Modern Attack Vectors in IoT Systems

Jon Starkey

Bournemouth University
Bournemouth, United Kingdom
s4921588@bmth.ac.uk

***Abstract*—This report explores the frequency and nature of modern attacks on IoT systems, both physical and virtual. Vulnerabilities are discovered and exploited throughout the complex new IoT stack. Honeypots enable analysis of exploits technically and statistically, aiding in prioritising and patching vulnerabilities. Physical attacks are investigated for effectiveness and impact.**

***Index Terms*—IoT Security, IoT, exploits, honeypots, vulnerabilities, hardware**

I. Introduction

IoT systems are becoming ubiquitous, Evans estimates 50 billion IoT devices by 2020 [1], they are present in cars, factories, hospitals, fridges [21], and even in bins, baby diapers and batteries [16]. IoT devices typically operate in bespoke configurations, with low power consumption, minimal processing power, long unattended uptimes and often decentralised communications. IoT is data-driven [9], the value is in the data, the hardware devices are cheap and generally considered disposable. However their existence in an IoT system is imperative for operation and thus require security and protection. Do IoT vunrabilities exist and how can they be fixed?

In this paper we discuss the presence of attack vectors for IoT systems. Section 2 focusses on software and hardware IoT attacks. In section 3 we discuss virtual vulnerabilities analysing these attacking vectors in regards to operation and resolutions, displaying themes of attacks and attacks that prevail or pose high threat. In section 4 we discuss physical attacks on a range of components across the IoT architecture, questioning commonality and security. In section 5 we conclude.

II. Attack Vectors

An attack vector is the method along which an attack will infect a given system, in the form of an application or protocol exploit and abused via payload(s). Virtual attack vectors are identified by attackers using discovery tools such as Shodan.io [14] and nmap [15]. Physical attack vectors such as device tampering or theft of course exist and are discussed later in the paper.

Honeypots are controlled environments that intentionally publicly host applications or protocols known to feature exploits, enticing exploiters and learning from their attacks.

The IoT stack proposed by Akyildiz et al. [2] deviates from the typical two dimensional stack in the seven-layer OSI and four-layer TCP/IP models (figure 1). The three dimensional model demonstrates the vulnerability of IoT systems, three planes each requiring five layers, fifteen layers with multiple interdependent protocols. An attack could take place on one or more protocols, dependant on the device and attackers experience, using different protocols for stages of attack, resulting in more vulnerabilities. However this complex and often bespoke attack surface makes it harder to devise generic attacks [18].

Securing IoT devices is not trivial, these devices are heavily resource constrained, often running of battery or renewable energy. The devices suffer from limited RAM and ROM preventing security protocols from maintaining state and the lack of processing power renders public-key cryptography unusable [22]. Furthermore devices of varying age may be deployed within a network, so compatibility between new and old security mechanisms must occur.

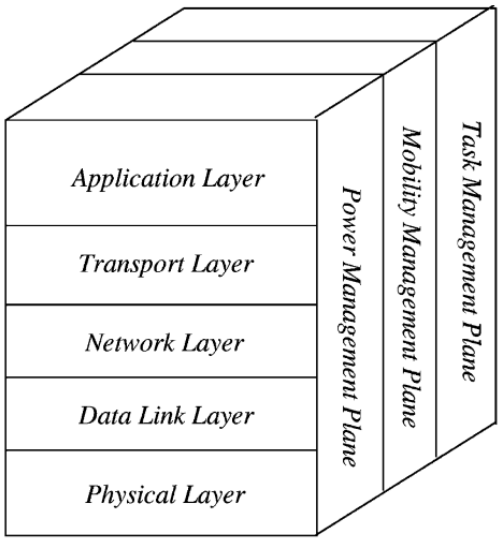

Fig. 1. The sensor networks protocol stack. [2]

III. Virtual Attacks

Virtual attacks revolve around manipulating behaviours in software, mostly through network protocols. As IoT is derived from traditional networking, both older and newer protocols are supported - Older protocols refrain developers from reinventing the wheel and allow existing technologies to connect to the IoT system, newer protocols allow the monitoring, control and data transmission. Given the nature of

IoT configurations, notably the long (up to ten year) battery life, these protocols must be resilient - cryptography methods are often insecure less then ten years from conception [3].

