International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 5.449, Volume 03, No. 02(II), April- June, 2023, pp .09-18

5 WAYS TO BECOME A SMART USER OF SMART DEVICES

Dr. Vandna Bhalla*
Mrs. Pratibha Gupta**

ABSTRACT

Digital devices are an indispensable part of our daily life and smart devices have ` to it, computing everywhere. We have Voice Assistants, Alexa, Smart A.C., Smartwatches, RFID cards etc. All such Smart devices have access to users' personal data, health records and financial data. A standalone device like a conventional T.V., wristwatch etc. poses no cyber-attack threat but a smart device, when connected to the Internet, makes data accessible to smart device at risk.It is like opening a new door for a hacker to intrude in. Users know little about the security vulnerabilities in IoT devices. Hackers can exploit this vulnerability; people's sheer negligence give access to sensitive data and result in threatening cyber-attacks. During the 2016 US Presidential election the MIRAI botnet, consisting of millions of infected IoT devices attacked the DNS provider for Twitter, GitHub and other major services, the world's largest DDoS attack to date. Mozi botnet infects IoT devices by exploiting Telnet default login credentials, and the botnet owner triggers Distributed Denial of Service attack. It mainly targets home routers and DVRs.In this paper, we create awareness about more such common vulnerabilities in IoT devices and propose some simple and effective ways on how to combat these vulnerabilities for safe and secure use of IoT Devices. We also share the data analysis from a survey form which gives insights into how common people are not only unaware about these threats and risks but are generally negligent/careless about small little techniques to fortify their presence on the Internet.

Keywords: *Availability, Combat, Confidentiality, Integrity, IoT, Mitigation, Security, Sensors, Smart Device, Vulnerability.*

Introduction

The Internet of Things popularly called IoT is a set-up that interconnects common objects, devices, and sophisticated smart tools like sensors, cellular devices, smart security systems and smartwatches. This new technology is permeating the modern world from industry to enterprise to end users [1].These devices have software embedded to enable connections with each other and to exchange data. IoT device refers to an electronic or mechanical device with sensors, actuators, and microcontrollers. Sensors, actuators and microcontrollers give them computer-like capabilities i.e. input, processing, output and ability to communicate over the network. The IoT devices can be categorized into two main groups- Sensors (these basically collect data and forward it over to another device) and Switches (these remit commands). We are surrounded by smart devices at home, employees wearing RFID cards at the workplace, and health gadgets for the elderly [2]. The benefits are many like comfort and ease, energy efficiency,and can be controlled from anytime anywhere, to mention a few. IoT has a huge application area in health care where the patients are monitored remotely.A smart fridge can order milk as soon as the need arises. Lights are switched on as soon as an employee enters the office premises. Users can check images online of smart house cameras. All these smart devices have access to personal data, financial data and health records.

[*] Associate Professor, Department of Electronics, Sri Aurobindo College,Delhi University, Malviya Nagar, New Delhi, India.

[**] Assistant Professor, Department of Computer Science, Sri Aurobindo College,Delhi University, Malviya Nagar, New Delhi, India.

Due to the small size of the microcontroller, data is usuallystored in the cloud. Data is vulnerable while in transit and at third-party maintained clouds. IoT security is at risk by a vulnerable device which may unwittingly permit access to cyber criminals [3]. This can jeopardize user credentials, critical data etc. compromising the security of the entire system and its users. It can cause serious disturbance in operations or even human lives can be endangered. According to Kaspersky, the security and antivirus service provider IoT cyber-attacks were over double in the first half ofthe year 2021[4]. Most of these are due to a lack of adequate/requisite security protocols. New technologies like edge computing and AI are presenting a galore of opportunities but at the same time, they are convoluting the data and cyber security landscape. Most of these strikes are preventable with little effort and some cognizance and awareness.

This paper reviews common IoT device usage vulnerabilities and safe and easy-to-remember ways to combat these vulnerabilities[5]. As IoT is the latest buzzword, a lot of existing research work is there on IoT device security and privacy issues. Baho [6] discusses security vulnerabilities in IoT devices at different layers. For the application layer,the most common vulnerabilities include weak authentication procedures, unpatched firmware, devices configured as Universal Plug and Play(UPnP), interconnected IoT devices etc. “User awareness and education regarding the purchase and use of IoT devices” [7] is paramount andour research is a step in this direction. The approaches suggested are simple and easy to remember. The development of specific educational resources [8] will be beneficial in the long run. This paper specifically talks about usage vulnerabilities in general and presentsfive simple and effective ways of mitigation.

