COUNTERING ATTACKS FROM THREAT VECTORS ON IOT

Abstract

With the emergence of the Internet of things (IoT), the Industrial Internet of Things (IIoT), and artificially intelligent devices, more and more devices are now getting connected to the internet. The increased adoption of IoT applications has aided the development of smart cities, surveillance systems, and home automation devices. From smartwatches to self-driving vehicles, these technologies offer a wide range of applications. Countless applications like this are being designed and developed every day that will be viable soon. Although these applications make our lives easier, they open doors to new security concerns and leave us vulnerable to cyber threats. The major problem persisting in the IoT paradigms is data protection and improper handling of cryptographic algorithms. An attacker might exploit ineffective authentication approaches to append spoofed malicious nodes or violate data integrity resulting in an intrusion of IoT devices and network communications. This article throws light on the threats associated and ways to mitigate the risk at different levels.

Keywords: component; formatting; style; styling; insert (key words)

Authors

Thasni T
Department of Computer Science and Engineering

Tintu Vijayan
Department of Computer Science and Engineering

Arshiya Lubna
Department of Computer Science and Engineering

Mary Divya Shamili
Department of Computer Science and Engineering

I. INTRODUCTION

Imagine you wake up, the blinds on the window roll up on their own, an intelligent assistant greets you, "good morning!" and your smart kettle has hot water ready for your morning cup of tea even before you get off your bed. [6] You realize that you are out of milk, but you have a smart fridge that has already placed the order for all groceries that you'll need. The groceries are brought to your doorstep by an autonomous drone. You finally get ready, and your self-driving car takes you to your office. All this sounds like a scene straight out of a sci-fi movie, but this is very much possible now, thanks to technological advancements and the advent of the Internet of Things (IoT), Industrial Internet of Things (IIoT), and Artificially Intelligent Systems. The Internet of Things is a network of devices that can communicate via built-in mini computers. Intelligent devices like voice assistants, talking eyewear, and self-mowing lawn robots, are meant to make our lives easier, but they also collect our personal information. Security analysts say the number of cyber-attacks on IoT devices is rising. Between January and June, 1.51 billion IoT breaches occurred. Cyberattacks on IoT devices more than doubled year over year in the first half of 2021.

Security and privacy are the most important problems for the Internet of Things. Consider the possibility that someone with access to your smart home system may remotely unlock the door and commit theft or lock you out of your own home. The possibilities seem endless and should not be taken lightly. Before making a decision, people should assess how much smart technology they need in their homes. When hackers gain access to one device on a network, they gain access to all other unprotected devices on the network. They can reprogram those devices to launch new attacks, making it even more essential to understand the technology behind the Internet of Things.

Ordinary users cannot see the data that is collected and transferred. The same is true for the software built into their gadgets, so the main issues are who has access to the data collected and, in the worst-case scenario, who can remotely control the smart devices. Also, security gaps make the entire network of IoT devices vulnerable. This article mainly focuses on emerging technology like IoT and related security issues and ways to mitigate the same.

So, what is IoT ? [7] IoT is a collection of rapidly evolving technology that interacts with the physical world. IoT is the combination of IT Information Technology and OT Operational Technology. The improvements in cloud computing, mobile computing, big data, hardware manufacturing, and other technological advances gave way to the birth of IoT. IoT provides computing, data storage, and network connectivity for equipment, enabling new remote access for monitoring, accessing, and troubleshooting. With the advent of smart vacuum cleaners, your house stays clean all the time, without you even having to think about it. You can remotely monitor activities going on in your home from anywhere on the planet with just your smartphone in hand. IoT devices have applications that are useful in numerous sectors of society, not just in households. These devices are used by the medical industry to monitor patients and provide assisted living for the elderly.

While an IoT- enabled future appears to be a promising prospect, it is not without obstacles. Many aspects of IoT have become a reality, but there are far too many challenges to overcome before IoT becomes ubiquitous in industry and our daily lives. A few of the challenges and solutions to mitigate the risk are discussed in sections 2 and 3.