A. Application Layer Protocols

Attacks on IoT systems share commonalities with traditional networks. The act of 'sniffing','probing' and 'port scanning' are typical inspection methods attackers use to observe networks and network traffic for vulnerabilities. In an experiment hosting three honeypots over three months, Metongnon and Sadre [4] experience 37.4% of incoming network traffic as ICMP network discovery attempts. They note that other scanning softwares, such as Shodan.io are used to targetted the honeypots. Their research reveals the use of SSH as a probing tool on linux machines, "One could expect that SSH sessions are used in a similar way as telnet. However, a manual inspection of the traffic reveals that it mostly consists of connection attempts without further communication or of reflected traffic." [4].
When targets are identified attackers use the same methods to attempt access as typically seen in traditional networks. Telnet, like SSH, is used for probing and for remote commands. Metongnon and Sadre recorded that attackers utilised dictionary attacks using bruteforce to login over the telnet protocol. They note that when successful, attackers typically enabled bash and after checking that the machine is not a honeypot, they proceed to 'wget' or 'curl' utilities to download malware or viruses. These programs:- 'ICMP', 'SSH', 'Telnet', 'wget' and 'curl' are standard utilities not hacking tools and subsequently, can not be blocked.

B. Transport Layer

IoT systems share similar properties with torrenting (the act of downloading and sharing files over torrent networks), namely the use of peer-to-peer and decentralised technologies. Using decentralised protocols in IoT systems features a number of benefits for power consumption and data propagation, benefits that can be abused by hackers. A virus need only infect one device before it can distribute itself throughout the sensor network, "using BitTorrents DHT protocol for peer discovery and the uTorrent Transport Protocol (uTP) for data exchange" [17], protocols originally designed for torrenting. This poses a considerable threat - with the adage "a chain is only as strong as its weakest link" actualised here. Such threats can be removed by blocking the ports associated with these two protocols (blacklist) or by blocking all ports except those trusted (whitelist). Another solution proposed is too implement a trust metric between devices to prevent compromised devices spreading viruses [19].

C. Data Link Layer

Devices not using traditional 802.11 TCP/IP networking still offer vectors of attack. IoT devices use 802.15 low-powered low-rate radio communication protocols such as Bluetooth and Zigbee. Zigbee is used in Philips Hue smart lamps, which have been subject to numerous attacks [12] [13]. These lamps run a proprietary Amtel stack [11] containing a software bug discovered in research by Ronan et al. [10], which when exploited can call a reset procedure forcing smart lamps to disconnect and reconnect to a malicious controller. This exploit was built into a *war-flying* drone and was able to affect lamps more then 400 meters away. This type of low layer exploit can not be software patched. Whilst seemingly an innocent threat, an attack could be used in combination with a physical attack for example a burglary or trigger epilepsy.

D. Physical Layer

Jamming is a common attack technique designed to disrupt traffic through collisions and link saturation. Radio communications such as Wifi (802.11), Bluetooth (802.15.1) and Zigbee (802.15.4) have been demonstrated to suffer from collision attacks. The configuration of an IoT network makes use of ISM radio communication bands which are publicly available and can be subject to mistreatment. Networks such as Sigfox and LoRaWAN gave consideration to collision reduction through channel hopping and low transmission rates [25]. However these precautions did not prevent abuse by non node entities. In simulation research [26] LoRaWAN showed that both channel-oblivious and channel-aware jammers could be used to attack a network. LoRaWAN must distinguish its communication with that of other applications. To do this LoRaWAN packets contain a pre-amble to synchronise the sender and receiver. By listening and identifying the pre-amble and frequency a channel-aware jammer can disrupt a network by increasing the interference and noise for the channel, resulting in a node to gateway throughput decrease of around 56%. Channel-oblivious jamming operates by periodic jamming of many channels, causing collisions across frequencies, used by multi-channel LoRaWAN devices. Channel-oblivious jammers also cause bottlenecks at the gateway, Martinez et. al. showing gateway packet processing of jamming packets occupied resources hindering legitimate packet processing by a decreasing factor of 16 per minute [26].
In physical research [25] it was shown commodity hardware could be purchased that executes jamming attacks effectively on LoRaWAN devices. They use channel-aware (referred to as 'Triggered Jamming') selective jamming technique to block a specific node's traffic whilst allowing the continued operation of the remaining network.
To reduce the effectiveness of jamming, multiple gateways can be configured. Jammers operate most effectively closer to the gateway, multiple gateways would require multiple jammers to ensure the packet never reaches a gateway. Another proposed solution varies the packet size in order to increase transmission speed. An increase in transmission speed allows packets to arrive at the gateway sooner, reducing