IoT Security

Information Security goals of confidentiality, integrity and availability as shown in Fig. 1, the CIA triad. These are also applicable in IoT devices. Confidentiality means that information is accessible to authorized users only and generally implemented via user id and password. Integrity refers to the correctness and completeness of the information. Availability means information is available as and when requested. The intersection of the three goals isthe secure information. [9]

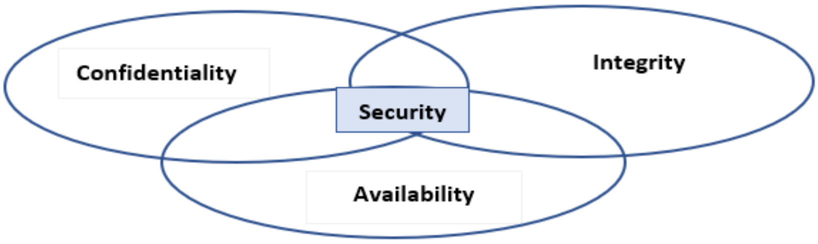


Fig. 1: CIA Triad

There must be a perfect balance between all three for safe, secure, and usable communication. However, manufacturers of IoT devices in order to provide 24*7 availability have made the confidentiality process very simple. If it continues, then the integrity of information is at potential risk.

IoT devices have access to users’ personal and confidential data and given the small size of microcontrollers inside smart devices, this data is stored in the cloud. Though data is stored in encrypted form, having access to large amounts of encrypted data from a particular user is a boon for malicious intruders. IoT devices have been interconnected for efficiency, accessibility, and usability and have a galore of applications. Smart homes are energy efficient by automatically reducing the load depending on usage. Health practitioners can access real-time vital parameters of patients via the in-house Internet of medical things. Voice assistants have found essential usage in the busy lives of users. Device interconnection, connected on the same network further increases the amount of vulnerable data, available for interception[10].

Vegas Casino Fish Tank Heist is an example of hackers entering the casino network through an IoT thermostat installed to maintain the temperature inside a high-tech fish tank kept on the casino premises. The hackers cracked the weak authentication procedure of the thermostat, entered the network, located sensitive data of the casino stored on the cloud and passed it out through the thermostat [11]. A similar analogy is shown in Fig. 2. It depicts a Voice assistant, Smartphone, Smartwatch all connected on the same network. We have a set of heterogeneous IoT devices, from a device storing highly sensitive data like a smartphone having user contacts, bank account details, UPI pins etc., to a device storing least sensitive data like a smartwatch countinguser steps, alarms etc. The devices are interconnected on the same network. Compromising a smartwatch is easy as users generally keep a simple authentication process which can be cracked. One device hacked allows access to other interconnected devices and the underlying connecting network. Now the hacker, once inside the network, can intercept all traffic that is being sent on the network and can access data that is stored on the cloud. The intruder can extract data from the cloud to his machine. The intruder can also download and run a malicious payload tolaunch a DDoS attack[12].

Fig. 2: Interconnected IoT Devices

The small size of the IoT device microcontroller, lack of security standards and user unawareness about cyber security protocols to be followed while using IoT devices lead to IoT device data being vulnerable.“Great power comes with great responsibility” this Stan Lee proverb is rightly applicable in today’s world of interconnected devices. Severe security protocols violation in IoT devices may make us Zombies controlled by these hacked IoT devices.Weak/Hardcoded passwords, Insecure Updating Mechanisms, Networks, Components, Data Transfer/Storage, Default settings and Ecosystem Interfaces are some of the IoT risks that can compromise the devices. The next section discusses the common IoT vulnerabilities[13].

Common IoT Devices Vulnerabilities

Despite advancements in technology, cyber criminals adapt quickly to security updates and continuously bring susceptibility. There were 1.5 billion IoT cyber-attacks reported in the first half of the year 2021. Fig.3 lists the various types of cyberattacks in 2022 [14].

