Examining how cyber criminals target certain parts of Internet of Things infrastructures

Mrs. VELPURI PADMA[1], Mrs. V. LAVANYA[2] , ASSISTANT PROFESSOR,[12], DEPARTMENT OF ECE,
SWARNANDHRA COLLEGE OF ENGINEERING AND TECHNOLOGY, NARASAPUR

Abstract

This article discusses the Internet of Things (IoT), including its analysis, techniques and means of protection, the potential of employing edge computing to reduce traffic transmission, the decentralisation of decision-making systems, and information security. There was intensive research into the ways in which IoT systems are attacked, and safeguarding suggestions were developed as a result.

keywords

Cybersecurity, intrusion, and defence in an IoT environment; edge computing; IoT. keywords.

Introduction

Technologies related to the Internet of Things (IoT) have grown and been used much more recently. Researchers studying the Internet of Things sector have discovered that the overall count of devices that are connected is increasing at a remarkable rate. In just a few years, there will be over 50 billion IoT devices, even if the current estimate of 21 billion devices is correct [1, 2]. Because of the proliferation and widespread use of IoT devices, IT security experts are concerned about the lack of protection provided by these devices [3, 4, 5, 6, 7]. They contend that the increase in the number of unsecured Internet-connected devices has given scammers additional opportunities. There have been several reported cases of IoT systems malfunctioning. Regarding the application of these

Contextualization in Theory

The advantages of these devices and technologies, as well as humanity's evolution towards using Industry 4.0, are confirmed by an examination of the aforementioned works [1, 2, 10], demonstrating the importance of IoT research. The authors of [1, 2, 3] discuss the lightning-fast rate at which the Internet of Things is being adopted by diverse sectors of the modern information society. According to testimony provided by Ammerman [1], cloud computing was first used to process, analyse, and store sensor data before being used to inform management decisions. Edge computing is no longer a luxury but a necessity due to the exponential growth of connected devices and the resulting strain on network bandwidth and cloud storage capacity (measured in the billions of gigabytes). The author explains how edge computing and cloud technologies may work together and how they may even be required in certain situations, particularly in business. If you want to decrease latency and boost the dependability of your deployed systems, then edge computing is the most crucial part of the Internet of Things [1]. Models of the IoT architecture are described, the requirement for IoT security is identified, and findings from studies on the design of information security systems for IoT devices are provided, both centralised and decentralised options being considered. Securing information in its entirety is a pressing concern. With this in mind, Byler [3] outlines eight essential security technologies for protecting the Internet of Things, including: network security, authentication, encryption, attack security, security analytics, threat forecasting, interface protection, and delivery methods. The future of the Internet of Things (IoT) and the dangers it faces are discussed in [4, 5, 6, 10, 11, 12]. Based on their study, these studies corroborate the importance of security concerns, protective zones, and primary conceptual approaches to security. There have been several instances of disruptive cyberattacks, and the frequency with which hackers strike is increasing [7, 13, 14, 15]. Incidents, the losses from which may be estimated in billions of dollars, highlight the seriousness of the issue.

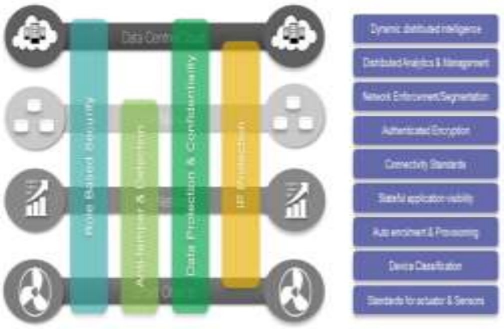
Data Centre
Role Based Security
Anti-tamper & Detection
Data Protection & Confidentiality
IP Protection
Dynamic distributed intelligence
Distributed Analytics & Management
Network Enforcement/Segmentation
Authenticated Encryption
Connectivity Standards
Stateful application visibility
Auto enrolment & Provisioning
Device Classification
Standards for actuator & Sensors

Figure 1: IoT security environment

HP experts have discovered, on average, 25 distinct security vulnerabilities in the mobile and cloud components of the devices they are examining [13]. Regretfully, HP's experts have concluded that there isn't now a safe Internet of things system. The overall increase in targeted attacks masks the unique risk to the Internet of Things. Our IoT friends betray us and provide hackers complete access to their owners' environments once they start to show interest in someone. The severity of the issue is such that companies that produce network and communication devices, software, hardware, and other components are rushing to come up with fixes [15]. Cisco Systems, a leader in IoT security and a major force behind the development of the IoT model at the World IoT Forum, developed

Results

We've broken down the hardware of our wireless Internet of Things (IoT) research system into the following categories [3, 4, 11, 6]:

1. communication subsystem (wireless communication in the sensor network, includes a radio receiver),