the chance of collision within the network.

E. Power, Mobility and Task Management Plane

It is the resource constrained ad-hoc distributed nature of IoT networks that requires the addition of these three planes. The vulnerabilities shared between them are a result of the complexity of challenges faced in such networking environments. Ranking traffic and sources, directing traffic efficiently with NP-hard problems like the travelling salesman and power to performance costs underlying it all, alternative 'best effort' algorithms and protocols have been developed.

One such example, event driven operations rely on Timing-Sync Protocol for Sensor Networks (TPSN) for time synchronisation in order to:- Coordinated sensing tasks and subsequent data aggregation, sensor scheduling for triggered uptime and communication clock rates, time stamp routing tables. TPSN is subject to a number of attacks identified in research [20] [23].

- Masquerade attacks - where new nodes are disguised as trusted nodes in order to relay false information to disrupt the network timing. This can be patched by providing authentication of message exchange to prevent node impersonation by outsiders.
- Replay attacks - Where trust metrics exist, an an unauthorised node replays old packets from an authorised node to disrupt the network timing. This can be patched by maintaining a sequence number between nodes.
- Message manipulation attacks - A man-in-the-middle attack where nodes modify, destroy or fake time synchronisation packets to disrupt the network timing. This can be patched through use of misbehaviour detection schemes.
- Delay attacks - Where nodes delay packets in order to prevent time synchronisation occurring. This can be mitigated using delay detection schemes.

Song et. al. proposes a threshold-based delay attack detection mechanism. This mechanism calculates a maximum time threshold. When nodes join the network they derive this threshold to detect subsequent delay attacks - delay attack timing intervals can be detected as outliers and rejected when calculating the time synchronisation. This process relies on a beacon, which is not compromised, to observe the initial threshold between nodes and calculate the upper threshold without causing false positives (setting the threshold too low).

Likewise IoT routing protocols experience security attacks similar to the TPSN attacks. Direct Diffusion (DD) is a data-centric flat routing protocol featuring a base station (Fig 2 'sink') and reinforced gradients connecting nodes. The protocol design for ranking the gradients has vulnerabilities. Similar to replay attacks a base station can be be cloned, as the base stations are trusted nodes in routing protocols. With control of a base station an attacker can send data requests and over rank gradients to take control of the network [20].

Many routing protocols on traditional networks, such as Open Shortest Path First (OSPF) feature 'HELLO' packets to neighbouring routers. Likewise Direct Diffusion and LEACH have set-up phases where nodes are required to broadcast 'HELLO' packets to their neighbors to judge signal strength and map the immediate network. Typically these types of packet have a sending rate to reduce network flooding, however an attacker would not be bound by the constraints of an IoT device. By using a laptop, desktop or even smartphone the attacker could broadcast more frequent, further reaching and stronger signal packets. This has two effects, it can flood the network halting all packet transfer or convince all nodes the attacker is the closest neighbour creating a sinkhole effect [24], by not forwarding on packets.

IV. Physical Damage Attacks

IoT systems are complex resulting in many areas for attack. Physical attacks can range from arbitrary damage to the owning of entire systems. Figure 2 displays a typical IoT network configuration, of which any element (nodes A to X, sink, task manager) can be attacked, including social engineering of the user.

