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:

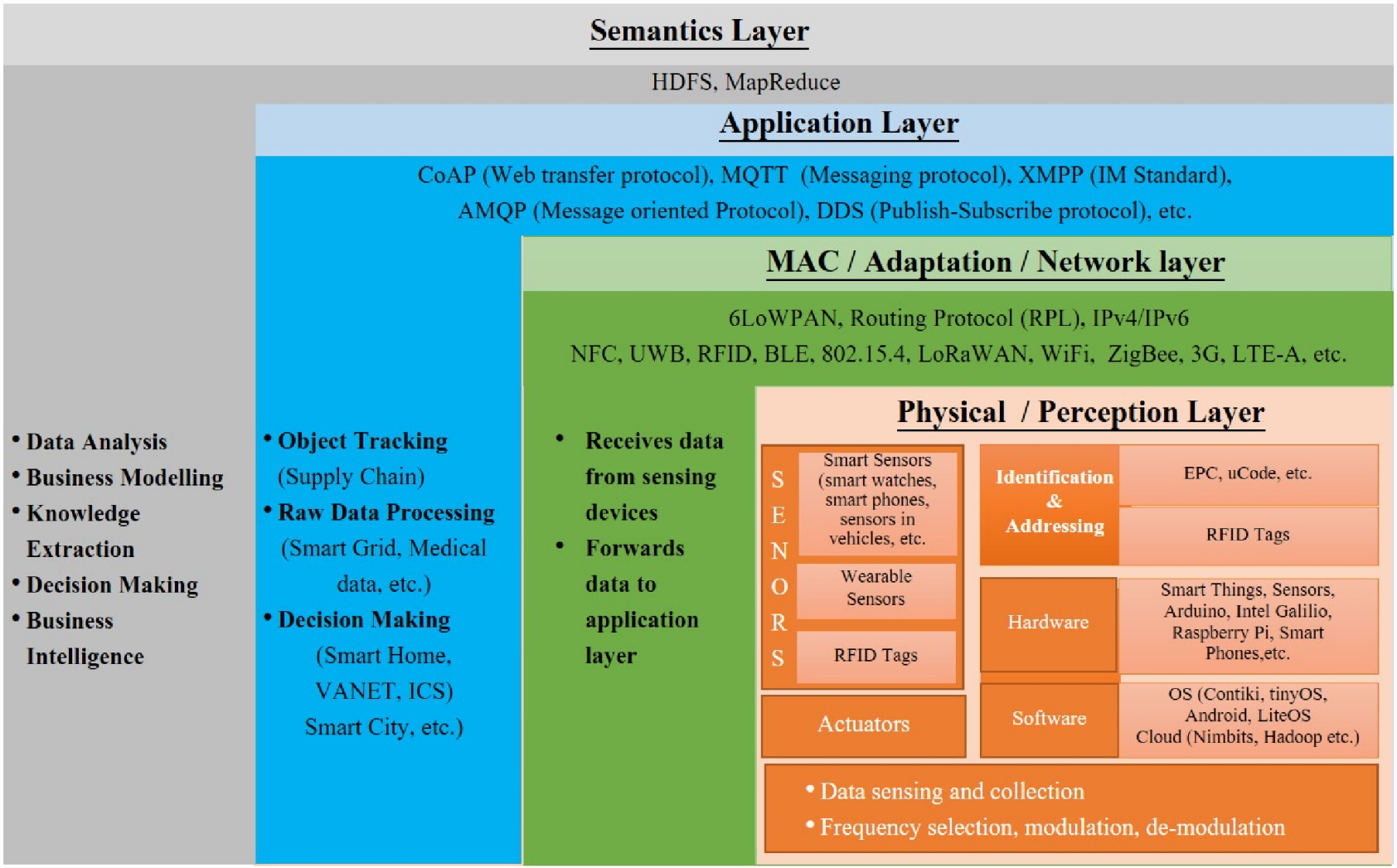
1. enterprise all turning to IoT in some form;
2. IoT security seems to suck;
3. previous survey papers incomplete;
4. thus: this paper.