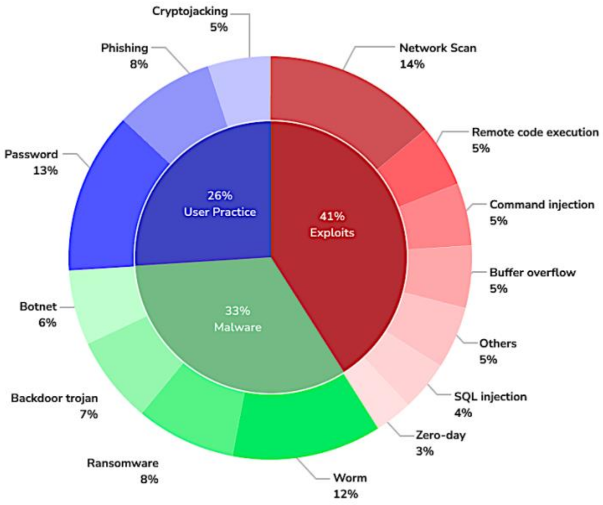
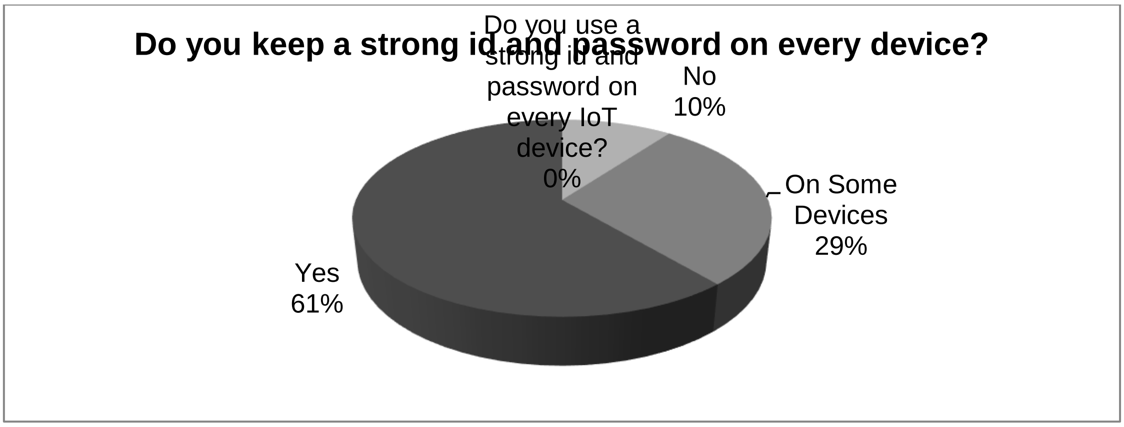


Fig. 3: Breakdown of top IoT threats

A typical IoT device lacks the much-needed in-built mechanism to counter security attacks. Highly sophisticated cyber-attacks have been launched by breaching devices on IoT due to common vulnerabilities. Due to their minimal computational capability, there is very little space for resilient data security and protection. Also, these devices use diverse technology for transmission which further makes it difficult to implement appropriate robust security protocols and methods. The elementary components of these devices are pregnable which renders millions of these smart devices open to strike. The users from big organizations are the largest security threats. Lack of awareness and not implementing the best practices puts IoT devices exposed to attacks. We present some of the common vulnerabilities.

Weak Authentication Procedure

Almost all IoT devices come with an authentication procedure generally implemented through login id and password but people due to sheer negligence keep it to default, reused or weak passwords or common passwords. These are usually very easy to guess as they are short and simple. These are easy for cyber criminals to crack and the device is compromised which leads to a big-scale attack(s). Size limitations and cost constraints keep biometrics out of reach. This weakness provides intruders with an easy way to get access to the device. One device access allows access to other connected devices of the same user and the underlying network. Mirai DDoS attack is an example of exploiting this vulnerability [15]. Mirai scrutinized the Internet for victims and violated security by attempting default password and username combinations. And in a very short time, Mirai infected hundreds of thousands of IoT devices around the world.A Google form related to the use of IoT devices by common people was developed by us to ascertain the prevailing level of information/awareness. We collected over 100 responses, out of which 90% admitted they use an IoT device, 10% of such students admitted that they do not keep strong passwords and 20% accepted the fact they keep the same password on different devices as shown in Fig. 4. The survey responses ascertain the fact that generally usersdo keep weak, same or default passwords. This is still prevalent despite various awareness campaigns.



