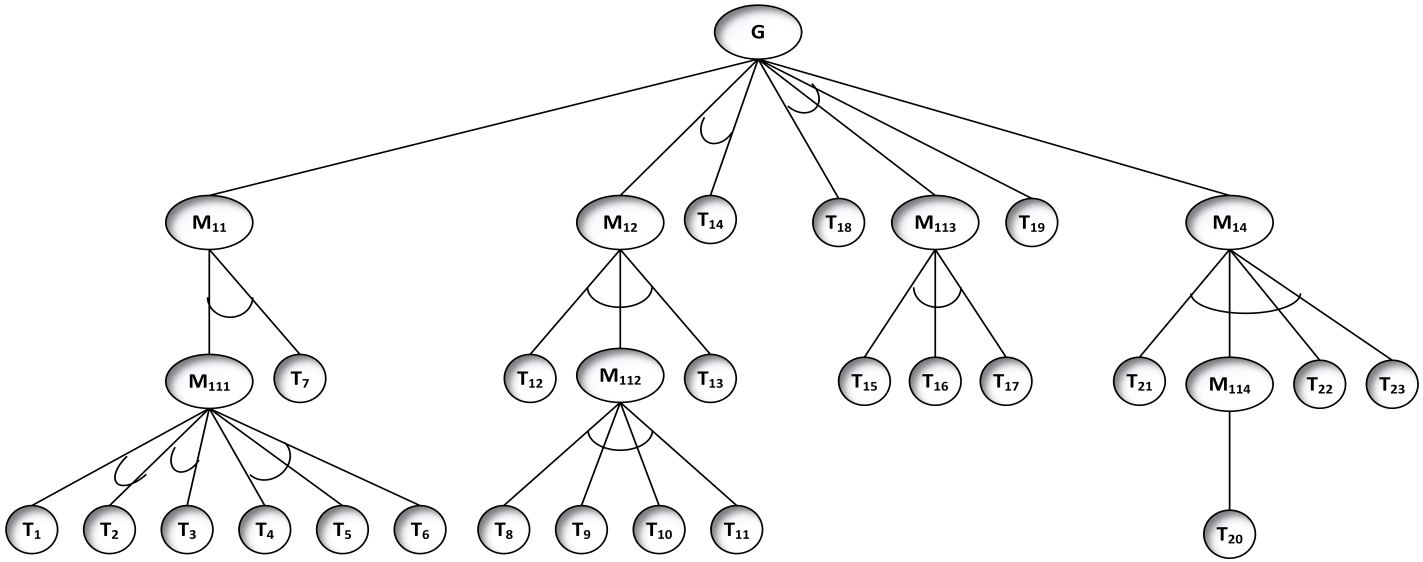
Intrusion Kill Chain

Each one of the intrusion kill chain phases should be *detected, denied, disrupted, degraded, deceived or destroyed* through the deployment of countermeasures in key positions according to the U.S. Department of Defense information operations (IO) doctrine.

Security Model: IoT Infrastructure Countermeasures

- **Preception Layer**: Secure booting, IPSec Security channel, Physical secure design, Anonymity
- **Network Layer**: GPS location system, Cryptographic hash functions, Security-aware Ad hoc Routing protocol (SAR), Dynamic routing tables
- **Processing Layer**: Fragmentation redundancy scattering (FRS), Homomorphic encryption, Advanced Encryption Standard, Attribute based encryption
- **Application Layer**: User Authentication, Access Control Lists (ACLs), Firewalls, Risk Assessment

