## Anatomy of Threats to the IoT CDT Threats & Risks: Session 4

Matthew Edwards

Oct. 31st, 2019

# Section 1

## Overview

#### Introduction What is this paper about?

#### Survey paper of threats to the Internet of Things (IoT).

Argument:

- 1. enterprise all turning to IoT in some form;
- 2. IoT security seems to suck;
- 3. previous survey papers incomplete;
- 4. thus: this paper.

| Existing<br>Survey | Consolidated<br>Introduction to<br>IoT | Illustration of<br>generalized<br>and threats at<br>IoT layers  | Threats to IoT<br>Communica-<br>tion Protocols | Examples of<br>real-world<br>attacks | Security issues<br>of Cloud-based<br>IoT and Fog<br>computing | Malware Threat | IoT Botnets             | Defense-In-<br>Depth security<br>measures  | Summary of<br>threats to IoT<br>and associated<br>vulnerabilities | Open research<br>issues                  |
|--------------------|--|---|--|--------------------------------------|---|----------------|-------------------------|--|---|--|
| [8]                | x                                      | Limited security<br>issues at IoT<br>layers   | x  | x                                    | x   | x              | x                       | Theoretical se-<br>curity solutions  | x   | x  |
| [10]               | x                                      | DoS attacks in<br>WSN and some<br>security issues<br>in RFID  | x  | x                                    | x   | x              | x                       | x  | x   | x  |
| [22]               | x                                      | Generalized<br>security gaps<br>concerning IoT<br>standardization   | x  | x                                    | x   | x              | x                       | -Pros and<br>Cons of<br>existing security<br>frameworks,<br>e.g., COBIT,<br>ISO/IEC<br>27002-2005<br>-Generalized<br>recommen-<br>dations for<br>hardware and<br>protocol security | x   | x  |
| [23]               | x                                      | Broadly covers<br>generalized se-<br>curity and pri-<br>vacy threats<br>Internal and ex-<br>ternal attacks<br>Physical<br>attacks and<br>attacks on user<br>privacy | x  | x                                    | x   | x              | Simple DoS at-<br>tacks | x  | x   | x  |
| [24]               | x                                      | x   | <b>√</b>                                       | x                                    | x   | x              | x                       | ×  | x   | IoT communi-<br>cation protocols<br>only |
| [25]               | x                                      | Security and<br>privacy issues<br>in some smart<br>home devices   | x  | x                                    | x   | x              | x                       | Proposes<br>an SDN-<br>based network<br>level security<br>mechanism  | x   | x  |
| [26]               | x                                      | Security issues<br>in WSN and<br>RFID   | x  | x                                    | x   | x              | x                       | Proposes an<br>loT security<br>architecture<br>comprising<br>perception,<br>transport and<br>application layer   | x   | x  |

TABLE I: Comparison of Existing Surveys

#### Threats to the IoT IoT Architecture

| Semantics Layer                                 |  |   |   |                                   |   |  |  |
|---|--|---|---|-----------------------------------|---|--|--|
| HDFS, MapReduce                                 |  |   |   |                                   |   |  |  |
|   |  | Ap  | oplication Layer                                    |                                   |   |  |  |
|   | CoAP (Web transfer protocol), MQTT (Messaging protocol), XMPP (IM Standard),<br>AMQP (Message oriented Protocol), DDS (Publish-Subscribe protocol), etc. |   |   |                                   |   |  |  |
|   |  | MAC / Adaptation / Network layer  |   |                                   |   |  |  |
|   |  | 6LoWPAN, Routing Protocol (RPL), IPv4/IPv6<br>NFC, UWB, RFID, BLE, 802.15.4, LoRaWAN, WiFi, ZigBee, 3G, LTE-A, etc. |   |                                   |   |  |  |
|   |  |   | Physical / Perception Layer                         |                                   |   |  |  |
| Data Analysis     Business Modelling            | (Supply Chain)   | Receives data     from sensing  | S Smart Sensors<br>(smart watches,<br>smart phones, | Identification<br>&<br>Addressing | EPC, uCode, etc.  |  |  |
| Knowledge     Extraction                        | Raw Data Processing     (Smart Grid, Medical   | devices<br>• Forwards   | E sensors in<br>vehicles, etc.                      |                                   | RFID Tags   |  |  |
| • Decision Making<br>• Business<br>Intelligence | data, etc.)<br>• Decision Making<br>(Smart Home,<br>VANET, ICS)<br>Smart City, etc.)   | data to<br>application<br>layer   | O Wearable<br>Sensors<br>R<br>S RFID Tags           | Hardware                          | Smart Things, Sensors,<br>Arduino, Intel Galilio,<br>Raspberry Pi, Smart<br>Phones,etc. |  |  |
|   |  |   | Actuators   | Software                          | OS (Contiki, tinyOS,<br>Android, LiteOS<br>Cloud (Nimbits, Hadoop etc.)                 |  |  |
|   |  | Data sensing and collection     Frequency selection, modulation, de-modulatio                                       |   |                                   | on, de-modulation   |  |  |