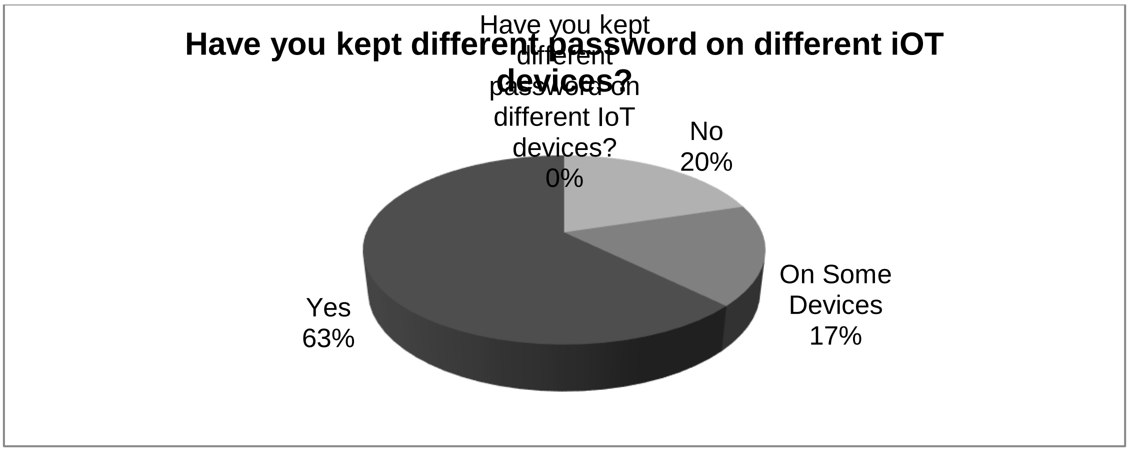


Fig.4: Weak, Same Passwords in IoT devices

The 64K Transport Layer Ports that open by default on a single IoT device

Once the internet connection of a device is open, 65536 ports are open on that device, provided for accessing different services on different ports simultaneously. Port 20,21 for FTP, port 80 for HTTP, port 443 for HTTPS, Port 25 for Email and Port 3389 for RDP Remote Desktop Protocol. An intruder can perform port scanning, find open ports and can passively listen on any open port without user knowledge. For example,an intruder can connect to port 3389, if left open and get access toa device which was meant for employees working remotely.The intruder can intercept user id and password information that is being shared on the network, and use this for session hijacking, and man-in-the-middle attacks. The hacker can download and run malware on infected devices causing DDoS attacks.

Intruders can enter from a Less Sensitive Device

IoT devices are being interconnected for providing 24*7 connectivity. This has a disadvantage as well, as a small open window can make the whole house's security vulnerable. A simple IoT device smart watch if compromised can put a sensitive device like a smartphone at risk. UPnP protocol if enabled on the Wi-Fi router allows any device to open a port on the router and act like a server. Hackers once inside the network by exploiting weak authentication procedures, can take advantage of UPnP protocol on routers and run malicious payload scripts causing DDoS attacks.[12]50% of respondents accepted that they have synchronized IoT devices on their smartphones as shown in Fig.5. If a malicious intruder is able to enter a less sensitive device by exploiting 2 or 3 vulnerabilities, he can access data stored on a sensitive device i.e. smartphone as well. The vulnerability is prevalent and confirmed.

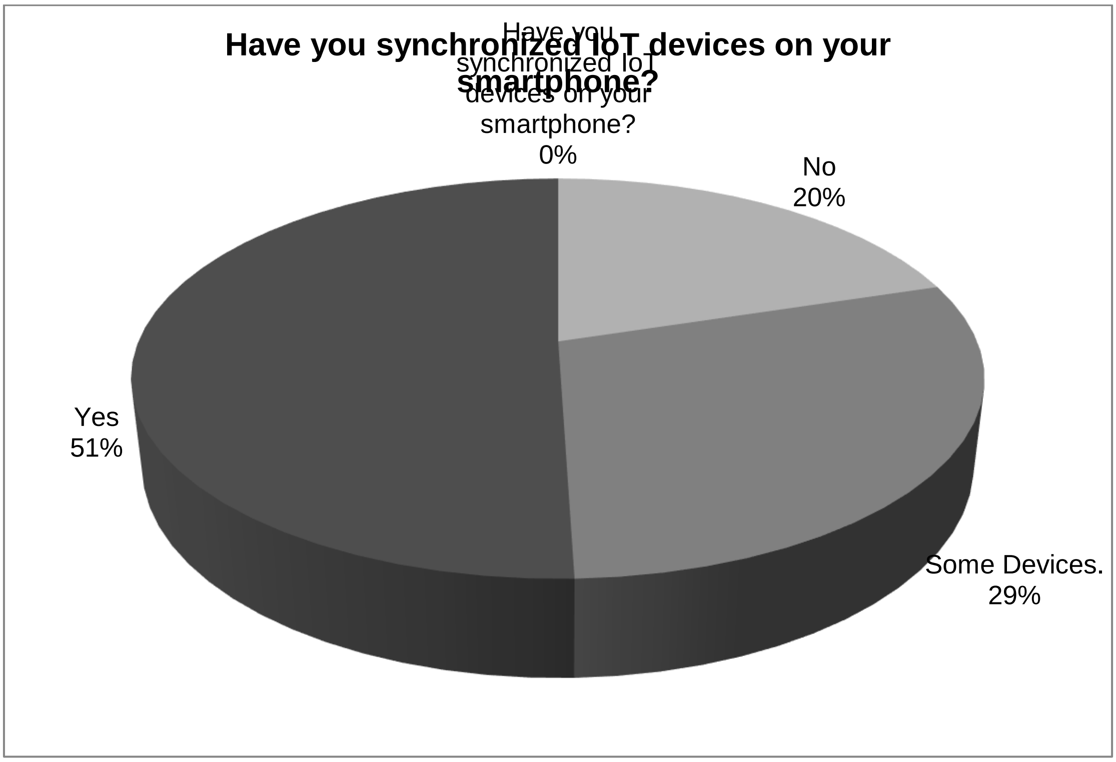


Fig. 5: IoT Device Synchronized on Smartphone

Lack of updates on IoT Device Firmware

We have a wide range of IoT devices smart refrigerators, voice assistants, and smart AC from different manufacturers. There are yet more manufacturers of microcontrollers and firmware installed on these microcontrollers. Security protocols among different OEMs have not been standardized. Vulnerabilities if any are reported, the companies do not send updates to the end user and users are also lazy to promptly update devicesoftware.