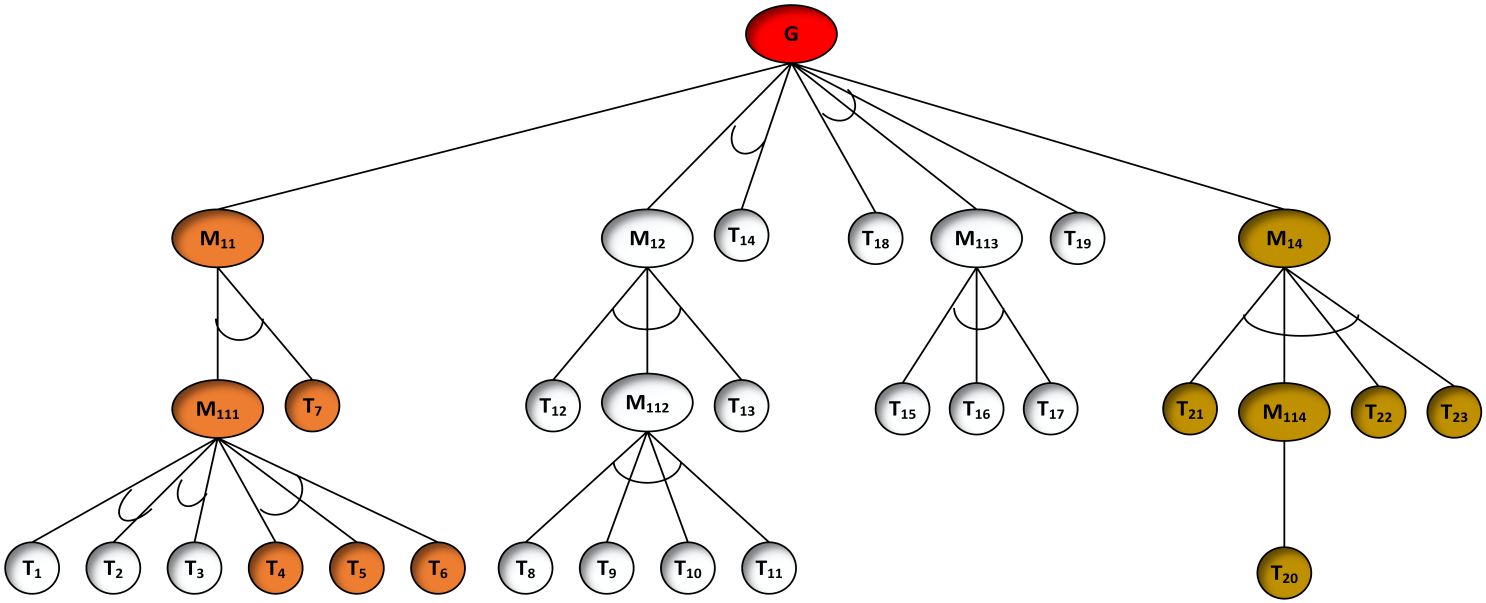
Security Model: Attack-Tree based Risk Assessment



G : Disclosure of Personally Identifiable Information (PII)
M_{111} : Eavesdropping Wireless Traffic
M_{112} : Capture Wireless Traffic with Encrypted Format of Password
M_{113} : Gain Access to Backend Environment
M_{114} : Connection to Compromised Machine
M_{11} : Extract Clinical Health Data
M_{12} : Break in the Wireless Network
M_{14} : Data Warehouse Discovery
T_1 : Malicious Sensor Node Injection
T_2 : Acquire Access to Unauthorized Areas of Hospital
T_3 : Medical Sensor Tampering
T_4 : Infect a Router with Malware
T_5 : Gain Command & Control
T_6 : Conceal malicious connection behind a proxy chain
T_7 : Traffic Analysis
T_8 : Capture Wireless Traffic
T_9 : Target one of the Hospital's Access Points by its Channel
T_{10} : De-Authenticate Access Point's Devices
T_{11} : Capture four-way Handshakes during Automated Authentication
T_{12} : Create a Profiled Dictionary
T_{13} : Brute Force the Wireless Traffic File
T_{14} : Deploy Monitoring Equipment/Services
T_{15} : Social Engineering
T_{16} : Information Gathering
T_{17} : Services Enumeration
T_{18} : Privileges Escalation
T_{19} : Data Repository Reconnaissance
T_{20} : Client Side Attack on Personnel
T_{21} : Network Foot printing
T_{22} : Restful APIs Enumeration
T_{23} : HTTP Parameter/Path Pollution Attack to add Attacker on Administrative Group

Working Paper: T. Mavroeidakos, N. Tsolis and D. D. Vergados. Security Model employing Attack-Tree based Risk Assessment on Cloud-oriented WBAN Health Care Infrastructure.