II. CHALLENGES AND RISK

1. **Data protection:** Because the data is essentially personal, the Internet of Things and its applications introduce new challenges to data privacy and people's ability to determine what information is gathered about them and how it is used. [8] The most typical causes of data security problems in IoT applications are insecure connections and data storage. One of the major concerns for IoT privacy and security is the ability of compromised devices to access personal data.

2. **Improper handling of cryptographic algorithms:** Cryptographic algorithms are needed to create security solutions that protect IoT network activities while lowering security concerns. [9] Cryptographic algorithms employ a sequence of mathematical operations to make attempts to compromise the findings so computationally expensive that they are impossible or impractical to complete in time for the attacker to be helpful. Furthermore, a resource-constrained IoT device will have difficulty performing a software implementation without jeopardizing the device's basic functionality. However, due to the computational and energy limits of IoT end devices, the actual performance of such cryptographic methods is hampered.

3. **Risk associated with old network architecture:** A misinterpretation of standards and best practices and a poorly managed network pose the greatest threat to network security. [10] Knowing that communication paths are unsafe is preferable to not knowing them from the standpoint of security design. Over time, ad hoc updates and particular changes to hardware and machinery without consideration for the broader network impact have become more common. This form of sustainable growth has resulted in network expansion errors and wireless connectivity without concern for the effect on the original security architecture.

4. **Risk with legacy applications:** Today's cyber threats are likely to be vulnerable to applications not developed with cloud connectivity in mind. [11] Cyberattacks are becoming more complex, and a breach of an IoT device could violate a legacy system that isn't secure.

5. **Lack of awareness in users:** Users have gained a lot of knowledge about privacy and security over time, but many are still unclear about the hazards posed by IoT. [12] As a result, manufacturers, consumers, and organizations may be concerned about the security of IoT devices. Both individuals and IoT devices are targets for hackers. Some people have a rudimentary understanding of electronics. As a result, people participate in activities without thinking about the consequences.

6. **Lack of a robust management system:** Many companies lack a robust management system that can track activity and alert them to potential risks. [13] An organization cannot identify potential intrusions without this type of technology.

7. **Man in the middle or device spoofing:** An attacker will place themselves between the IoT device and the cloud or network and send data as if the IoT device was sending it. [14] This is a significant concern since the attacker could alter production-related data or get access to confidential information. The following section sheds some light on some of the items that appeared to be excellent but had significant security issues. Padlocks with a smart key in which to unlock these smart padlocks, a fingerprint scanner was utilized instead of a key. Figure 1 depicts the product image. After reverse engineering, it was revealed that the Bluetooth MAC address of the device in question, which is transmitted out by the device, is the key to unlocking them.

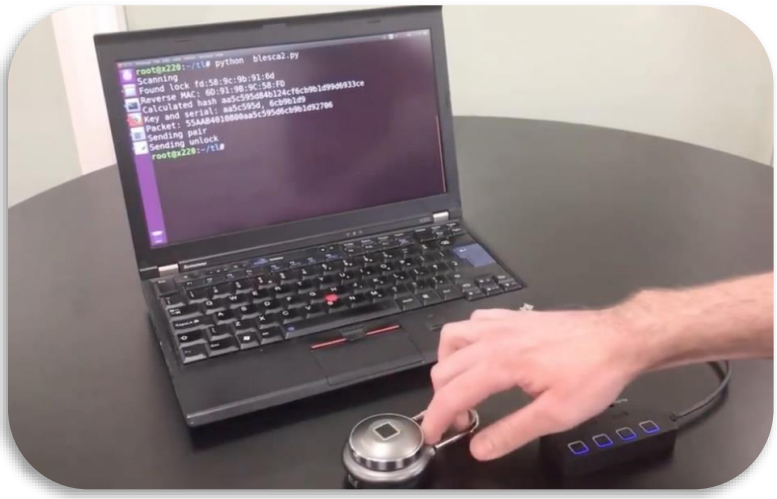

Figure 1: Tapp Padlock [1]

