Smart Households

Protection of technologies/implementation of cybersecurity

Introduction to the subject

Definition:
A smart home is a residence equipped with a communications network linking sensors, domestic appliances, and devices, that can be remotely monitored, accessed or controlled and which provides services that respond to the needs of its inhabitants. Smart buildings are flexibly connected and interacting with the energy system, being able to produce, store and/or consume energy efficiently. The user can remotely monitor and/or control home attributes, beginning with security and alarm systems, lighting, climate, entertainment systems and appliances. Smart homes and many of their connected devices can be included in the category Internet of Things (IoT).

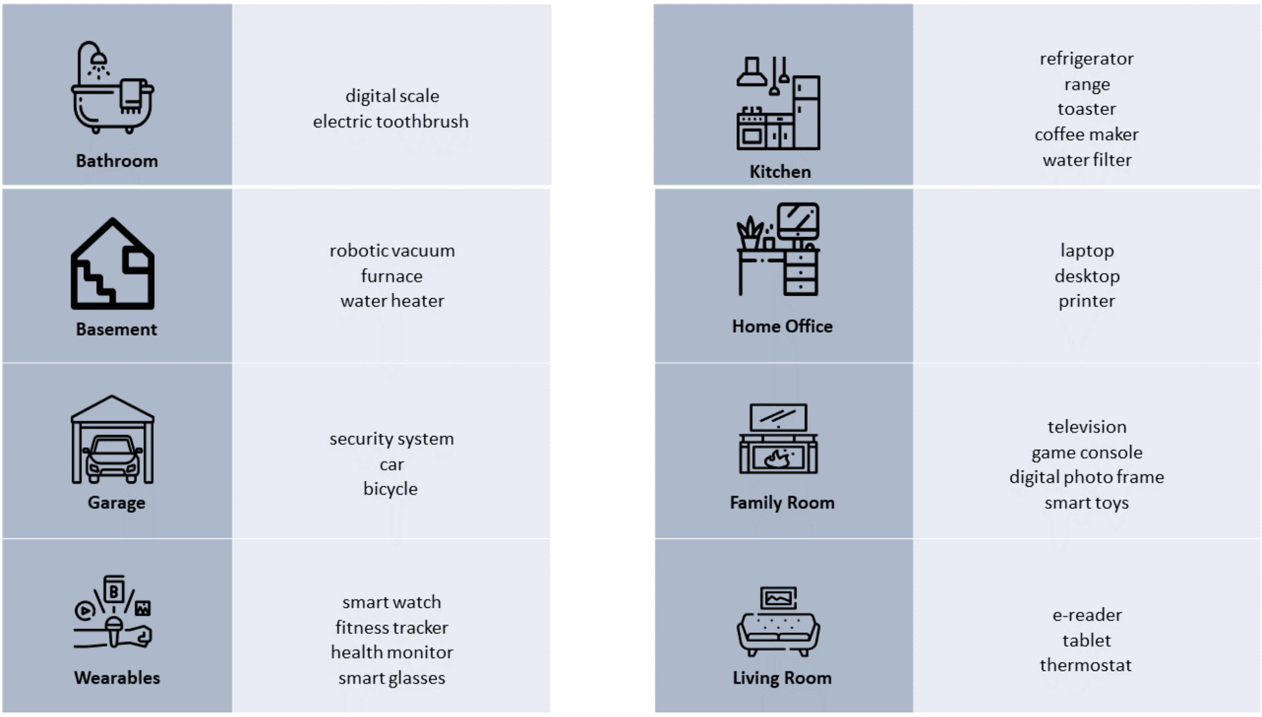
IoT is defined as a network of physical objects that are embedded with software that allows for them to connect to the internet, these devices have the ability to collect and transfer data over a wireless network according to programmable specifications.

Deliverable 1 -

What is a Smart Home or Smart Building?