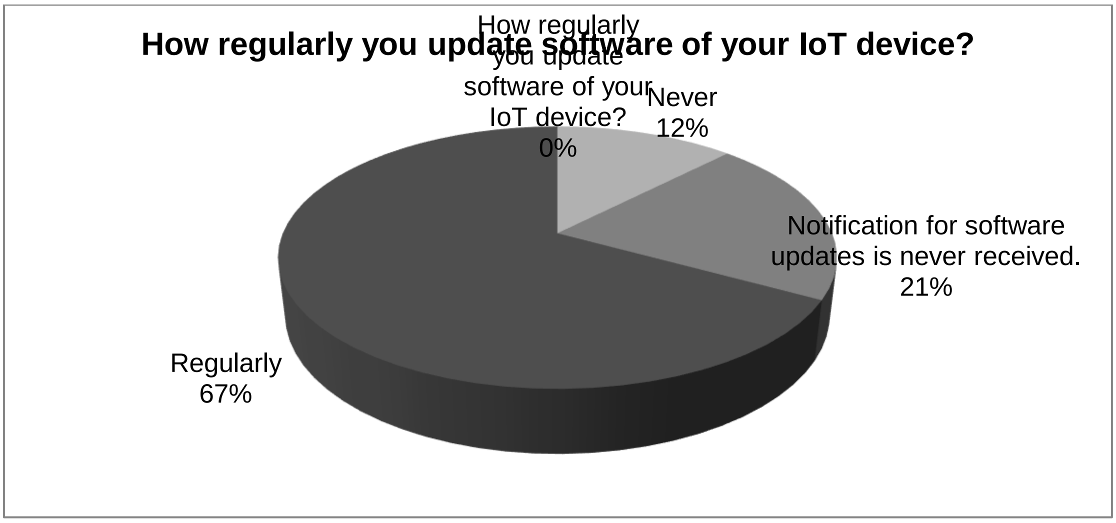


Fig.6: Firmware update on IoT Device

Almost 21% of respondents admitted that they never receive notifications for software updates and IoT devices they are using and 12% admitted they never update their IoT device software as shown in Fig.6. This again verifies the vulnerability that IoT device software is not updated regularly.

Physical Attack

The users are careful about the security of sensitive devices like smartphones and laptops, whereas careless about other IoT devices like smart toys, smart watches etc. So their physical security is often ignored. An intruder who has physical access to the device can view the credentials, create a new user password and change some security settings like disabling the firewall. This may lead to unauthorized access to the network.34% of respondents admitted that they keep only smartphones and laptops safe from physical attack and 10% admitted they do not keep IoT devices safe from physical attack as shown in Fig.7. This further confirms the vulnerability.

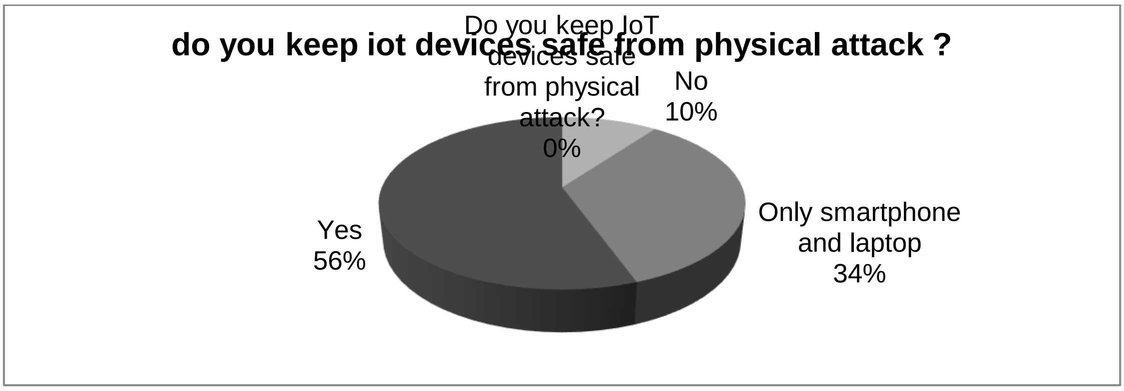


Fig. 7: Physical Attack on IoT Device

Data is Vulnerable due to storage on the cloud

The small size of IoT device, lack of expertise in data storage of manufacturing company, and competitive pricing models encourages companies to store data generated while using IoT device on the cloud. The cloud may be owned by a third party. Both manufacturer and user may not be aware ofthe security aspects of data. The cloud server may allow access to data stored without proper authentication/authorization.