TABLE I:
Comparison of Existing Surveys

Existing Survey	Consolidated Introduction to IoT	Illustration of generalized and threats at IoT layers	Threats to IoT Communication Protocols	Examples of real-world attacks	Security issues of Cloud-based IoT and Fog computing	Malware Threat	IoT Botnets	Defense-in-Depth security measures	Summary of threats to IoT and associated vulnerabilities	Open research issues
[8]	X	Limited security issues at IoT layers	X	X	X	X	X	Theoretical security solutions	X	X
[10]	X	DoS attacks in WSN and some security issues in RFID	X	X	X	X	X	X	X	X
[22]	X	Generalized security gaps concerning IoT standardization	X	X	X	X	X	•Pros and Cons of existing security frameworks, e.g., COBIT, ISO/IEC 27002:2005 •Generalized recommendations for hardware and protocol security	X	X
[23]	X	•Broadly covers generalized security and privacy threats •Internal and external attacks •Physical attacks and attacks on user privacy	X	X	X	X	Simple DoS attacks	X	X	X
[24]	X	X	√	X	X	X	X	X	X	IoT communication protocols only
[25]	X	Security and privacy issues in some smart home devices	X	X	X	X	X	Proposes an SDN-based network level security mechanism	X	X
[26]	X	Security issues in WSN and RFID	X	X	X	X	X	Proposes an IoT security architecture comprising perception, transport and application layer	X	X

Threats to the IoT

IoT Architecture



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	**Vulnerability exploited**
Traffic introspection	Lack of encryption/network access control.
Masquerading, data leakage	Poor authentication /authorisation mechanisms.
Device integrity	Physical security, tamperproofing, booting.
Remote code execution	Missing host/network security.
Threats to comms	...
Resource exhaustion attacks	'Weak network and application layer security'

Threats to the IoT

Physical Layer Threats

Threat	**Vulnerability exploited**
Eavesdropping nodes	Unprotected communications.
Battery drainage attack	Lack of spam control.
'Hardware failure'	Unprotected interfaces . . .
Malicious data injection	Weak access control.
Sybil attack	Lacking ID management.
Activity information	. . .

Threats to the IoT

Physical Layer Threats Continued.

Threat	**Vulnerability exploited**
Side-channel attacks	
Device compromise	Vulnerable interfaces, booting.
Timing attacks	...
Node cloning	Lack of hardware security.
Invasive intrusions	Lack of tamper-proofing.
Change of config	...
Unauthorised device access	Default/hard-coded credentials.

Threats to the IoT

Network Layer Threats

Threat	**Vulnerability exploited**
'Unfairness, interrogation . . . '	Weaknesses in comms protocols, access control.
DoS attacks	MAC and comms protocol flaws.
Fragmentation attack	. . .
MITM, eavesdropping	Weak authentication & data security
Spoofing, hello flood, homing	Weak authentication & anti-replay.
Message integrity attacks	”

Threats to the IoT

Network Layer Threats Continued

Threat	**Vulnerability exploited**
Network intrusion	Poor IDS/IPS, access control, identity management
Node replication	Weak network access control.
Storage attacks	Centralised data store; non-replication of data, no ransomware protection.
DoS attacks	Weak link authentication & anti-replay.

Threats to the IoT

Application Layer Threats

Threat	**Vulnerability exploited**
Malicious codes	Lack of application / web security, authentication and authorization mechanism.
Software modification	Lack of application / web security
Brute force/dictionary attacks	Weak authentication and authorisation
SQL injection attacks	Injection flaws in SQL/noSQL databases + OS
Identity/credential theft	Incorrect authentication implementations
Disclosure of private data	Insecure web applications and APIs.
XSS	Vulnerabilities in web applications and user unawareness.