Mr.Robot - Smart House Scene

Applications and devices that can be found inside a smart household



Bathroom	digital scale electric toothbrush	Kitchen	refrigerator range toaster coffee maker water filter
Basement	robotic vacuum furnace water heater	Home Office	laptop desktop printer
Garage	security system car bicycle	Family Room	television game console digital photo frame smart toys
Wearables	smart watch fitness tracker health monitor smart glasses	Living Room	e-reader tablet thermostat

Following is a list of some of the devices and services that can be found in smart households. These systems enable the consumer to manage the systems while away from home, and adjust the settings according to their needs, at any given time, regardless of their physical location. Home automation is prevalent in a variety of different realms, including, but not limited to;

Home robots and security:
A household security system integrated with a home automation system can provide additional services, such as remote surveillance of security cameras over the Internet, or access control and central locking of all perimeter doors and windows.

Heating, ventilation and air conditioning (HVAC):
It is possible to have remote control of all home energy monitors, over the internet, incorporating a simple and straightforward user interface.

Lighting control system:
A smart network that incorporates communication between various

lighting system inputs and outputs, using one or more central computing devices.

Occupancy-aware control system:
It is possible to sense the occupancy of the home using smart meters and environmental sensors, which can be integrated into the building automation system to trigger automatic responses for energy efficiency and building comfort applications.
Appliance control and integration with the smart grid and a smart meter, taking advantage, for instance, of high solar panel output in the middle of the day to run washing machines.

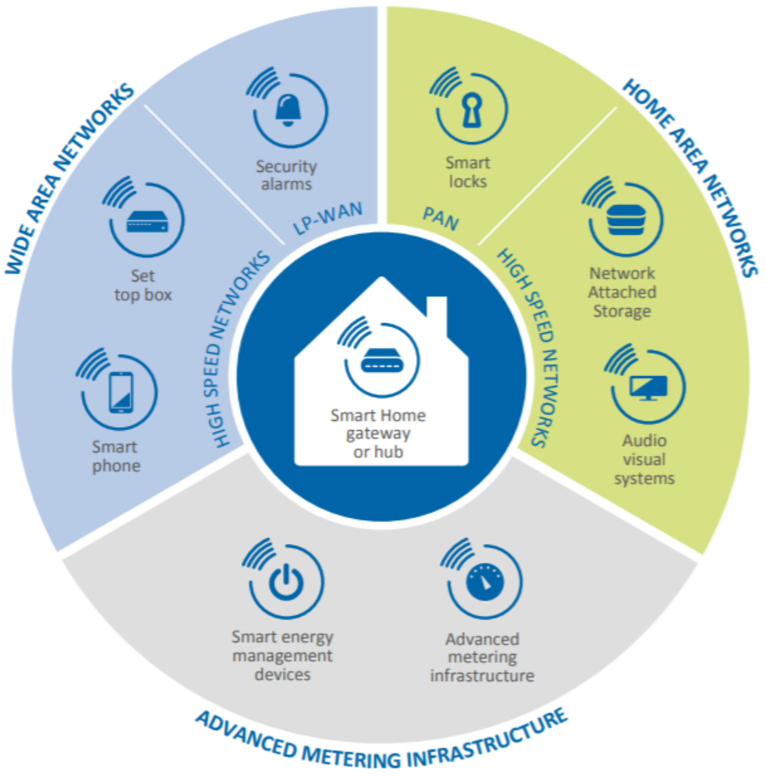
Leak detection, smoke and CO detectors:
This is possible using indoor positioning systems (IPS), a network of devices used to locate people or objects within a building/area.

Baby/ Pet monitors:
These are used to monitor children and pets, connecting them to the smart home network can assist in providing the owner the ability to view the monitors 24/7 from anywhere.

Smart Kitchen and Connected Cooking.

Voice control devices:
Devices like Amazon Alexa or Google Home used to control home appliances or systems.

As technology advances, more and more products, items and services get added to the list of smart devices. Many things that were once considered basic items can now be viewed as smart devices, who knows where the technology will take us, and what future items will be considered “smart”.



Advantages of smart households

The most significant advantage to living in a smart household is that the owners have the ability to remotely monitor their homes, control any smart devices in the home using a centralized application, adjust thermostat, run laundry/ dishwasher, turn off devices that have been left on, lock a door that was left open, the possibilities in this area are endless. Instead of roaming around, turning on and off machines, they can access everything from one point. Additionally, users can receive updates and notifications regarding their devices, upgrades or communication and control of their home, even when they're out and about.