Cayla (interactive toy) [2]: This toy is an interactive toy that can initiate a conversation with young children. The product image is shown in Figure 2. It has a microphone, a speaker, and Bluetooth that connects to your cell phone. The Bluetooth built into this toy did not have password encryption, effectively allowing anyone in the neighborhood to link to this device and spy on your kids. The toy can be made to swear by a simple change to the software. For this reason, this toy has gained popularity as “the swearing toy”. These concerns were raised, and this toy was quickly withdrawn from the markets of many countries.

Figure 2: Cayla (Interactive Toy) [2]

The iKettle 2.0[3] from Smarter allows users to boil water with a single click on their smartphone. Figure 3 depicts the product image. The WIFI password was simply given to the attacker with just one command while hacking this kettle, which was proven to be a severe security issue. As a result, an attacker can gain access to the network and intercept all data/money transactions, potentially compromising all other devices on the network. Fortunately, the producer discovered the flaw and corrected it in subsequent product models.

Figure 3: Smarter's iKettle 2.0 [3]

The list is limitless; everything is a threat/risk, from botnet attacks to DDoS attacks, and we need better security standards to counteract them. We'll talk about risk mitigation techniques in the next section.

III. APPROACHES TO MITIGATE THE RISK

1. **Have a plan of action:** Security is not something that should be done on the spur of the moment. Organizations should create a phased approach with tasks assigned to the right people. An audit of the infrastructure, for example, could be a good place to start to compile a list of what devices the organization has and determine whether any shadow IT devices are present on the system. Having a Plan of Action will help control the damage caused by an attack.

2. **Upgrading/patching legacy software and applications:** Although it is never a good idea to ignore or postpone a security update, several attackers have been able to effectively breach an environment using a known exploit for which a patch is already available. [15] However, as more IoT devices are added to the infrastructure, keeping everything up to date, much alone staying informed about security alerts and fixes, becomes increasingly difficult. Repairing on the fly isn't enough, nor is it organized enough, to ensure that you're fully aware of and patching all of your network's security flaws. It's critical to set up a strategy for patching and updating to ensure that it doesn't fall by the wayside. Some networked devices tend to fade into people's consciousness. In most people's view, a printer isn't considered connected equipment. It's pretty common to see older PCs connected to devices running operating systems like Windows XP or Windows NT in many industrial and healthcare settings. Legacy devices and applications should be patched with security updates or upgraded if feasible. Regularly scanning your

system using a vulnerability assessment solution is one of the quickest ways to discover what vulnerabilities may be affecting it.

3. **Data protection:** To deal with the data protection problem, cryptography is a good option. [16] In the event of unlawful access or theft, data encryption keeps information hidden. It's widely used to protect data in transit, and it's becoming more popular for data protection at rest. Data encryption and decryption ensure data privacy and confidentiality, as well as lowering the danger of data theft It's a good defense against eavesdropping

   (also known as sniffing) attacks, which occur when a cybercriminal passively examines data as it's transferred or received over a network.

4. **Deception technology [4]:** Deception technology is one technique to solve these inherent issues and detect an assault quickly. To confuse the attacker, organizations use decoys and lures that appear to be genuine IoT assets, as well as various forms of misdirection that steer the attacker away from real assets by supplying them with incorrect information. Simply touching one of these decoy assets discloses the attacker's presence, alerting the security team as soon as they are touched. These misleading assets divert the adversary's attention away from anything of real value, allowing them to protect true assets while wasting time in a decoy environment. Simultaneously, the deception engagement servers document their tactics, methods, and procedures (TTP) to better inform defensive measures and gain vital knowledge, such as the vulnerabilities and exploits that attackers employ. This is visually represented in Figure 4.