# Threats to the IoT IoT vs Ordinary Networks

Differences between IoT and traditional networks:

- 1. Resources available on the endpoint.
- 2. Primarily slower/less secure wireless media.
- 3. Different types of data.
- 4. No 'perimeter', little room for host-based approaches.

#### Threats to the IoT General Threats

. . .

**Threat** Traffic introspection

Masquerading, data leakage

Device integrity

Remote code execution Threats to comms Resource exhaustion attacks **Vulnerability exploited** Lack of encryption/network access control. Poor authentication /authori-

sation mechanisms.

Physical security, tamperproofing, booting. Missing host/network security.

'Weak network and application layer security'

#### Threats to the IoT Physical Layer Threats

#### Threat

Eavesdropping nodes Battery drainage attack 'Hardware failure' Malicious data injection Sybil attack Activity information

#### Vulnerability exploited

Unprotected communications. Lack of spam control. Unprotected interfaces ... Weak access control. Lacking ID management.

#### Threats to the IoT Physical Layer Threats Continued.

#### Threat

Side-channel attacks Device compromise Timing attacks Node cloning Invasive intrusions Change of config Unauthorised device access

#### Vulnerability exploited

Vulnerable interfaces, booting. ... Lack of hardware security. Lack of tamper-proofing. ... Default/hard-coded credentials.

#### Threats to the IoT Network Layer Threats

**Threat** 'Unfairness, interrogation ....'

DoS attacks

Fragmentation attack MITM, eavesdropping

Spoofing, hello flood, homing

Message integrity attacks

#### Vulnerability exploited

Weaknesses in comms protocols, access control. MAC and comms protocol flaws.

Weak authentication & data security Weak authentication & antireplay.

#### Threats to the IoT Network Layer Threats Continued

Threat Network intrusion Node replication Storage attacks

DoS attacks

Vulnerability exploited Poor IDS/IPS, access control, identity management Weak network access control. Centralised data store; nonreplication of data, no ransomware protection. Weak link authentication & anti-replay.

## Threats to the IoT Application Layer Threats

Threat Malicious codes

Software modification

Brute force/dictionary attacks

SQL injection attacks

Identity/credential theft

Disclosure of private data

XSS

Vulnerability exploited Lack of application / web security, authentication and authorization mechanism Lack of application / web security Weak authentication and authorisation Injection flaws in SQL/noSQL databases + OSIncorrect authentication implementations Insecure web applications and APIs. Vulnerabilities in web applications and user unawareness.

#### Threats to the IoT Semantics Layer Threat

Threat Identity theft, privacy compromise

#### Vulnerability exploited

Lack of data/application security.

## Malware Threats

Xafecopy Trojan September 2017 trojan disguised as battery optimiser app, targeting Android devices. Subscribes user for mobile billing. Bypasses CAPTCHAs, sends SMS to premium numbers, hides notifications about billing.

- WannaCry May 2017 ransomware exploiting an SMB vulnerability in Windows. Demanded payment in Bitcoin. Foiled through counter-analysis trap.
- CryptLocker 2015 ransomware making use of exploit kit. Malware embedded in PDF and propagates as an email attachment. Removes itself from system once demand made, to counter forensics.

## Malware Threats

- Mirai DDoS attack launched against Brian Krebs (+ some other targets) from IoT botnets created from CCTV cameras with default credentials.
- Havex ICS-focused RAT aimed at spying on host. Targeted three ICS vendors with three different vectors, including official software download sites.
- Stuxnet Targeted worm designed to sabotage Iranian nuclear enrichment facility, delivered through infected USB flash drive. Exploited four zero-day vulnerabilities in Windows-based systems. Acted as a MITM attacker, masking malicious execution by replaying legitimate signals.