Threats to the IoT

Semantics Layer Threat

Threat	**Vulnerability exploited**
Identity theft, privacy compromise	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

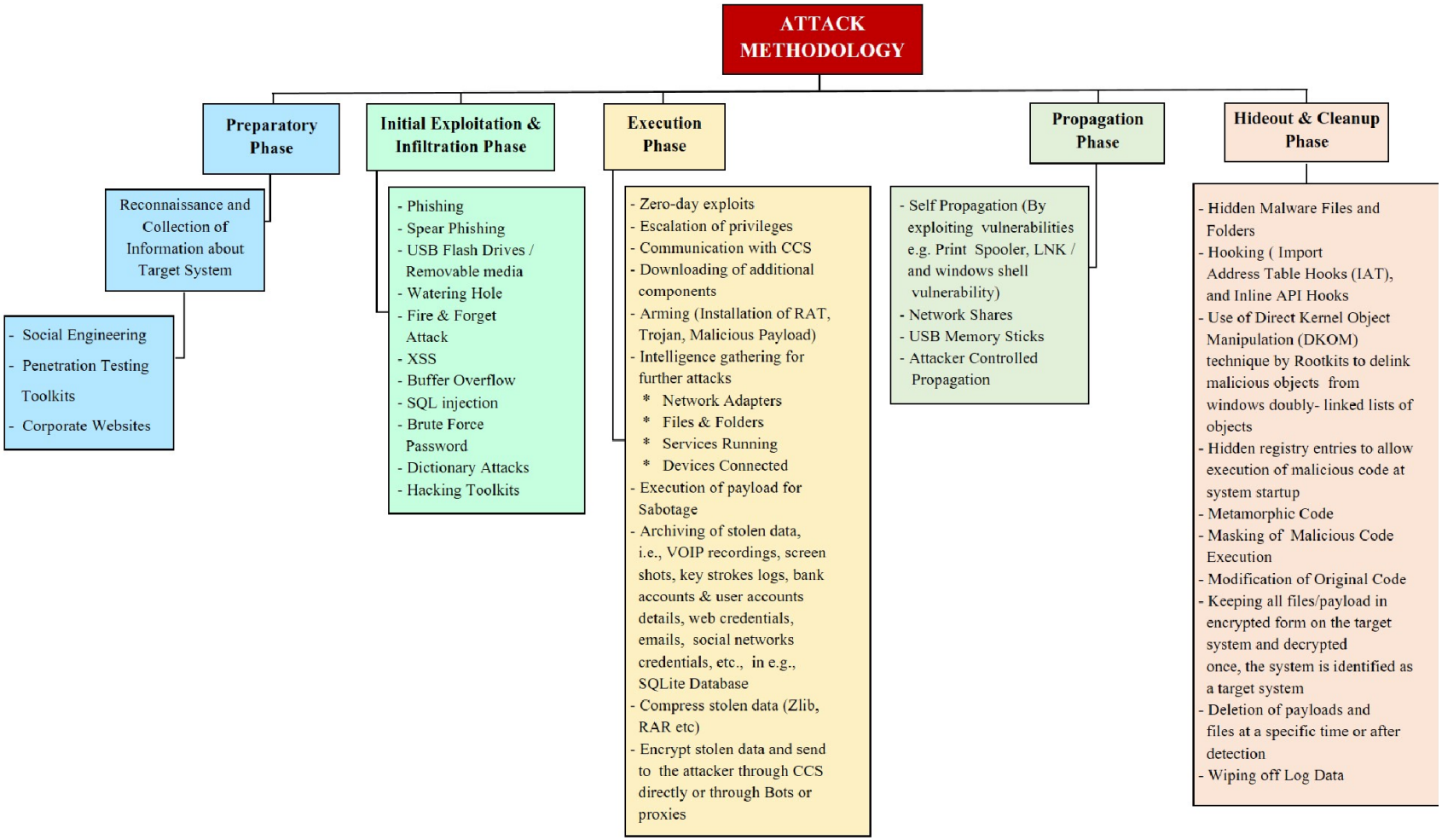
Mirai DDoS attack launched against Brian Krebs (+ some other targets) from IoT botnets created from CCTV cameras with default credentials.

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.

