Securing the Connected Home: Addressing Security Hurdles in IoT Smart Homes

Ridhu Shree V S
Keerti Dhanyaa R
Abinandhana V

Securing the Connected Home: Addressing Security Hurdles in IoT Smart Homes

ABSTRACT

Smart home systems use IoT devices which operate together, sharing consumer usage data among themselves and automates actions based on the one's instructions. This paper aims to explore security issues and elucidate the risks posed by data breaches, unauthorized access, and surveillance within smart home ecosystems. Thus, the objective of the paper is to highlight such problems and recommend a suitable solution.

INTRODUCTION

Smart Homes: Trusted and Secure Environments?

The Internet of Things (IoT) comprises a vast network of connected physical objects, programmed for specific applications within one's household, exchanging data with other devices and systems via the internet. From vacuum robots, to smart lock doors, the increased use of such technology has fundamentally changed contemporary lifestyles, transforming the way we interact with technology and the world around us.

According to research by IoT Analytics, the IoT market is projected to grow by 18%, and expected to reach 14.4 billion active connections in 2022. By 2025, it is estimated that there will be approximately 27 billion linked IoT devices.[1] However, along with this surge in connectivity, numerous security and privacy concerns have emerged that require attention. As more data is generated from these interconnected devices, it is crucial to recognize the potential risks associated with IoT-generated big data.

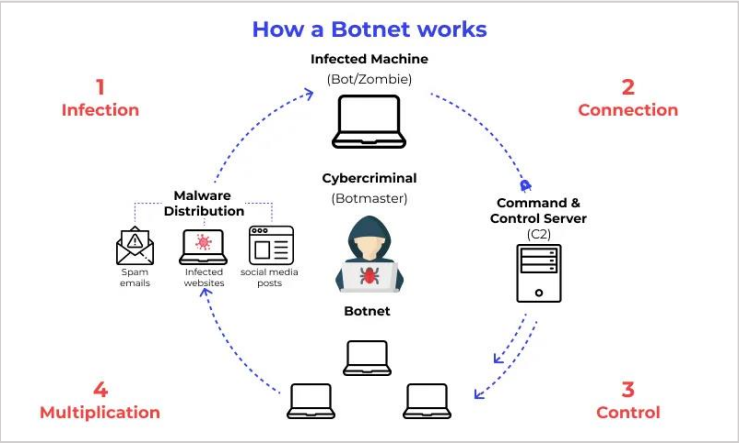
[1] Zenarmor, 2016

PROBLEM STATEMENT

The proliferation of IoT devices in smart homes has led to a surge in botnet attacks and privacy breaches. IoT devices come equipped with cameras, microphones, and various sensors, allowing them to monitor activities in the most private spaces of our homes, , including users' activities, behaviours, and preference. They can collect and store information about usage, habits, and preferences, posing potential privacy risks Additionally, since these devices are connected to the internet, they serve as potential entry points into the wider network containing sensitive data, making them susceptible to botnet attacks and data breaches, jeopardizing individuals' most sensitive information. Such vulnerabilities not only threaten sensitive information and privacy, but also potentially compromise the safety of individuals in a smart environment. Thus, the scope of this paper is to address the pressing challenges of botnet attacks, privacy breaches, and other security concerns in IoT smart homes, proposing effective solutions to safeguard users' privacy and security.

EXPLORING PROBLEM

1. Botnet attacks on IOT devices



An IoT botnet is a network of infected computers that is controlled by malicious attackers. They are usually created by installing malwares onto computers and controls C2 architecture of the network. 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.[2] Because of the generally low patch level of IoT assets, the most frequent attacks are exploited via long-known vulnerabilities and password attacks using default device passwords. Especially in weakly secured IoT devices, botnets can gain access into the required network. They can use different forms of C2 (command and control) to access data on social

[2] Team GRL, 2023

media or responses to DNS queries. A botnet's strength is determined by the quantity of devices that comprise it. They are usually managed by a single command-and-control (C&C) server that is linked to all of the compromised devices. However, some botnets employ peer-to-peer (P2P) networking, which makes it more challenging to shut them down.

The Mirai botnet attack of 2016 is one of the most horrendous cyberattacks, where millions of devices that were connected to IoT were all infected, with a peak traffic rate of 1.2 terabits per second. The malware, Mirai attacked IoT devices including routers, cameras and turned them into bots used for DDoS attacks. The attack targeted Dyn, a major DNS provider, and disrupted access to major websites such as Amazon, Twitter, Netflix, and GitHub.

