**Threats and Vulnerabilities**

Intelligent home device technology has recently increased and is widely adapted in multiple homes worldwide. State-of-the-art architects are now designing homes with smart devices. People have termed technology as efficient since it makes life easier. However, smart homes have posed huge potential risks affecting some users. There are several established threats to smart home devices and vulnerabilities the devices have.

When smart home gadgets do not have strong defences against hacking assaults, fraudsters may acquire so much personal information, including credit card details or birth date. They might then conduct targeted attempts to entice the owner of this information into dubious trades using the stolen data. For instance, if a hacker learns that a family member is in debt, he may send the individual a bogus request for cash on behalf of that person (Heartfield et al. 2018, p.413). The case is considered a targeted attack.

Identity theft is another vulnerability with these intelligent devices. Instead of getting into an individual’s smart device to obtain his data, hackers may occasionally breach the database of a smart-device company to acquire available user data. Numerous users of specific smart gadgets may have their data exposed by significant data breaches. A cyberthief may mimic an individual and end up ruining their life by applying for credit cards using their identity, getting a mortgage in that name, or doing other things (Park et al. 2019, p.2148). In addition to that, location tracking is an established vulnerability. Confidence in these smart home appliances to protect personal information, especially information about the personal address, might be a threat. These gadgets risk betraying confidence by revealing personal whereabouts and allowing hackers to track down and spy on individual activity. For instance, when a device like a computer or a mobile phone the phone or computer is connected to a network similar to that of intelligent devices, hackers can send malicious links to these devices. When these links are clicked, there exists the threat of exposing the street address of these devices. Smart cameras and door locks pose the vulnerability of break-ins that result from manipulating these remote devices. These gadgets might have undiscovered security flaws that would allow hackers to access and manipulate doors and cameras (Ali & Awad, 2018, p.817). The chances of a burglary will be high in such a situation.

Digital voice assistants are always alert, constantly listening to any voice or activity. Hackers may gain access to these smart speakers and use security flaws to give orders of their own or collect previous recordings. Moreover, a virtual bad guy can examine and change the data that these smart gadgets collect since it is rarely encrypted. The technique allows hackers to access and replace camera live feeds to perform malicious activities like burglaries. Cybercriminals may find it much simpler to use intelligent gadgets for evil purposes if they run outdated, threat-prone software (Karimi & Krit, 2019, p.3). Software that is not up to date lacks security updates, making it relatively easy for hackers to hack into and take advantage of the situation.

**Solutions**

Determining whether gadgets are internet-capable and if it is necessary or desirable to connect those particular devices is the first step in securing intelligent home technology from attacks. Before buying, installing, and connecting a device to a home network, it is critical to be aware of the security features offered for that item. These will help deal with the threats from a primary level.

Sharing limited information with these intelligent devices, ensuring the use of up-to-date software, and using advanced tools for network monitoring also form part of the solution. The safest measure is using advanced network monitoring tools since they alert a user of suspicious operations on the network. Verification of device originality and flashing could help reduce physical attacks. Original devices can be identified using IMEI info and crosschecking the device details on a manufacturer’s website. The original devices make it safer compared to when using fake devices in smart homes.

Moreover, flashing any purchased devices helps erase data making the device as good as before. When reselling the same device, flashing is vital to clear any stored usernames and passwords; this will help prevent physical attacks. With more attacks being based on DDoS attacks and DNS hijacking, an improved design or architecture of the intelligent devices in these smart homes could be the most effective solution (Yan & Lee, 2020). Good network design prevents DDoS attacks, and DNS hijacking since any available loopholes on a network are sealed, making an intelligent home system safer.

**References**

Ali, B. and Awad, A.I., 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), p.817.

Park, M., Oh, H. and Lee, K., 2019. Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors*, *19*(9), p.2148.

Karimi, K. and Krit, S., 2019, July. Smart home-smartphone systems: Threats, security requirements and open research challenges. In *2019 International Conference of Computer Science and Renewable Energies (ICCSRE)* (pp. 1-5). IEEE.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R., Filippoupolitis, A. and Roesch, E., 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, pp.398-428.

Yan, Z., & Lee, J. H. (2020). The road to DNS privacy. *Future Generation Computer Systems*, *112*, 604-611.