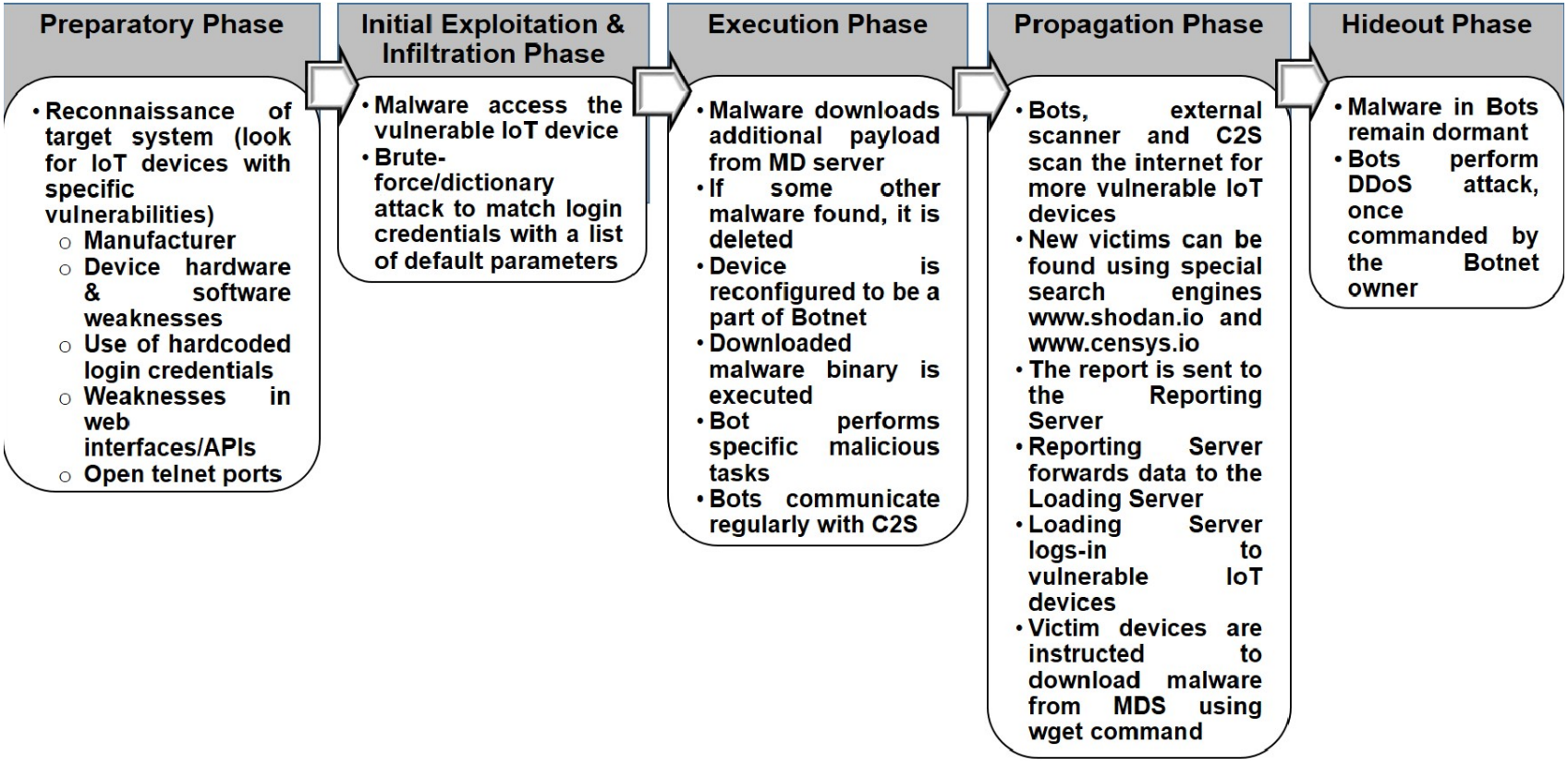
Malware Threats

Attack Methodology

