A Review on Internet of Thing (IoT) Network Security

Hao Nguyen

Boston University

EC601

Project 1

Introduction

The IoT is the 21st century's concept that refers to a technology of connecting devices and objects. The rapid increase in IoT can be attributed to its use in various sectors such as communication, manufacturing, education, transportation, and general business development, among others. According to Gartner, there were 5.8 billion endpoints by the end of 2018 and expected to rise to 100 billions in 2025. Dignan (2019) reports that by 2025, the IoT industry will generate more than 79.4 zettabytes of data. Yet, the security of IoT devices are severely are severely outdated and is in no way sufficient to prevent malicious attack

IoT architecture

Traditional IoT architecture

A generic IoT system consists of 3 layers, perception, transportation and application.

Perception Layer

The perception layer is the physical layer that contains sensors and actuators that gathers data from the environment. A sensor node is a small standalone device that operates with limited computation power and battery resources. Sensor nodes can be categorized as radio-frequency identification (RFID), wireless sensor network (WSN), RFID sensor network (RSN), and GPS (Frustaci et al., 2018).

Transportation Layer

The role of the transport layer is to transfer data and information from the perception layer to other processing components. This layer uses the medium for the transmission such as the WIFI, LAN, 3G, Bluetooth, broadband, NFC, and RFID. If there is an issue with any of the mediums, the same issue will affect the IoT device. Another role of the transportation layer is

acting as the main connector among all the network devices, smart things and connecting with other networks such as an intranet, internet, and VPN.

Application Layer

The application layer plays the core role in IoT. According to Sen (2018), this layer connects all applications and services running IoT devices. They are the applications that receive data requests, process them, and issue responses. IoT users rely on these responses to make their decisions or consume them directly as the services. In fact, they are at the basis of the communications among applications and services running on different IoT devices and cloud/edge infrastructures. For example, a customer can ask for temperature data in a town in a different country. By performing a request query through a smartphone, the devices send a request to a cloud server that holds the applications, and the application concerned with weather data can respond by sending back that data. The significance of this layer makes its security one of its priorities.

IoT securities threat

Each of the layers of the IoT faces a different level of threats, both hardware and software.

The most common threats faced by the perception layer is the physical attack, malicious code injections and denial of service attack (DDoS). As this perception layer is essentially the physical infrastructure, some of the attacks are physical. For example, jamming the node can disrupt the node partially or entirely. The limitation of computation power, battery resources, and distributed organized structure also facilitate DDoS attack due to the ease of being overloaded. Other attacks include the intermediate malicious nodes, particularly in WSN, where the attackers modify the routing paths and redirect the data

The work of Baraković et al. (2016) provides an overview of attacks and vulnerabilities that happen over all forms of networks by taking advantage of the increased interconnectivity.

One of the common threats in the transportation layer is routing attacks. Such attacks happen when malicious people divert the traffic from going to the legitimate destination to their destination. DoS Attacks are also common in IoT. According to Galeano-Brajones et al. (2020), most commercial IoT low-end appliances and devices lack strong security mechanisms, making them easy targets for DoS and Distributed Denial of Service(DDoS) attacks. The third form of attack is Data Transit Attacks (DTA). According to Frustaci et al. (2018), DTA criminals can interfere with data integrity and confidentiality during data transit in access or core networks. Tsiknas et al. (2021) emphasize that DTA can also happen through Man in the Middle (MitM) attack or packet sniffing.

TRADITIONAL IT SECURITY VERSUS IOT SECURITY

Traditional IT Security	**IoT Security**
Add-on Security	Built-in Security
Complex algorithms	Lightweight algorithms for resource-constrained devices
User Control	Privacy issue: IoTs often collect automatically user private information
Small technological heterogeneity	Large technological heterogeneity and thus also large attack surface
Many security guards	Few security guards
IT devices are located in closed environments	IoT devices are also located in open environments

According to Frustaci et al. (2018), the main threats that experts need to consider for this layer are data Leakage, DoS Attacks, and Malicious Code Injection. For instance, the attackers

can penetrate this layer to steal passwords, personal data, and debit card numbers (Wu et al., 2020). In DoS Attack, the attackers can have ill motives, such as extorting money from an IoT company. For instance, ransomware attackers can take an online service out and demand a ransom payment before releasing it (Nozomi Networks Labs, 2020). Similarly, Malicious Code Injection such as SQL injection can be aimed at destroying data or stealing it.