Smart houses allow people to have greater awareness of their homes' resources, what appliances use the most electricity, and avoid overuse of appliances. The home automation systems are also capable of learning the behavior of the residents, for example, adjusting the thermostat for the time the homeowners arrive at home. A smart irrigation system can ensure that plants are only watered when needed, and with the precise amount of water necessary. With all these automated systems, energy, water and other resources are used more efficiently, which helps conserve both natural resources and money, for the consumer.

Smart homes can be beneficial to the elderly and disabled, having systems in place that can allow for more independence, while maintaining a level of safety and providing assistance if needed.

Alongside the many advantages and comforts the owners of smart homes enjoy, there are a considerable number of disadvantages and risks that accompany the installation of automated systems. These disadvantages can be separated into different fields, which we will elaborate on in the upcoming sections. These constitute the reasons a consumer might choose to not to turn their home into a smart household.

Monetary pitfall

Installing a fully-smart home can become expensive and users might encounter a steep learning curve, to get used to using their new system. Additionally, smart devices are infamous for their relatively short shelf-life, which can result in homeowners needing or wanting to upgrade their devices every few years. Technology is constantly evolving, and devices quickly become obsolete, and are no longer supported by manufacturers after a few years. This can cause the rapid turnover of appliances that would not otherwise have been replaced, if they were not “smart devices”.

Security concerns

Any device that is connected to a network opens up a new port, which poses a threat to the home’s network, and exposes the whole home to potential attacks and breaches.

So in the case of smart households, not only is the front door an access point into our houses, now the toaster, air conditioner or even the baby monitor can provide entry for intruders into our homes. Any device that connects to a network requires security, however the level of defense provided in “simple” smart devices is much less robust than that provided in PCs, which are known to have vulnerabilities and can be accessed by someone with enough persistence and motivation to do so.

Example:

HP did a study in 2014 looking at 10 popular IoT products and found that 70% of IoT devices are vulnerable to attack, and what's more, the devices average 25 vulnerabilities per product. They found that 60% of devices did not use encryption when downloading software updates. This means that some downloads have the potential to be intercepted, extracted, modified and installed without end-user knowledge.

To protect against security hazards that come along with the rise of IoT, it is imperative for organizations to implement an end-to-end approach to identify software vulnerabilities before they are exploited.

Energy consumption

We need to consider the lack of concern in the world for energy consumption. While it's true that manufacturers try their very best to make state-of-the-art homes and devices that are useful and energy reliable, we need to understand that when we integrate more devices into our day to day lives it results in adding power usage. Efficient as any particular device may be, most of us don't stop at one or two.

Alongside the surge of smart homes and smart households, IoT devices add an additional layer of energy consumption. It is important to remember that there is a finite amount of energy, at least until we find another reliable energy source.

Dangers that accompany smart household:

Physical attacks

These can arise from a well-identified attack vector (physical manipulation of devices). They might lead to various types of risks, including the categories described as activity/abuse or eavesdropping/interception/hijacking. A physical attack typically threatens all assets.

Hijacking the smart home's systems

An attacker that finds a vulnerability in the smart home security systems, whether it is a weak password, misconfigured devices or any other type of weakness, can use this flaw to their advantage. The attacker can leverage the vulnerability to hijack the systems and take full control over the smart house.

Example:

In 2019, a hacker took over the smart house of a Milwaukee couple and terrorized them. The hacker changed the temperature of the house to 90°F, by manipulating their thermostat, played loud music and disturbing videos on their media systems and spoke to them via their security camera. It is believed that the attacker gained access by using compromised passwords, rather than breaching their security network.

Home intrusion

While the potential for remote device tampering is very scary, it pales in comparison with the risk of physical break-ins, posed by security devices like smart door locks and surveillance cameras. Unidentified security loopholes in any of these devices could grant a hacker permission to disable cameras or even unlock doors to let in accomplices, burglarize the property, or in some cases lock you out of your own home.

Appliance or property damage

Breaches of smart devices that control critical functions of the home,such as cooling and heating can be even more disastrous. A hacker with access to the thermostat could fiddle with it. Worse yet, a hacker could crank up the oven and cause a house fire, all while the unsuspecting consumer is away from home.