#### Malware Threats Attack Methodology



# Security Framework

Describes 'an attack methodology of a DDoS attack on IoT devices'

| Preparatory Phase  | Initial Exploitation & Infiltration Phase  | Execution Phase   | Propagation Phase  | Hideout Phase  |
|--|--|---|--|--|
| <ul> <li>Reconnaissance of<br/>target system (look<br/>for loT devices with<br/>specific<br/>vulnerabilities)</li> <li>Manufacturer</li> <li>Bavice hardware<br/>&amp; avice hardware<br/>&amp; avine sea</li> <li>Use of hardcoded<br/>login credentials</li> <li>Weaknesses in<br/>weaknesses in<br/>weaknesses in<br/>interfaces/APIs</li> <li>Open telnet ports</li> </ul> | Malware access the<br>vulnerable for device<br>Brute-<br>force/dictionary<br>attack to match login<br>credentials with a list<br>of default parameters | <ul> <li>Malware downloads<br/>additional payload<br/>from MD server</li> <li>Malware owne other<br/>malararound, it is<br/>deprice is<br/>peorfigured to be a<br/>part of Botnet</li> <li>Downloaded<br/>malware binary is<br/>executed</li> <li>Bot performs<br/>specific malicious<br/>tasks</li> <li>Bots communicate<br/>regularly with C2S</li> </ul> | Bots, external<br>scanner and C2S<br>scan the internet for<br>more vulnerable location<br>divices<br>found using special<br>wow.shodan.io and<br>www.censys.io<br>the Reporting<br>Server<br>• Reporting Server<br>forwards data to the<br>Loading Server<br>logs-in to<br>vulnerable loT<br>devices<br>vivicim devices are<br>instructed to<br>download malware<br>from MDS using<br>wget command | • Malware in Bots<br>remain dormant<br>• Bots perform<br>DDoS attack,<br>once<br>commanded by<br>the Botnet<br>owner |

## Security Framework Countering DDoS

| <ul> <li>Limit loT devices to communicate with legitimate website/l address</li> <li>By design, change of default login credentials at the time of device activation</li> <li>Strong password</li> <li>Firmware/software updates or patches</li> <li>Device activation through vendor's website after verification based on minimum security standards for that papilication</li> <li>Protect against atlacker's</li> <li>Vise of network firewall and IDS</li> <li>Obs onnect IoT devices in the volume destination addresses only</li> <li>Check for sudden increase in the volume of out going network traffic</li> <li>Watch for sudden increase in CPU usage</li> </ul> | Preventive   | Detective  | Responsive   | Corrective   |
|--|--|--|--|--|
|  | Measures   | Measures   | Measures   | Measures   |
| internet initial   | Limit IoT devices to<br>communicate with<br>legitimate websiteI/P<br>address     By design, change of<br>default login credentials<br>at the time of device<br>activation     Strong password     Firmware/software<br>updates or patches     Device activation through<br>vendor's website after<br>verification of user and<br>the device     Device certification based<br>on minimum security<br>standards for that<br>particular device type and<br>application     Protect against attackers | <ul> <li>Use of network firewall<br/>and IDS</li> <li>IP white and black<br/>listing at the network<br/>ingress</li> <li>Egress filtering to allow<br/>packets to legitimate<br/>destination addresses<br/>only</li> <li>Check for sudden<br/>increase in the volume<br/>of out going network<br/>traffic</li> <li>Watch for sudden<br/>increase in CPU usage</li> </ul> | Follow a well prepared<br>incident response plan<br>• Disconnect IoT devices<br>from the internet<br>Helps in interrupting<br>malware operation and<br>mitigating its effects and<br>further propagation | Reboot the infected IoT<br>devices<br>Change default/current<br>login credentials<br>Update the<br>firmware/software     These steps are aimed at<br>recovering the infected<br>devices. As malware<br>resides in the RAM<br>therefore, restarting the<br>device helps in the<br>removal of malicious<br>code, even if it is dormant<br>for sometime |

execution of the attack by making it difficulty for him to find weaknesses and infiltrate the network

#### Security Framework Overall Security Measures



#### Security Framework Preventive Security Measures



#### Open Challenges Basic Security Standards

- IoT products are being manufactured without security
- Need to develop lightweight versions of crypto for IoT
- Low manufacturing costs and energy consumption needs

#### Open Challenges Privacy-Preserving Data Aggregation

- Privacy requirements in IoT
- Homomorphic encryption in constrained IoT

#### Open Challenges Software/Code Integrity

- Secure software which can be updated
- Swarm attestation for heterogeneous devices

#### Open Challenges Blockchain

A distributed ledger for decentralised information store.