Security Model: Attack-Tree based Risk Assessment



G : Disclosure of Personally Identifiable Information (PII)
M_{111} : Eavesdropping Wireless Traffic
M_{113} : Gain Access to Backend Environment
M_{11} : Extract Clinical Health Data
T_4 : Infect a Router with Malware
T_5 : Gain Command & Control
T_6 : Conceal malicious connection behind a proxy chain
T_7 : Traffic Analysis

M_{114} : Connection to Compromised Machine
M_{14} : Data Warehouse Discovery
T_{20} : Client Side Attack on Personnel
T_{21} : Network Foot printing
T_{22} : Restful APIs Enumeration
T_{23} : HTTP Parameter/Path Pollution Attack to add Attacker on Administrative Group

Working Paper: T. Mavroeidakos, N. Tsolis and D. D. Vergados. Security Model employing Attack-Tree based Risk Assessment on Cloud-oriented WBAN Health Care Infrastructure.

Security Model: Attack-Tree based Risk Assessment

Four attributes are assigned to each leaf node in order to determine to what degree, the attacks are accomplishable. The probability of exploitation takes into acount these attributes.

Attack cost	Technical difficulty	Probability to be discovered	Probability to be exploited	Degree
>1	quite difficult	quite simple	very high	5
0.8 - 1	difficult	simple	high	4
0.5 - 0.8	mediate	mediate	moderate	3
0.2 - 0.5	simple	difficult	low	2
<0.2	quite simple	quite difficult	very low	1

Table: *Attack attributes.*

Risk = *f(AssetValue, Threat Probability, Vulnerability, Impact)*
Threat = *f(Capability, Opportunity, Motivation, Expected Impact)*

Conclusions

- The IoT devices consist only a branch of the IoT infrastructure which can be targeted as a means to mislead the organization's attention with the recovery, when other parts are exploited.
- Botnets can be utilized by a *master* not only for DDoS, but also to achieve cascading failures in the IoT infrastructure, leading even to physical damages (i.e. stuxnet).
- The risk assessment process should calculate the probability of at least one succesful exploitation for each asset of the IoT infrastructure.

Conclusions

Future Areas of Research

- Security on 5G - IoT devices
- Access to licenced and unlicenced spectrums of 5G - Operational risks
- Security Controls on M2M Communication Protocols
- Implementation of Privacy by Design & Defence in Depth in parallel

Thank you for the attention!
Questions?

References I

- Wu, T., Wu, F., Redout, J.M. and Yuce, M.R., 2017. An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications. IEEE Access, 5, pp.11413-11422.
- Dorsemaine, B., Gaulier, J.P., Wary, J.P., Kheir, N. and Urien, P., 2017, June. A new threat assessment method for integrating an IoT infrastructure in an information system. In Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on (pp. 105-112). IEEE.
- Minoli, D., Sohraby, K. and Kouns, J., 2017, January. IoT security (IoTSec) considerations, requirements, and architectures. In Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual (pp. 1006-1007). IEEE.
- Ahemd, M.M., Shah, M.A. and Wahid, A., 2017, April. IoT security: A layered approach for attacks & defenses. In Communication Technologies (ComTech), 2017 International Conference on (pp. 104-110). IEEE.
- Zahra, A. and Shah, M.A., 2017, September. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In Automation and Computing (ICAC), 2017 23rd International Conference on (pp. 1-6). IEEE.
- ENISA Threat Landscape Report 2016 15 Top Cyber-Threats and Trends
- Hutchins, E.M., Cloppert, M.J. and Amin, R.M., 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), p.80.