VULNERABILITY OF SMART HOMES

Xurramov Shohboz Xurram o‘g‘li
TUIT Karshi branch, student
shohboztuit@gmail.com

Shokirov Shoxrux Husen o‘g‘li
TUIT Karshi branch, student
shoxruxshokirov9@gmail.com

Faxriddinova Dilso‘z Faxriddin qizi
TUIT Karshi branch, student
faxriddinovadilsoz@gmail.com

ABSTRACT

The number of smart homes globally is expected to growth to 478.2 million by next year [1]. One of the biggest attractions of smart home technology is using internet-connected devices to secure personal dwellings remotely. Despite the ease smart home security devices provide for protecting homes against theft, damage, or accident, smart home devices also create the risk of lowering personal data security.

A 2021 research project discovered that typical smart homes are helpless to a high number of data attacks.[2] Reported instances of smart home attacks have included hackers remotely controlling smart lights and smart TVs [3], unlocking IoT-enabled doors, and remotely turning on and streaming video from smart cameras.[4] In one example, a Milwaukee home only realized they had been attacked when they woke up after their thermostat had been programmed to over 30 degrees Celsius [5].

Two major faults in connected homes make them susceptible to these attacks; vulnerable local networks and weak IoT devices.

Keywords: *Smarthomes, IoT, attack.*

Weak IoT devices

Researchers tested a total of 16 commonly used smart home devices from a range of brands and found 54 vulnerabilities that exposed users to attack by hackers. The potential of the attacks ranges from deactivating security systems to stealing personal data.[6] An estimated 80% of IoT devices are vulnerable to a wide range of attacks.[7]

Smart home devices are vulnerable to attacks because they are special-purpose devices. The IoT vendors fail to provide the required special-purpose security

solutions. Further, smart home devices often run small operating systems such as INTEGRITY, Contiki, FreeRTOS, and VxWorks, whose security solutions are not as robust as those of Windows or Linux-based systems. Most commonly available devices, once deployed, cannot be upgraded to update the security capability against the evolving cyber-attacks.

Common smart home device attacks

Attacks on smart home devices are performed in a range of methods depending on the device and communication protocol. Common attacks methods include:

- Data Breach and Identity theft:

Insecure IoT devices generate data and provide cyber attackers with ample space to target personal information. This could potentially end up in identity theft and fraudulent transactions.

- Device hijacking and Spoofing:

The smart devices can be hijacked, rendering the control to attackers' hands. The attackers manipulate the device, spoof the communication between two ends, and can assume control over the other devices, even the whole network.

- Distributed Denial of Service (DDoS): The device or network resource goes unavailable to its intended users by temporarily or indefinitely disrupting the services.
- Plashing: Such attacks brutally damage the device to the extent that it needs replacement.

Securing smart homes devices after purchase

While some devices have embedded security properties, for smart home devices to be resilient to attack, their owners must abide by some basic protection measures.

- Strong passwords: Ensure routers and all devices have strong passwords. Retained default passwords are a common access point for hacks.
- Guest Networks: Use the guest network to set up smart home devices when possible. This can help separate the devices from the valuable information stored on laptops or phones. Even if cyber-criminals hack one of the IoT devices, they will not be able to penetrate the main network and compromise the computers and smartphones connected to it.[3]
- Two-factor authentication: Enabling two-factor authentication, where a device requires an additional verification via a mobile or authenticator app, significantly reduces the ability of hackers to manipulate devices.

- Update Firmware: While many devices will provide automatic updates, manually checking and updating the firmware of routers and IoT devices ensures the latest security protocols are active.
- Avoid Cloud, use local storage: Use local storage instead of the cloud to minimize the risk of the data being attacked while being fetched to the cloud.
- Highest Level Encryption: Use the highest-level encryption (WPA3) on the router to ensure secure communication.
- Firewalls: Using firewalls is one of the famous ways to secure smart home devices. A firewall enables the user to see potential attacks and manage the security level of individual connected devices. Firewalls send notifications to the host when any abnormality in the network or devices is detected.

Role of IoT device developers:

The responsibility of IoT devices' security lies mostly on the IoT device developers. They must take the necessary measures to make devices safe. Some potential measures could be:

- Incorporating Edge Computing: Process the data collected from the devices at the edges close to the data sources. The data does not travel through the weak networks to the remote servers, so the risk of breaching is reduced.
- Designing Over-The-Air Update Capabilities: Manufacture the devices with efficient Over-The-Air (OTA) update capabilities. Many consumers have their devices in remote locations and so update them irregularly. The developers must incorporate a robust OTA update strategy that can execute efficiently and regularly.

Conclusion

Devices connected to the internet are inherently vulnerable to attack. As smart home devices increase in functionality and are more widely installed in homes, understanding personal data security risks and how to mitigate them is critical. IoT engineers must also take responsibility for ensuring smart homes of the future have security built-in as a core feature and not an add-on.

REFERENCES

1. [Online]. Available from: https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world.

2. Laughlin A. which.co.uk. [Online].; 2021. Available from: https://www.which.co.uk/news/2021/07/how-the-smart-home-could-be-at-risk-from-hackers/.

3. Qodirov, F. E., O. D. Doniyorov, and H. Shokirov Sh. "Basic concepts of information security in information systems. Wide threats and their consequences." концепции устойчивого развития науки в современных условиях (2021): 153-155.

4. Qodirov F. E., Akbarova D. A., Shokirov S. H. Software for working with computer graphics and their tasks. Application of digital image processing fields //Инновации в технологиях и образовании: сб. ст. участников XIV Меж. – С. 57.

5. Шокиров, Ш. Х., and Ш. Т. Турамурадов. "преимущества и эффективность использования искусственного интеллекта в социально-экономической сфере." international conferences. Vol. 1. No. 5. 2022.

6. Shokirov, Sh H., Sh B. Nusratova, and Y. Q. Shoniyozova. "advantages of neural networks." концепции и модели устойчивого инновационного развития (2020): 56.

7. Рустамов М. А., Шокиров Ш. Ҳ., Шониёзова Ю. Қ. Развитие компьютерных языков и программистов //теоретические и практические основы научного прогресса в современном обществе. – 2020. – С. 14-18.