Possible solution for security vulnerabilities

According to Frustaci et al, the security must be developed at multiple levels:

1. Hardware Security
2. Access Control and Authentication System
3. Data Encryption Mechanisms
4. Secure Routing
5. Risk Assessment:
6. Intrusion Detection System
7. Anti-Malware Solution
8. Firewall
9. Trust Management System

Current standard protocols for IoT security are developed for all three levels, physical, network and service level.

For the physical level, the four most common protocols are IEEE 802.15.4, BLE,Wi-Fi, and LTE. IEEE 802.15.4 is the operational standard for low-rate wireless networks. It relies on keys management and the master key must be kept physically safe to avoid the entire network being exposed. Blue-Tooth Low Energy(BLE) is based on short range radio It often consists of a host and a controller and encrypts a portion of the payload

to ensure security. IEEE 802.11/WiFi., a very popular and expanding protocols using WEP,WPA and WPA2 for security. It utilises a wide range of algorithms, from 64 to 128 static encryption key that must be manually entered to dynamically generated 128 bit key using the temporal key integrity protocol (TKIP). The newest algorithm (CCMP) used by WPA2 is a significant improvement over TKIP, reducing the load on the network while maintaining performance. LTE is a standard communication technology for mobile device, often use EIA or EPS algorithms, for their security.

For the network layer, the tree main protocols are IPv4/IPv6, 6LoWPAN and RPL. IPv4/IPv6 is the main drive for IoT expansion. IPv6, in particular, is the main component for IoT expansion due to its significantly better security algorithms than IPv4. The secure neighbor discovery protocol (SEND) in IPv6 incorporates cryptographically generated addresses (CGAs). This enhances IPv6 protection against DDoS, routing, soliciting and replay attacks. 6LoWPAN is developed to use by IoT devices with limited resource to implement the IP protocols. It has three general solutions for security: using IEEE 802.15.4 (link layer security), compresses IPsec for end-to-end security at the network layer or compress DTLS for security at the transport layer. RPL is the standardized routing protocol for all IoT devices.

At the service levels, there are 2 prominent proposed solutions, the Message Queuing Telemetry Transport (MQTT) and the constrained application protocol (CoAP). MQTT is an IoT lightweight data protocol. It employs a publisher-subscriber communication paradigm and enables easy data transfer between devices. The architecture of MQTT is its prominent selling feature. Its genetic make-up is simple and lightweight, allowing it to deliver minimal power consumption for gadgets. It also operates on top of the TCP/IP protocol suite. IoT data protocols

were created to address the issue of unstable communications systems. Constrained Application Protocol (CoAp) is utilized in the application layer. It is intended to meet the requirements of HTTP-based IoT systems

IoT Protocols: Issues and Solutions

	Protocols	Issues	Solutions	Type of Solutions
Physical Ac. Level	*IEEE 802.15.4*	Data Transit Attacks	AES-CCM algorithms [35]	standard
	BLE	Data Transit Attacks	AES-CCM algorithms [30]	standard
		Data Transit Attacks: header information is not encrypted	Black network solution [30]	NEW
	Wi-Fi	Data Transit Attacks	WEP, WPA, WPA2 protocols [32]	standard
	LTE	Data Transit Attacks	EEA and EIA algorithms [33]	standard
Network Level	*IPv4/IPv6*	Data Transit Attacks	IPsec protocol	standard
		Threats to NDP protocol	SEND protocol in IPv6 [34]	standard
	6LoWPAN	Data Transit Attacks	Compressed IPsec protocol [35], [38]	NEW
			Compressed DTLS [35]	NEW
			802.15.4 security features [35]	standard
	RPL	Routing and DOS Attacks	SVELTE IDS solution [41]	NEW
		Data Transit Attacks	AES/CCM algorithms [40]	standard
Service & Application Level	*MQTT*	Data Transit Attacks	TLS (PSK, Certificates) [49]	standard
		Data Transit Attacks, Scalable Key management, Heavy computation cost of TLS	Secure MQTT solution with ABE [42]	NEW
		Privacy for lack of user control	SecKit solution [44], [45]	NEW
	CoAP	Data Transit Attacks	DTLS protocol (PSK, RPK, Certificates) [47]	standard
		Data Transit Attacks, Heavy cost of computation and high handshake of DTLS	Lithe solution [48]	NEW