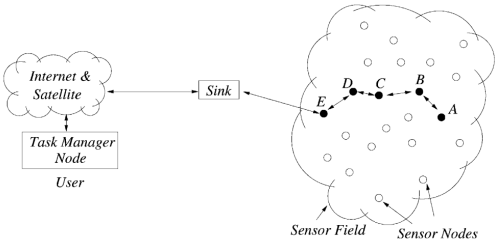

Fig. 2. IoT Network architecture. [2]

"Sensors and actuators are physical parts of the real environment and can be damaged or destroyed by any human intruder or natural disaster if not secured properly." [5]. However damage to or loss of nodes (low powered IoT devices) is expected, nodes are manufactured at minimal cost and considered disposable [2].

A well known recent example of physical damage is the Stuxnet worm [8]. Iran were using an IoT system for the running of their nuclear facility, the centrifuges were hacked forcing them revolve in an unsustainable manner causing considerable damage.

A. Sabotage and Theft

Ding et al. [6] discussed how an attacker could use the physical properties the system is monitoring to undertake physical 'attacks' using 'interaction chains'. For instance, a temperature driven window system - An attacker could

externally block air flow into a restricted room, heating the room and triggering the temperature driven window to open, subsequently gaining access.

IoT devices are typically bespoke, the theft of a node for example would not warrant in building another IoT network likewise a sole node would not justify selling. However the code, software and firmware may hold value, security vunrabilities like CWE-798 (Use of hard-coded credentials) and CWE-256 (unprotected storage of credentials) enables thieves to inspect systems with the possiblity of discovering exploits or reverse engineering systems for alternative attacks. Techniques to mitigate extracting sensative information from devices include Trusted Platform Module (TPM) [7] and Physical Unclonable Functions (PUF).

Song et. al. [20] states that if an attacker were to compromise a node subsequently to a break-in, "the adversary could easily compromise all the sensor nodes and then take over the network." They suggest that an effective key management system to overcome the problem.

B. Batteries Abuse

Similar to Ding et al. [6] work on interaction chains, battery abuse is physical attack by means of manipulating the sensor environment. Sensor networks operate in one of two ways, either the sink makes data requests or nodes send data only when a change is detected [2]. In the case of the latter configuration, attackers can frequently manipulate the sensing environment, to over work the nodes, resulting in premature battery power loss. Little can be done to tackle such abuse. In order to reduce such threats a deep learning algorithm must detect abusive triggers from natural triggers, but this is not within the processing or battery power of a node.

V. Conclusion

IoT devices are not built with security in mind and subsequently, we can see the impact this has had on all levels of security within the protocol stack. As attacks are deployed against IoT systems we see traditional protocols designed for similar resource constrained, decentralised and ad-hoc networks used in new IoT networks for probing and data distribution. We see attacks targeting multiple layers of the newly designed IoT protocol stack and efforts to mitigate these attacks in the form of protocol changes and design configurations. Lastly the physical threats to IoT are visited. Sabotage, theft and battery abuse are difficult security challenges for IoT to overcome and research continues to address these security concerns.

References

[1] D. Evans, "How the Next Evolution of the Internet Is Changing Everything", p. 11, 2011.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, p. 30, 2002.

[3] K. Kiningham, M. Horowitz, P. Levis, ad D. Boneh, Cesel: Securing a mote for 20 years", in Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, ser. EWSN 16. USA: Junction Publishing, 2016, pp. 307312.

[4] L. Metongnon and R. Sadre, "Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements", in Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity - WTMC 18, Budapest, Hungary, 2018, pp. 2126.

[5] S. ur Rehman, M. Ceglia, S. Siddiqui, and V. Gruhn, "Towards an Importance of Security for Cyber-Physical Systems/Internet-of-Things", in Proceedings of the 2019 8th International Conference on Software and Information Engineering - ICSIE 19, Cairo, Egypt, 2019, pp. 151155.

[6] W. Ding and H. Hu, "On the Safety of IoT Device Physical Interaction Control", in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS 18, Toronto, Canada, 2018, pp. 832846.