These are some of the most common vulnerabilities on IoT devices. IoT devices have definitely improved quality of life by making users in charge of the device from anytime anywhere but users as well as manufacturers need to work on designing strong control mechanisms for removing or minimizing the impact of these vulnerabilities to completely eliminate any cyber security threat. [16]

Techniques to combat the security vulnerabilities

5 ways to become a Smart user of Smart devices

To mitigate risks and to be secure against common IoT devices' vulnerabilities, we propose five S-M-A-R-T techniques, Fig.8. These steps can be followed by a user without requiring training or expertise in security.

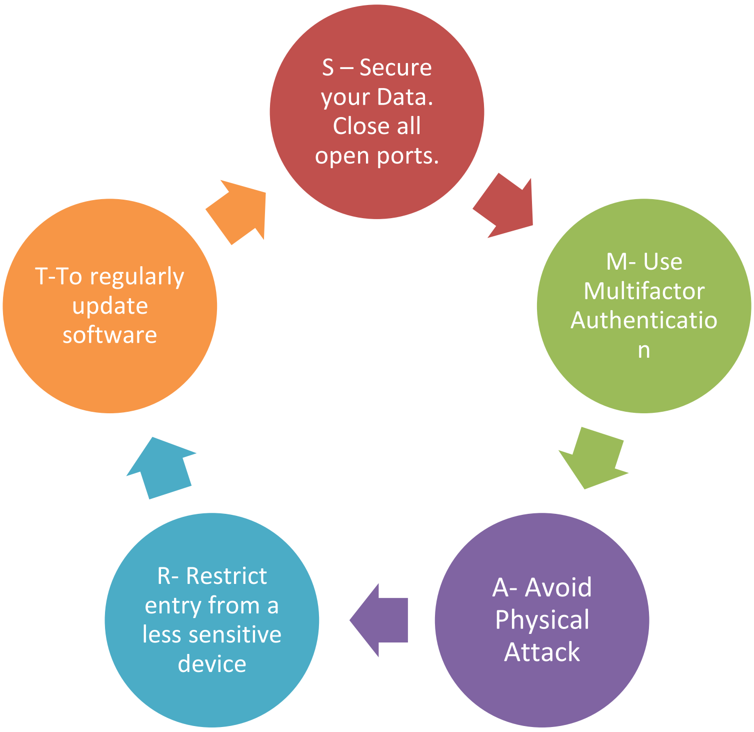

S – Secure your Data. Close all open ports.
M- Use Multifactor Authenticatio n
A- Avoid Physical Attack
R- Restrict entry from a less sensitive device
T-To regularly update software

Fig. 8: S-M-A-R-T Techniques

These SMART strategies are discussed in detail below:

- **S – Secure your Data. Close all open ports**

Retain only the needed services (& corresponding network ports) and close others. Keep such IoT devices on a private network, inaccessible from the internet. Ifthe need arises to connect the network to the internet, then enable Firewall on the router: If data encryption is supported by such devices, then configure to use that also to further fortify,[17] [18] [19].Data can be encrypted while stored on the cloud. As described in the previous point, as far as possible, avoid putting personal data (email, phone etc.) and instead put in temporary/secondary email, phone, and One-time credit card, [20].The common network Wi-Fi router must disable UPnP (Universal Plug and Play),[12].

- **M- Use Multifactor Authentication**

To mitigate the risk of weak passwords, it must be mandatory for the user to create strong and unique passwords consisting of a combination of upper- and lower-case letters, numbers, and symbols. Two-factor authentication should be implemented wherever possible to add an extra layer of security. These are all the more significant for when the biometric sensor is too costly to be provided on the device, [18], [19][21].

- **A-Avoid Physical Attack**

A poor or weak password is one of the biggest challenges today. This is despite constant reminders by all online accounts that we need to create strong passwords. One way of securing against this type of attack is to change passwords very frequently, like daily or every week. Keep strong and difficult-to-guess answers, required when the Forgot-password option is chosen. Do not continue with default passwords or easy-to-guess options Do not configure your personal email in the device settings, instead use some other email, configured to forward to your primary email, [16] [22].

- **R-Restrict Entry from a Less Sensitive Device**

A firewall would prevent access to the less sensitive device from outside. If the firewall isn’t there, then limiting access at every point will help. For example, the less sensitive device is allowed to post or query or access services on other devices, limiting to what is absolutely necessary for it to function properly. If possible, alternatively, the less sensitive devices can be added to another network, which is not connected to the main devices [16].