2. computing subsystem (data processing, node functionality),

3. sensor subsystem (network connection with the “outside world”),

4. power subsystem. Tasks facing the system to the hardware:

• low electricity consumption,

• the ability to work with a large number of nodes at relatively short distances,

• relatively low cost,

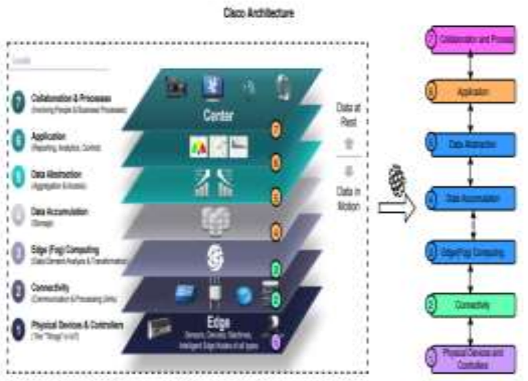
Cisco Architecture
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines, Intelligent Edge Nodes of all types
Data at Rest
Data in Motion
7 Collaboration and Process
6 Application
5 Data Abstraction
4 Data Accumulation
3 Edge/Fog Computing
2 Connectivity
1 Physical Devices and Controllers

Figure 2: Cisco IoT Architecture

• work autonomously and without maintenance,

• have a camouflage effect,

• be resistant to the environment.

We opted for Cisco's 7-tier model for IoT systems' structure (figure 2). The adoption of IoT systems to guard the periphery of the regime object raises the problem of cybersecurity in light of the fact that sensor networks are susceptible to several assaults. During the movement of cargo/persons/reconnaissance operation, it is assumed that temporary perimeter protection must be carried out. Figure 3 displays a simulation of a single IoT perimeter security zone created in Cisco Packet Tracer. A temporary perimeter security system zone may be set up with the help of the gadgets included in this plan. Also modelled a typical fire alarm system for a single room using the garage as an example (figure 4). The equipment is quite standard. In order to investigate possible cyber dangers and offer suggestions for the safety of IoT components, we have developed computer models, as shown in figures 3 and 4. Future research will reveal the outcomes of modelling and preventing cyberattacks. Through careful system modelling, we were able to identify the following as the most pressing cybersecurity concerns:

• communication security,

• protection of the devices themselves,

• control over the operation of devices,

• control of network interaction

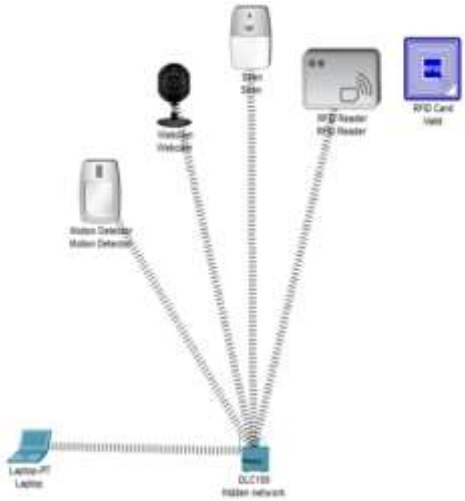

Figure 3: Cluster protection zone

As a result of research and analysis of the most likely attacks on simulated systems, the following classification of attacks is proposed (figure 5):

- Denial-of-Service (DoS) (D):
  - physical level (H):
    - obstacle attack (H_1)
    - attack of interference in the IoT system (H_2)
  - channel level (C):
    - collision attack (C_1)
- attacks on routing protocols (R):
  - "Black Hole" attack (R_1)
  - selective forwarding attack (R_2)
  - "Rapid onslaught" attack (R_3)
  - "Funnel" attack (R_4)

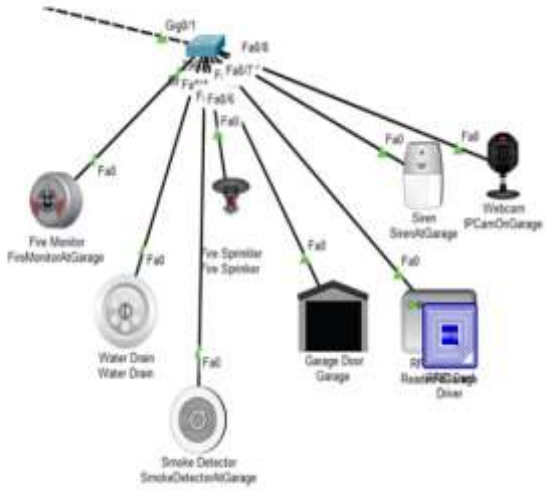

Figure 4: Scheme of fire alarm system of a separate room on the example of a garage

  - Sybil attack (R_5)
  - "wormholes" attack (R_6)
  - flood attack (R_7)
- attacks at the transport level (T):
  - avalanche attack (T_1)
  - desynchronization attack (T_2)
- attacks on data aggregation (G);
- privacy attacks (P).