[7] Steven, K. 2006. "Trusted Platform Module Basics: Using TPM in Embedded Systems". Newnes.

[8] Nicolas Falliere and Liam O Murchu and Eric Chien "W32.Stuxnet Dossier" https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2011, Last accessed: October 2019.

[9] A. A. Pflaum and P. Golzer, "The IoT and Digital Transformation: Toward the Data-Driven Enterprise", IEEE Pervasive Comput., vol. 17, no. 1, pp. 8791, Jan. 2018.

[10] E. Ronen, A. Shamir, A.-O. Weingarten, and C. OFlynn, "IoT Goes Nuclear: Creating a Zigbee Chain Reaction", IEEE Secur. Privacy, vol. 16, no. 1, pp. 5462, Jan. 2018.

[11] Amtel, 2009. "Atmel Lightweight Mesh Stack". San Jose, Available from: https://community.atmel.com/forum/atmel-lightweight-mesh-stack [Accessed 11 November 2019].

[12] Latest Hacking News, 2016. "Philips Hue Smart Bulbs Vulnerable To Hackers", Available from: https://latesthackingnews.com/2016/11/04/philips-hue-smart-bulbs-vulnerable-to-hackers/ [Accessed 11 November 2019].

[13] Sal Cangeloso, 2013. "Philips Hue LED smart lights hacked, home blacked out by security researcher", Available from: https://www.extremetech.com/electronics/163972-philips-hue-led-smart-lights-hacked-whole-homes-blacked-out-by-security-researcher [Accessed 11 November 2019].

[14] John Matherly, 2009. "Shodan". Available from: http://shodan.io [Accessed 03 December 2019].

[15] Gordon Lyon, 1997. "Nmap". Available from: https://nmap.org/ [Accessed 03 December 2019].

[16] Spiceworks, 2016. "Are smart devices dumb? 8 connected devices you probably dont need." Available from: https://www.spiceworks.com/it-articles/dumb-smart-devices/ [Accessed 3 December 2019].

[17] Sam Edwards and Ioannis Profetis. 2016. "Hajime: Analysis of a decentralized internet worm for IoT devices." Available from: https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf [Accessed 03 December 2019]

[18] A. Acar et al., "Peek-a-Boo: I see your smart home activities, even encrypted!", arXiv:1808.02741 [cs], Aug. 2018.

[19] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Securing IoT Communications in Edge Networks", arXiv:1810.08415 [cs], Oct. 2018.

[20] Hui Song, Sencun Zhu and Guohong Cao. 2005. "Attack-resilient time synchronization for wireless sensor networks" IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005., Washington, DC, 2005, pp. 8 pp.-772. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1542869 [Accessed 04 Jan 2020]

[21] A. Yearp, D. Newell, P. Davies, R. Wade and R. Sahandi, "Wireless Remote Patient Monitoring System: Effects of Interference," 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, 2016, pp. 367-370.

[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003., Anchorage, AK, USA, 2003, pp. 113-127. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1203362 [Accessed 04 Jan 2020]

[23] X. Du and H. Chen, "Security in wireless sensor networks," in IEEE Wireless Communications, vol. 15, no. 4, pp. 60-66, Aug. 2008. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4599222 [Accessed 04 Jan 2020]

[24] J. Du and S. Peng, ”Choice of Secure Routing Protocol for Applications in Wireless Sensor Networks,” 2009 International Conference on Multimedia Information Networking and Security, Hubei, 2009, pp. 470-473. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5368816 [Accessed 05 Jan 2020]

[25] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, ”Selective Jamming of LoRaWAN using Commodity Hardware”, Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems Computing Networking and Services, pp. 363372, 2017. Available from: https://arxiv.org/abs/1712.02141 [Accessed 06 Jan 2020]

[26] I. Martinez, P. Tanguy and F. Nouvel, ”On the performance evaluation of LoRaWAN under Jamming,” 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), Paris, France, 2019, pp. 141-145. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8881830 [Accessed 08 Jan 2020]