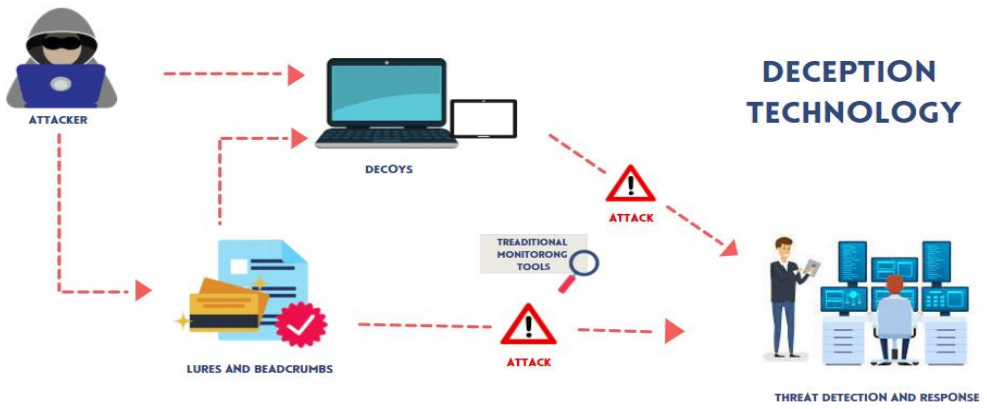

Figure 4: Illustration of Deception Technology [4]

5. **Securing home networks and devices:** For Home IoT Networks and Devices, one should start by securing the Router. [17] Basic things like using a strong encryption method like WPA for Wi-Fi-Access or using a guest network to share Wi-Fi with visitors can help limit the risk. A unique password should be used for each of your IoT devices. Hackers usually get access to a network by breaking into one device and then attempting to expand their control to other devices. If all of your IoT devices have different names, a hacker will have a difficult time spreading their footprint in your IoT network. The permissions should be checked, if you don't want something captured or stored, disable the permissions to prevent access.

6. **Solution for the issue related to cryptographic algorithms:** Modern cryptographic algorithms are extremely resistant to attack when properly implemented; their only weakness is their keys. However, if a key is compromised, it can have unforeseen consequences. Cryptographic keys, as a result, are among the most valuable assets, and they should be treated as such. The value of any key is equal to the entire value of all the data and/or assets it safeguards. One of the solutions suggested by the authors of [18] is asymmetric encryption of public key can be used to encrypt the symmetric encryption key

   The symmetric encryption key is decrypted using the private key by the recipient. The only time asymmetric encryption/decryption occurs is when the keys are exchanged, hence it doesn't require a lot of CPU power (ideal for IoT/IoE applications).

7. **Regularly testing the systems:** Putting your IoT security strategy to the test is the best way to learn about it. [19] Penetration testing can show how an attacker could utilize IoT to obtain access to sensitive data by abusing an organization's infrastructure. Penetration tests can also be used to validate repair efforts and ensure that any security measures implemented are effective. You can, for example, check the status of a recently added patch. While a vulnerability scanner may have detected it, it may not be working because the system hasn't been rebooted. Periodic testing ensures that companies keep one step ahead of the game by identifying and correcting security flaws before a threat actor exploits them.

8. **Solutions that detect compromised devices:** Finally, since many IoT devices lack standard antivirus, focusing solely on prevention is insufficient. [20] In reality, the difficulty isn't just keeping threat actors out; it's about promptly identifying and removing those who have gotten in. The more time an infection is in a network; the more harm it can cause. Rapidly detecting threats with tools like Network Traffic Analysis (NTA) solutions helps limit the amount of damage.