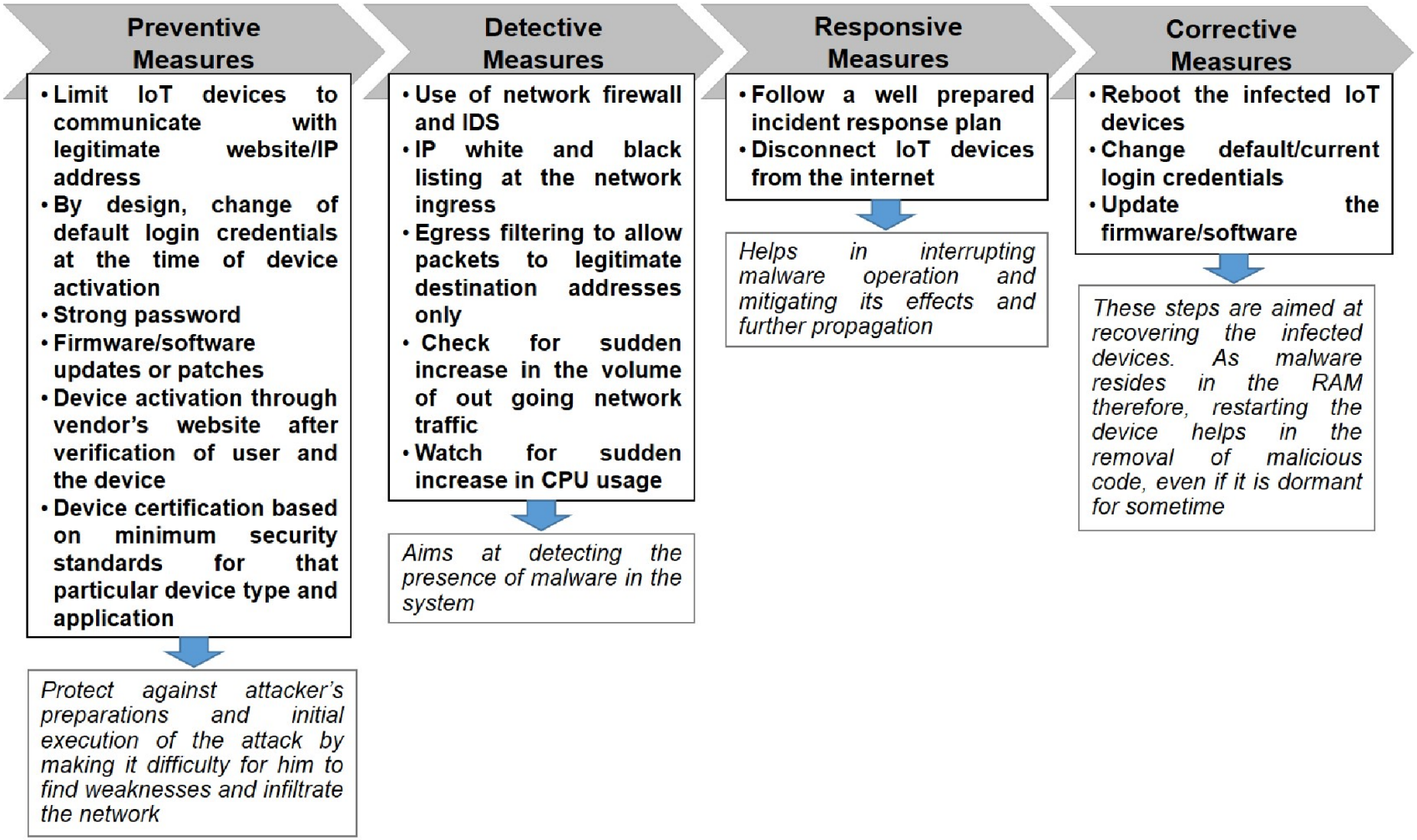


Security Framework

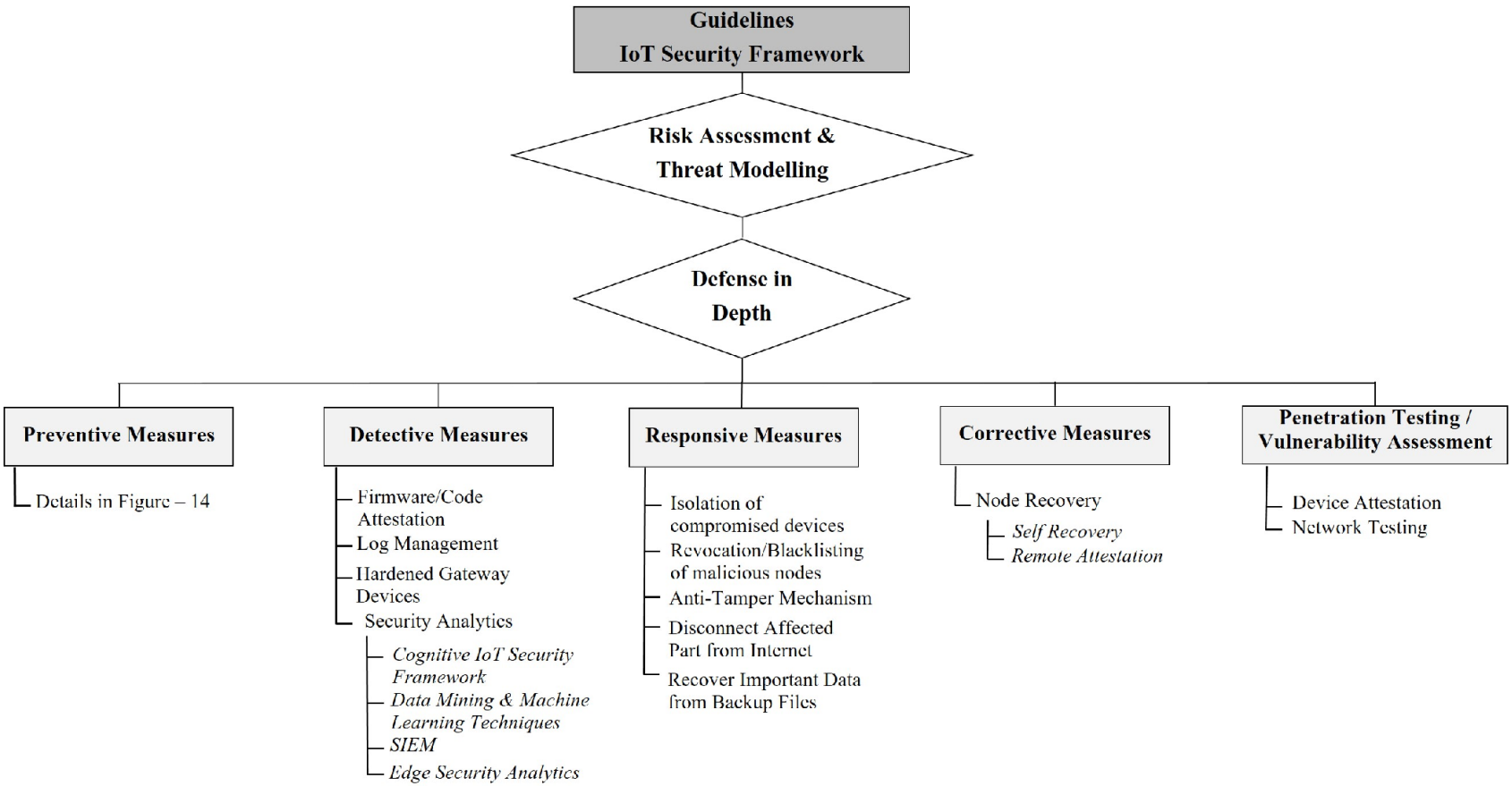
Describes 'an attack methodology of a DDoS attack on IoT devices'