Open source programs

PENIOT

PENIOT is an open-sourced penetration testing program for IoT devices. It is built using Python. The entire code, program and documentations are available on github. It provides testing for commonly used protocols such as BLE, COAP and MQTT. A wide array of attacks are used to test the securities of IoT devices such as DDoS, replay, Payload size fuzzer, Topic name fuzzer, Generation based fuzzer and uses different hardwares and program to capture communication packets for testing.

Conclusion

The rise of IoT is expected to come with various benefits. Apart from improving the efficiency of operations, IoT will enable appliances, devices, and operations to communicate with each other and respond to the nature of the communication without human interruptions. However, organizations seeking to implement IoT in their services need to consider the issue of security as they lay out their infrastructure. As IoT layers correspond to different kind of attacks, there are a wide array of security protocols to be implemented.

References

Baraković, S., Kurtović, E., Božanović, O., Mirojević, A., Ljevaković, S., Jokić, A., Peranović, M., & Husić, J. B. (2016). Security issues in wireless networks: An overview. *2016 XI International Symposium on Telecommunications (BIHTEL)*, 1–6.

Brandom, R. (2018, April 11). *Even if you're not signed up, Facebook has a shadow profile for you*. The Verge. https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

Dignan, L. (2019). *IoT devices to generate 79.4ZB of data in 2025, says IDC*. ZDNet. https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/

El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internet of Things Security: Layered classification of attacks and Possible Countermeasures. *Electronic Journal of Information Technology*, *9*.

Estrada, D., Tawalbeh, L. A., & Vinaja, R. (2020). *How Secure Having IoT Devices in Our Homes?*

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291

Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. *Sensors (Basel, Switzerland)*, *20*(3), 816. https://doi.org/10.3390/s20030816

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., & Gabrys, B. (2016). The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. *2016 IEEE Congress on Evolutionary Computation (CEC)*, 1015–1021.

Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. *Sensors*, *20*(9), 2495. https://doi.org/10.3390/s20092495

Nozomi Networks Labs. (2020, September 10). *OT/IoT Security Report 2020: Rising IoT Botnets and Shifting Ransomware Escalate Enterprise Risk*. Nozomi Networks. https://www.nozominetworks.com/labs/reports/ot-iot-security-report-2020-2/

Sen, J. (2018). *Internet of Things: Technology, Applications, and Standardization*. BoD – Books on Demand.

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, e9324035. https://doi.org/10.1155/2017/9324035

Simplicio, M. A., Silva, M. V., Alves, R. C., & Shibata, T. K. (2017). Lightweight and escrow-less authenticated key agreement for the internet of things. *Computer Communications*, *98*, 43–51.

Sjarif, N. N. A., Chuprat, S., Mahrin, M. N., Ahmad, N. A., Ariffin, A., Senan, F. M., Zamani, N. A., & Saupi, A. (2019). Endpoint Detection and Response: Why Use Machine Learning? *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, 283–288.

Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, *2*(1), 163–188.

Wu, H.-L., Chang, C.-C., Zheng, Y.-Z., Chen, L.-S., & Chen, C.-C. (2020). A Secure IoT-Based Authentication System in Cloud Computing Environment. *Sensors*, *20*(19), 5604. https://doi.org/10.3390/s20195604

Zhang, J., Chen, H., Gong, L., Cao, J., & Gu, Z. (2019). The Current Research of IoT Security. *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, 346–353. https://doi.org/10.1109/DSC.2019.00059

Znaidi, W., Minier, M., & Babau, J.-P. (2008). *An ontology for attacks in wireless sensor networks* [Ph.D. Thesis]. INRIA.