## Open Challenges Fog Computing

- Identity authentication quickly, given mobile context.
- Blockchain-based access control?
- Consistency of access control policy for multiple devices.

## Section 2

# Negatives

## Godawful Writing

## Anatomy of Threats to The Internet of Things

Imran Makhdoom<sup>1</sup>, Mehran Abolhasan<sup>2</sup>, Justin Lipman<sup>3</sup>, Ren Ping Liu<sup>4</sup>, Wei Ni<sup>5</sup> 1,2,3,4 University of Technology, Sydney, Australia, 5Data61-CSIRO imran.makhdoom@student.uts.edu.au1, mehran.abolhasan@uts.edu.au2, Justin.Lipman@uts.edu.au<sup>3</sup>, RenPing.Liu@uts.edu.au<sup>4</sup>, Wei.Ni@data61.csiro.au<sup>5</sup>

Abstract-The world is resorting to the Internet of Things (IoT) for ease of control and monitoring of smart devices. The ubiquitous use of IoT ranges from Industrial Control Systems (ICS) to e-Health, e-Commerce, smart cities, supply chain management, smart cars, Cyber Physical Systems (CPS) and a lot more. Such reliance\_on loT is resulting in a significant amount of data to be generated, collected, processed and analyzed. The big data analytics is no doubt beneficial for business development. However, at the same time, numerous threats to the availability and privacy of the user data, message and device integrity, the vulnerability of IoT devices to malware attacks and the risk of physical compromise of devices pose a significant danger to the sustenance of IoT. This paper thus endeavors to highlight most of the known threats at various layers of the IoT architecture with a focus on the anatomy of malware attacks. We present a detailed attack methodology adopted by some of the most successful malware attacks on IoT including ICS and CPS. We also deduce an attack strategy of a Distributed Denial of Service (DDoS) attack through IoT

services have seen an exponential economic growth in last five years especially in telehealth and manufacturing applications and are expected to create about \$1.1-\$2.5 Trillion contribution in the global economy by 2020 [2]. It is estimated that by 2020, the number of IoT connected devices will exceed to 30 billion from 9.9 million in 2013 [3] and M2M (Machine-to-Machine) traffic flows are also expected to constitute up to 45% of the whole internet traffic [4]. However, due to interconnection with the internet. IoT devices are vulnerable to various attacks [1, 5, 6, 7, 8, 9, 10]. Moreover, it is believed that IoT devices are being manufactured rapidly without giving much attention to security challenges and the requisite threats [11].

According to [12], more than 85% of enterprises around the world will be turning to IoT devices in one form botnet followed by requisite security measures. In the end 7 or the other, and 90% of these organizations are not 7 27

# Organisation

The goal of a survey paper is to collect and **systematically organise** research from within its topic.

This paper's use of categories is confusing to say the least:

- Lots of partial duplication between categories.
- Some categories are lists of things with no obvious commonality.
- Often lacks even definitions of things given as category of threat.
- Sometimes 'a threat' is a class of problems, sometimes it's one particular example of a problem, authors flop back and forth. The vulnerability enabling a particular attack is not always representative of the category.
- Malware is positioned as a section of its own for no clear reason.
- Threats 'per layer' seem to often refer to things on other layers.

## Accuracy

Some passages in this paper seem to be complete nonsense. 'Vulnerabilities exploited' list often bears little relationship to the actual problem mentioned in the discussion.

Sometimes extremely vague.

## Section 3

## Positives

## **Detailed Examples**

While sometimes very vague, the paper is littered with a few highly-detailed descriptions of particular kinds of technical attacks against computer systems.

The authors seem to have attempted to find examples of real attacks, and discuss those alongside the general threat categories, giving some grounding to what are often rather abstract discussions.

## Broad Coverage

Scoped the paper as being about all threats that might affect IoT

Ambitious and probably self-defeating, but means they've captured much more than is often considered.

## Section 4

# Next Week(s)

## Structure: Fortnights

Threat Modelling

Unknowns

Risk Management

**Driving Factors** 

Scaling Analysis