IoT botnets are known for launching DDoS attacks (distributed denial of service) on target entities to interrupt their operations. There are many types of botnet attacks and causes for IoT to be prone to these attacks:

- DDoS attacks: the attacker floods the internet with traffic unable for the user to render information. These attacks can disrupt services, render websites inaccessible, and cause financial losses for businesses.
- Phishing: irregular patch updates and inefficient passwords are vulnerable to botnet attacks, which cause the system to be liable to phishing by sending out mass spam emails, increasing the scale of the malicious email campaign.
- Credential Theft: botnets may collect login credentials through techniques like keylogging or phishing. Stolen credentials can be used for unauthorized access to accounts, networks, or sensitive information, worsening security risks.
- Cryptojacking: Some botnets are repurposed for cryptocurrency mining, using hijacked devices' computational resources to mine digital currencies like Bitcoin or Monero. This can degrade system performance, increase energy consumption, and generate profits for attackers.
- Uncleanable infections: an instance where the botnet malware is difficult to remove and traces back up to several years where the user infections had no admin access over their devices.

2. Privacy

The proliferation of Internet-connected devices in smart homes has led to significant privacy and security risks, with personal information being increasingly accessible in new ways. Alarmingly, 98% of

all IoT device traffic remains unencrypted, leaving personal and confidential data vulnerable to interception. [3] This lack of encryption exposes the households' data to data breach and misuse.

One concerning aspect is the potential for attackers to eavesdrop on wireless transmissions from sensors, enabling them to detect intimate activities such as showering, toileting, and sleeping. Moreover, hackers can exploit vulnerabilities in IoT devices to remotely take control of household devices, using them to hack the home network or launch attacks on other domains, such as overloading the energy grid.

> "In 2014 over 73,000 video cameras were found to be streaming their surveillance footage live on the Internet"
>
> – Bugeja et al, 2016

Likewise, Phishing attacks remain a common method for attackers to bypass initial defenses and establish command and control over IoT devices. Once infiltrated, attackers can intercept unencrypted network traffic, harvesting personal or confidential information for exploitation on the dark web.

Furthermore, the use of VLANs can inadvertently mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network, exacerbating security risks. Even seemingly, devices like smart robot vacuum cleaners can pose a threat by providing hackers with insights into the layout of a home, facilitating further nefarious activities.

Other concerns

1. One of the greatest threats to IoT security is the lack of encryption on regular transmissions. Many IoT devices don't encrypt the data they send, which means if someone penetrates the network, they can intercept credentials and other important information transmitted to and from the device.

2. In many cases users face lot of network congestion and potential security breaches. Video and voice traffic tend to happen a lot times. Someone can hack an IoT device to get their foot in the door and gain access to more sensitive data stored on the network or other connected devices.

3. There are high chances of not having complete data on what devices are connected to the network. There are problems of having improper and unclear storage.

[3] Team GRL, 2023

4. In the upcoming years, we require automation and personalization that pairs with the smart ecosystems as well. Manufacturers will have to create products that goes hand in hand with user comfortablity and nature.

5. Some users will require to change their privacy controls. They will not be comfortable with data sharing for third party organizations. That is a concerned problem.

SOLUTION

There are many tips to keep such malicious attacks at bay, like patch updates, password management, and more, so the proposed solution can integrate all such features into a single platform, one that takes care of all such matters in one place.

Features of the proposed solution:

1. Development of privacy-enhanced gateway/IoT device management platform
    - This platform serves as a centralized control point for all IoT devices within the home network.
    - It provides robust security measures including firewall protection, intrusion detection, and traffic monitoring.
    - Additional features such as VLAN segmentation, network isolation, and secure VPN access for remote management are included.
    - Device management capabilities encompass inventory tracking, automatic firmware updates, security configurations, and remote troubleshooting.
    - Integration with existing smart home ecosystems ensures compatibility with a wide array of IoT devices and manufacturers.
    - Enhanced privacy measures are integrated, such as end-to-end encryption for voice commands, local data processing, and transparent privacy settings.
    - Advanced privacy controls are included, allowing for anonymization of user data, opt-in consent for data sharing, and granular permissions for third-party integrations.
2. Implementation of advanced botnet detection
    - Real-time botnet detection is achieved through the analysis of network traffic, employing both signature-based and behavior-based detection methods to identify malware.
    - The solution aids in the identification and cleanup of unnoticed infections.
    - Top-level bot mitigation tactics are employed to prevent or minimize botnet attacks, including multiple layers of protection such as Captcha, and continuous monitoring of network activity for unusual activities.