- **T-To regularly update software**

This can be done using a two-pronged approach:

- Making end-users knowledgeable about the importance of regularly updating their devices as soon as security updates become available.
- Create a Security Notification Service which end-users can subscribe to. End-users will register their devices with this service. This service will be responsible for finding out whether there is a pending update which has not been applied, or is the device made End-Of-Life by the manufacturer, or whether has there been any threat reported in the recent past for the same software version of the device.[16]

Outdated Technology in fact presents many risks like incompatibility issues, low productivity due to unreliable software performance, data loss when the software fails, OS bugs besides an easy avenue for cyber criminals.

Conclusion

IoT devices are surely a silver lining in today’s busy lives, but proper care must be taken for their safe and stringent use. In this paper, we identified common user vulnerabilities in IoT devices. We discussed how a single compromised IoT device can act as a trampoline to launch a bigger attack on other devices in the same network. The wide existence of these vulnerabilities is supported by Google survey form responses as well. Recent large-scale DDoS attacks have been triggered by exploiting these vulnerabilities only. The peer-to-peer Mozi botnet [23] works by taking advantage of the unpatched vulnerabilities and conducts data exfiltration, DDoS attacks and payload or command execution Fig. 9.The proactive defense for this also is ensuring devices are up-to-date, patched and strong passwords practices [24]. The strategies proposed in this paper for mitigating many such vulnerabilities are from the literature and are strongly recommended, simple and effective. We refer to those five steps as SMART strategy and feel that every SMART user must follow these to have a safe and secure experience in the World of IoT.

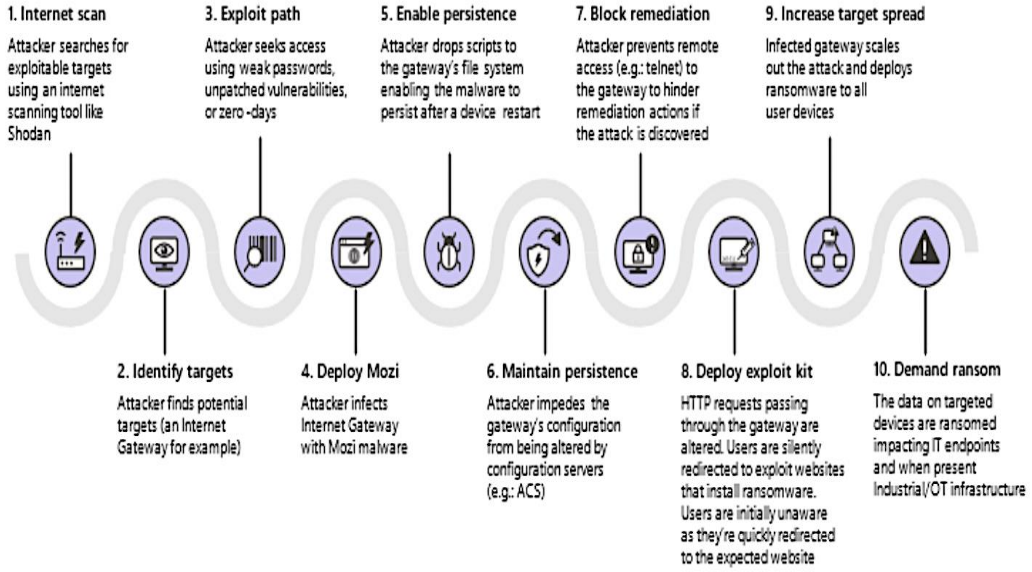

1. Internet scan
Attacker searches for exploitable targets using an internet scanning tool like Shodan
2. Identify targets
Attacker finds potential targets (an Internet Gateway for example)
3. Exploit path
Attacker seeks access using weak passwords, unpatched vulnerabilities, or zero -days
4. Deploy Mozi
Attacker infects Internet Gateway with Mozi malware
5. Enable persistence
Attacker drops scripts to the gateway's file system enabling the malware to persist after a device restart
6. Maintain persistence
Attacker impedes the gateway's configuration from being altered by configuration servers (e.g.: ACS)
7. Block remediation
Attacker prevents remote access (e.g.: telnet) to the gateway to hinder remediation actions if the attack is discovered
8. Deploy exploit kit
HTTP requests passing through the gateway are altered. Users are silently redirected to exploit websites that install ransomware. Users are initially unaware as they're quickly redirected to the expected website
9. Increase target spread
Infected gateway scales out the attack and deploys ransomware to all user devices
10. Demand ransom
The data on targeted devices are ransomed impacting IT endpoints and when present Industrial/OT infrastructure

Fig. 9: Mozi Botnet: Flow of Attack

It's very much recommended that passwords chosen be strong and not easy to guess. Abstain from choosing common and simple combinations. Install firewalls to protect stored as well as transferred data. Do not use outdated/obsolete software as it is a fragile link in IoT security. Regularly update software and upgrade whenever required. Actually, these concerns of security vary depending on the industry/application where the IoT is implemented. Health care pivots around safeguarding zero risk to life whereas smart cities need to ensure hackers do not manipulate operations and infrastructure. Such challenges make it more crucial to establish the various protocols at the network level. Botnet attacks can be prevented using advanced routers equipped with threat intelligence. All components sourced externally should have a security layer and follow standard encryption mechanisms.