IV. CONCLUSION

The risks and issues that have emerged as an integral part of IoT devices have been covered throughout this article. When it comes to IoT gadgets for your home, a few extra conveniences could put you in serious trouble. If you're thinking about purchasing an IoT gadget for your house, think hard about what you're getting yourself into and the potential threats you'll be exposed to. It's probably advisable to stay away from IoT devices as much as possible because they're still not secure enough for the times we live in. When it comes to IoT devices in large sectors and enterprises, you must have a thorough understanding of all devices and ensure that none of them are left unattended.

REFERENCES

[1] https://www.forbes.com/sites/thomasbrewster/2018/06/13/tapplock-smart-lock-hacked-in-2-seconds
[2] https://www.bbc.com/news/world-europe-39002142
[3] .https://www.pentestpartners.com/security-blog/new-wi-fi-kettle-same-old-security-issues-meh/
[4] https://foresite.com/deception-technology-fooling-the-enemy/

[5] Hasan, M.K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y.A., Nafi, N.S., Ciro Rodriguez, R., Vargas, D.E.: Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things Applications. Complexity 2021, 5540296 (2021)
[6] Chanal PM, Kakkasageri MS. Security and privacy in IoT: a survey. Wireless Personal Communications. 2020 Nov;115(2):1667-93.
[7] Abomhara M, Køien GM. Security and privacy in the Internet of Things: Current status and open issues. In 2014 international conference on privacy and security in mobile systems (PRISMS) 2014 May 11 (pp. 1-8). IEEE.
[8] Madakam S, Lake V, Lake V, Lake V. Internet of Things (IoT): A literature review. Journal of Computer and Communications. 2015;3(05):164.
[9] Fernandes E, Paupore J, Rahmati A, Simionato D, Conti M, Prakash A. {FlowFence}: Practical Data Protection for Emerging {IoT} Application Frameworks. In25th USENIX security symposium (USENIX Security 16) 2016 (pp. 531-548).
[10] Surendran S, Nassef A, Beheshti BD. A survey of cryptographic algorithms for IoT devices. In 2018 IEEE Long Island Systems, Applications, and Technology Conference (LISAT) 2018 May 4 (pp. 1-8). IEEE.
[11] Vishwakarma R, Jain AK. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems. 2020 Jan;73(1):3-25.
[12] Brou P, Janssen M. Effects of the internet of things (IoT): A systematic review of the benefits and risks.
[13] H. Mikusz M, Houben S, Davies N, Moessner K, Langheinrich M. Raising awareness of IoT sensor deployments.
[14] Awan KA, Din IU, Almogren A, Guizani M, Altameem A, Jadoon SU. Robusttrust–a pro-privacy robust distributed trust management mechanism for the internet of things. IEEE Access. 2019 May 13;7:62095-106.
[15] Gu T, Mohapatra P. Bf-iot: Securing the iot networks via fingerprinting-based device authentication. In2018 IEEE 15Th international conference on mobile ad hoc and sensor systems (MASS) 2018 Oct 9 (pp. 254-262). IEEE.
[16] Ray S, Basak A, Bhunia S. Patching the internet of things. IEEE Spectrum. 2017 Nov 2;54(11):30-5.
[17] Ziegler S, editor. Internet of Things Security and Data Protection. Cham: Springer International Publishing; 2019 Mar 19.
[18] Lastdrager E, Hesselman C, Jansen J, Davids M. Protecting home networks from insecure IoT devices. InNOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium 2020 Apr 20 (pp. 1-6). IEEE.
[19] Singh S, Sharma PK, Moon SY, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. 2017 May 24:1-8.
[20] Beilharz J, Wiesner P, Boockmeyer A, Pirl L, Friedenberger D, Brokhausen F, Behnke I, Polze A, Thamsen L. Continuously Testing Distributed IoT Systems: An Overview of the State of the Art. arXiv preprint arXiv:2112.09580. 2021 Dec 17.
[21] Van der Elzen I, van Heugten J. Techniques for detecting compromised IoT devices. The University of Amsterdam. 2017 Feb 12.