EVALUATING THE SOLUTION

The advantages it offers

- Ability to access the states of all the devices in your home in one place. And being informed about patch/software updates.
- It can detect network traffic before any botnet attacks, preventing the corruption of devices.
- The solution encrypts your data when communicating across devices, enhancing security.
- Segmenting the VLAN helps with decreasing broadcast traffic, safeguards against potential security breaches, and enables focused administration and control
- The solution helps in anonymizing user data, which helps in preventing unauthorized access and stops one from misusing personal information.

Some limitations to Consider

- Different IoTs may have different vendors, specifications, and connectivity; all of this must be compatible with the solution. All the IoT devices at home must be able to serve the features and functionality of the app. However, achieving this is difficult as different companies follow different standards; thus, we need to seek standardisation at universal or national level. Yet such standardisations would render the individuality of the companies useless. So if this solution were to be implemented, it is to be noted that all the functionality of the app will not work for all devices.
- Since the devices' data is connected to the cloud, it gives rise to the potential for data to be intercepted while transmitting to/from the cloud. So it is recommended to avoid cloud storage and use local storage instead; using local storage minimises the risk of interception, though the cost and space required to store data would be much higher.

CONCLUSION

The interconnected nature of IoT devices, along with their extensive data collection capabilities, exposes users to various threats, including botnet attacks, privacy breaches, and unauthorized access to personal information. Addressing these challenges is crucial to ensuring the safety and privacy of individuals in their own homes.

The proposed solution offers a privacy-enhanced IoT security platform with advanced botnet detection methods, and offers a comprehensive approach to mitigating these risks. By centralizing control,

enhancing encryption, and implementing real-time threat detection, the solution aims to prevent smart home ecosystems from malicious attacks and safeguard users' privacy. However, implementing the solution in real-time requires ongoing efforts to standardize IoT device protocols to fully experience the solution's proposed functionality. Additionally, collaboration between industry stakeholders, policymakers, and consumers, must be fostered to create a safer and more secure IoT environment.

As IoT technology continues to evolve, it is crucial that manufacturers prioritize security and privacy in their product designs. By identifying the importance of security and privacy in IoT smart homes and implementing proactive measures, individuals can be ensured to enjoy the convenience and efficiency of connected technology without compromising their safety and privacy.

BIBLIOGRAPHY

Bugeja, Joseph, et al. *On Privacy and Security Challenges in Smart Connected Homes*. No. 978-1-5090-2857-3/16, 2016, muep.mau.se/bitstream/handle/2043/21507/2857a172.pdf?sequence=4&isAllowed=y, https://doi.org/10.1109/EISIC.2016.21.

D21DCS151. "A Case Study on Mirai Botnet Attack of 2016." *Medium*, 10 Apr. 2023, medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508. Accessed 1 Apr. 2024.

"IoT Botnet - Definition." *Www.trendmicro.com*, www.trendmicro.com/vinfo/us/security/definition/iot-botnet.

"What Is a Botnet?" *Check Point Software*, www.checkpoint.com/cyber-hub/threat-prevention/what-is-botnet/#:~:text=A%20botnet%20is%20a%20network.

2020 Unit 42 IoT Threat Report. https://iotbusinessnews.com/download/white-papers/UNIT42-IoT-Threat-Report.pdf

Team GRL. "The Importance of IoT Cybersecurity a Connected World."Graniteriverlabs.com, Granite River Labs Inc. , 13 Sept. 2023, www.graniteriverlabs.com/en-us/industry-insights/iot-network-cybersecurity-standards#:~:text=The%20fact%20that%2098%25%20of. Accessed 3 Apr. 2024.

"What Is Is IoT Security? IoT Security and Privacy Issues - Zenarmor.com." Www.zenarmor.com, 4 Nov. 2023, www.zenarmor.com/docs/network-security-tutorials/what-is-iot-security#what-is-meant-by-iot-security. Accessed 3 Apr. 2024.

Image credits

https://drivestrike.com/smart-home-threat-deterrence/

https://www.moneycontrol.com/news/technology/do-it-yourself-how-to-set-up-a-smart-home-in-under-rs-75000-3387041.html