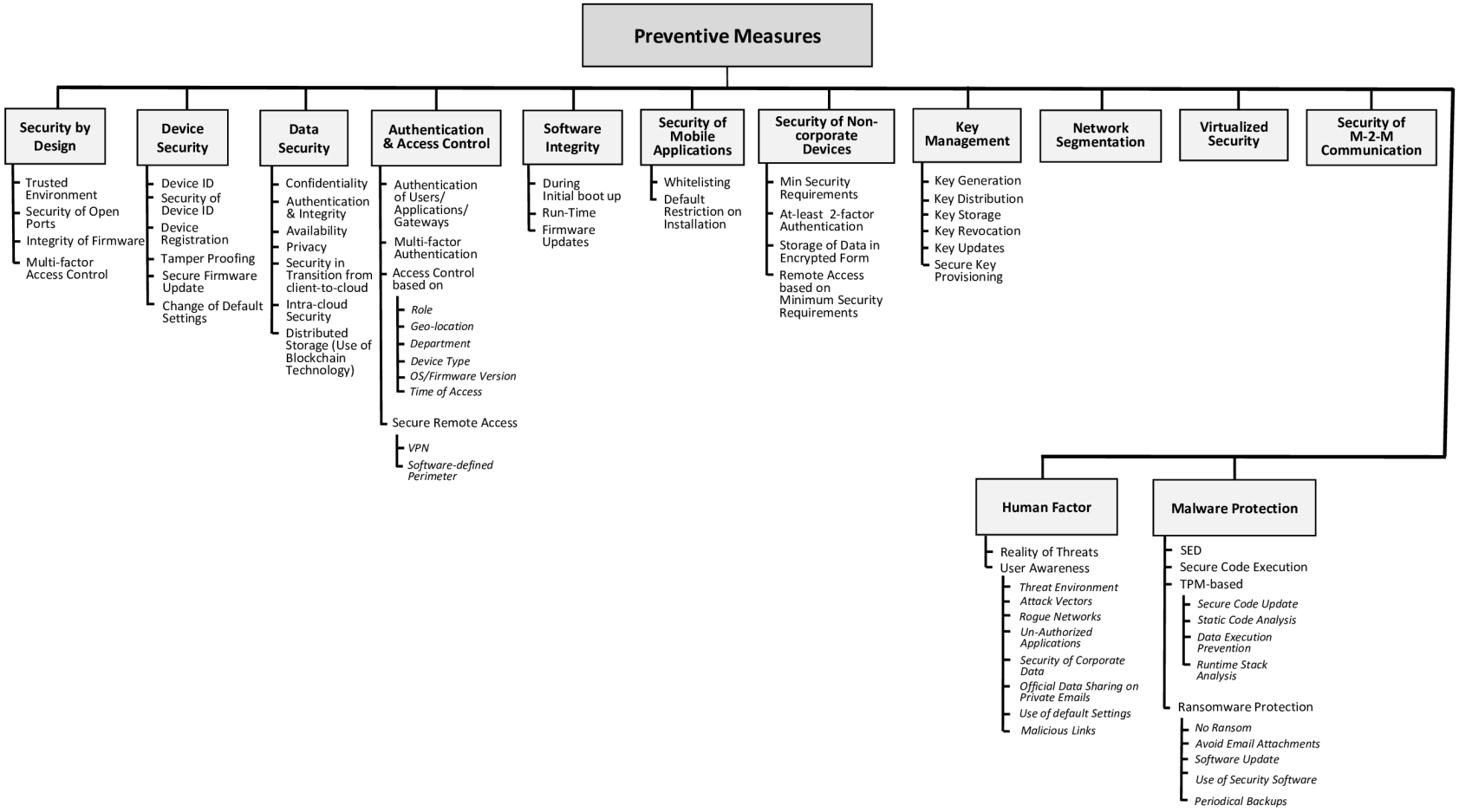
Security Framework
Countering DDoS



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[1], Mehran Abolhasan[2], Justin Lipman[3], Ren Ping Liu[4], Wei Ni[5]
[1,2,3,4] University of Technology, Sydney, Australia, [5]Data61-CSIRO
imran.makhdoom@student.uts.edu.au[1], mehran.abolhasan@uts.edu.au[2],
Justin.Lipman@uts.edu.au[3], RenPing.Liu@uts.edu.au[4], Wei.Ni@data61.csiro.au[5]

***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 IoT 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 botnet followed by requisite security measures. In the end,**

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 or the other, and 90% of these organizations are not

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