Attacks can be represented in the form of open classification groups. $D = H \cup C$ – a set of attacks that lead to denials of service, involves combining sets of attacks at the physical and channel level. Many attacks that lead to denials of service at the physical level:

$$H = \bigcup_{i=1}^{n} H_i$$

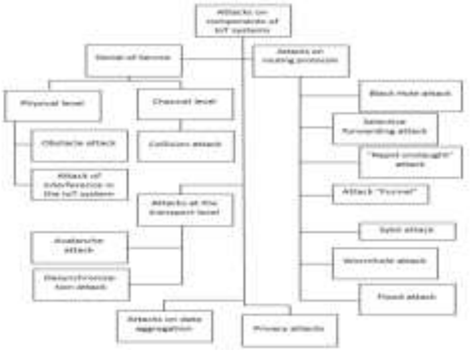

Figure 5: Attacks on IoT system components

The set of attacks that lead to denial-of-service link-level:

$$C = \bigcup_{k=1}^{z} C_k$$

The set of attacks on routing protocols:

$$R = \bigcup_{v=1}^{s} R_v$$

The open classification grouping of transport layer attacks is presented in the form of a set:

$$G = \bigcup_{j=1}^{m} G_j$$

The set of attacks on privacy:

$$P = \bigcup_{\gamma=1}^{\delta} P_\gamma$$

In general, attacks can be represented as a union of all classification groups:

$$A = D \bigcup R \bigcup T \bigcup G \bigcup P$$

Let’s analyse each attack that is part of the classification group.

A physical DoS assault. When an adversary attempts to disable a network or wipe out a network security service, they are launching a Denial-of-Service assault. DoS attacks in IoT systems may happen anywhere throughout the protocol stack, can impact many layers at once, and can take advantage of the interplay between them. The radio frequencies on which the system relies may be disrupted to launch a physical DoS assault. A single attacker node might cause a complete or partial network outage in this scenario (for example, blocking data transmission). Our approach relies heavily on the IoT's ability to identify an attack based on the presence of a sensor (in this example, a sensor/camera around a security item) and an effort to physically access it. An attacker may then either exploit the device to break into the network or destroy it, attempt to replace the data, get access to private information (including cryptographic keys), or all of the above.

DDoS attacks often target whole channels. The goal of a channel-level denial-of-service collision attack is often to exhaust the resources of nodes. As a result of this attack, various MAC protocols experience exponential latency and packet retransmission processes. Because of this, when a packet sustains extensive damage, the node will waste energy trying to employ error correction codes to recover the broken bits. A "collision" at the frame's conclusion is another kind of attack that causes the whole packet to be resent. Sending a Request for Transmission Suppression (RTS) message to a base station or neighbouring node can be a form of attack supported by the IEEE 802.11 protocols. This causes the receiving node to stop transmitting data to the sending nodes for the amount of time specified by the RTS message while it processes the RTS and sends a CTS message. Methods including a handshake may also be used.

Conclusions

From this study, we were able to generalise cyber risks to the individual parts of IoT systems. The results show that network nodes are the primary target of cyber assaults, and that the usage of wireless technologies for inter-system communication fosters an environment conducive to such attacks. Based on the newest technology means, qualified staff, control processes, administrative rules, and their strict adherence, it has been decided that today's multi-stage complicated protection systems are being implemented. By analysing attacks, we were able to compile a list of them and investigate their implementation details. Based on the findings of the analysis and generalisation, suggestions have been made to defend the individual nodes that make up the Internet of Things.

References

[1] G. Immerman, Edge computing's significance for the Internet of Things, 2020. Go to https://www.machinemetrics.com/blog/edge-computing-iot for more information.

[2] Research of the information security system of IoT devices, S. Khomich, A. Fedosiuk, M. Kulikovsky, Digital technologies 18 (2015) 166–171.

[3] J. Blyler, "8 critical technologies for IoT security," 2020. The following URL points to an article about 8 crucial IoT

security technologies: https://www.electronicdesign. com/industrial-automation/article/21805420.

[4] Security of the Internet of Things: perspectives and problems, Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Wireless Networks 20 (2014) 2481–2501. doi:10.1007/ s11276-014-0761-7.

[5] Information security of IoT systems, D. Kuznetsov, L. Ryabchina, Bulletin of Kryvyi Rih National University 49 (2019) 80–83.

[6] O. Turanska, "Development of information protection techniques in wireless sensor networks: master's thesis," NTU of Ukraine, "KPI named after Igor Sikorsky", 2018.

[7] C.