Further research work needs to be done for the development of hardware and software standards for IoT devices. IoT devices are heterogeneous in the sense that devices from different manufacturers with a wide range of hardware and firmware are connected. For end-to-end security in this heterogeneous environment, the devices must follow standard security protocols. The user and manufacturer both need to work towards securing today's environment comprising a number of IoT devices. The user must follow security guidelines related to usage and the manufacturer must follow security protocols. Along with this, developers involved in firmware development need to explore new algorithms for deploying security. The devices may have a rating mechanism for safety guidelines being followed.

References

1. Mardiana binti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey, Computer Networks, Volume 148,2019,Pages 283-294,ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2018.11.025. (https://www.sciencedirect.com/science/article/pii/S1389128618307035)
2. 'IoT'. Accessed: Apr. 29, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things
3. https://www.firstpoint-mg.com/blog/iot-cyber-security-vulnerabilities/
4. IoT Cyberattacks Escalate in 2021, According to Kaspersky (iotworldtoday.com)https://www.iotworldtoday.com/security/iot-cyberattacks-escalate-in-2021-according-to-kaspersky
5. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, 'IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices'.
6. S. A. Baho and J. Abawajy, 'Analysis of Consumer IoT Device Vulnerability Quantification Frameworks', *Electronics (Switzerland)*, vol. 12, no. 5, Mar. 2023, doi: 10.3390/electronics12051176.
7. G. Nebbione and M. C. Calzarossa, 'Security of IoT application layer protocols: Challenges and findings', *Future Internet*, vol. 12, no. 3. MDPI AG, Mar. 01, 2020. doi: 10.3390/fi12030055.
8. 'IoT Consumer tips act of 2017'. https://www.congress.gov/115/bills/s2234/BILLS-115s2234is.pdf (accessed May 02, 2023).
9. 'CIA'. https://en.wikipedia.org/wiki/Information_security (accessed Apr. 29, 2023).
10. Sapna Sharma and Dr. Shikha Lohchab, 'Internet of Things: Challenges and Privacy Issues', *International Journal of Advanced Research in Science, Communication and Technology*, pp. 587–592, Apr. 2022, doi: 10.48175/ijarsct-3355.
11. "Smart Thermostat as a Part of IoT Attack May 2019", Accessed: May 06, 2023. [Online]. Available: https://www.researchgate.net/publication/332987980_Smart_Thermostat_as_a_Part_of_IoT_Attack
12. "Persirai: New IoT Botnet Targets IP Cameras", Accessed: May 06, 2023. [Online]. Available: https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html
13. E. Richa, 'IoT: Security Issues and Challenges', in *Smart Innovation, Systems and Technologies*, Springer Science and Business Media Deutschland GmbH, 2021, pp. 87–96. doi: 10.1007/978-981-15-7062-9_9.
14. https://securityboulevard.com/2022/10/top-7-iot-cyber-security-vulnerabilities-for-2022

15. ‘Mirai Botnet’, Accessed: May 03, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Mirai_(malware)

16. ‘OWASP’, Accessed: Apr. 29, 2023. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

17. ‘How to Enable Your Wireless Router’s Built-In Firewall’, Accessed: May 03, 2023. [Online]. Available: https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668

18. ‘Heightened DDoS Threat Posed by Mirai and Other Botnets’, Accessed: May 03, 2023. [Online]. Available: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

19. ‘Cybersecurity Awareness in IoT Threats’, Accessed: May 03, 2023. [Online]. Available: https://www.computer.org/publications/tech-news/events/cybersecurity-month-2020/awareness-iot-threats

20. ‘One Time Credit Card’, Accessed: May 03, 2023. [Online]. Available: https://www.congress.gov/115/bills/s2234/BILLS-115s2234is.pdf

21. ‘Authentication’, Accessed: May 03, 2023. [Online]. Available: https://yourtechdiet.com/blogs/seven-most-popular-strong-authentication-methods/

22. ‘Move to New Email Account’, Accessed: May 03, 2023. [Online]. Available: (https://www.techlicious.com/tip/move-to-new-email-account/)

23. ‘Mozi IoT Botnet’, Accessed: May 02, 2023. [Online]. Available: https://www.csk.gov.in/alerts/MoziIoTBotnet.html

24. https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/.

□❍□