Rouge recording

When owning a smart speaker such as Alexa, there is a great likelihood that the user is being eavesdropped on by a third party. In a similar manner, hackers can also exploit security loopholes to gain access into the speakers and inject their own commands or even download prior recordings.

Location tracking

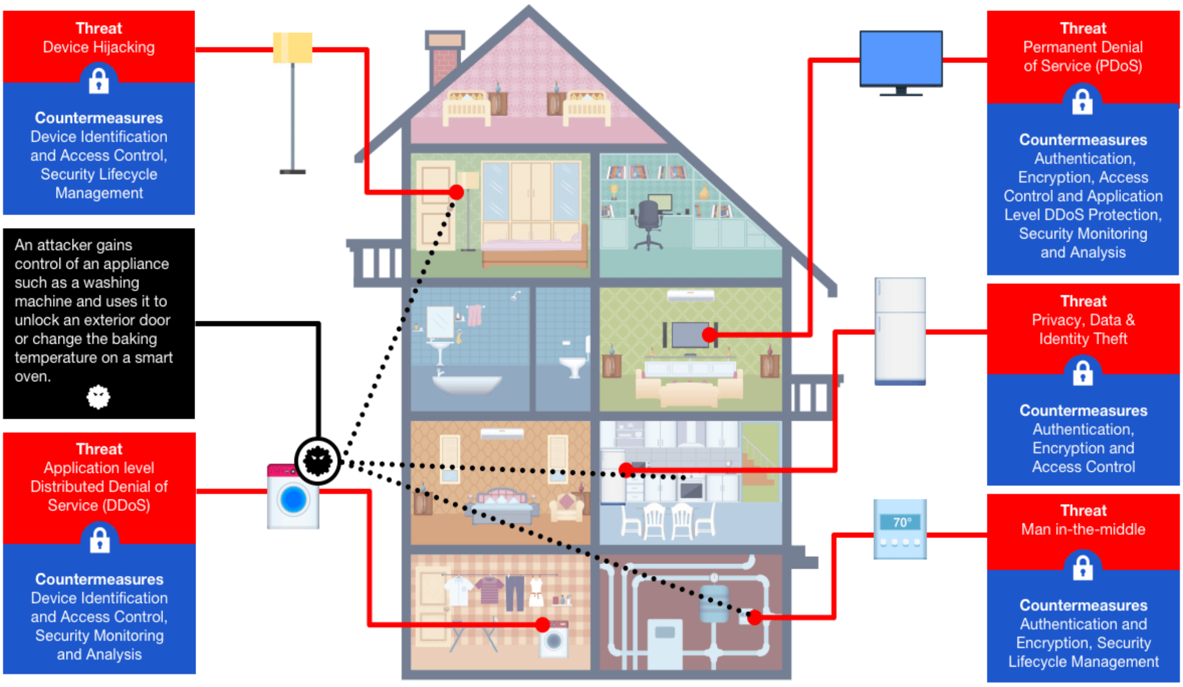
Smart home devices are trusted to keep private information private, particularly information about where the user lives or located.
But these devices can betray that trust by giving away your location and making it possible to locate your current position. This means, potentially

doxxing (act of publicly revealing previously private personal information about an individual or organization).

Data and usage habits can be sold to third parties
The smart devices transmit data to their manufacturing companies. This data could potentially be sold to advertisers or malicious actors. All discarded smart devices can constitute potential threats, and provide access points to hackers or anyone who wants to gain access into a personal network for their own gains.

Example:
An ethical hacker located a discarded smart light bulb, and was able to access personal information, accounts and passwords from the chip located in the lightbulb.
https://www.news5cleveland.com/news/local-news/investigations/ethical-hacker-shows-us-how-easily-smart-devices-can-be-hacked-and-give-access-to-your-personal-info

Relevance to the global cyber threat



Threat
Device Hijacking

Countermeasures
Device Identification and Access Control, Security Lifecycle Management

An attacker gains control of an appliance such as a washing machine and uses it to unlock an exterior door or change the baking temperature on a smart oven.

Threat
Application level Distributed Denial of Service (DDoS)

Countermeasures
Device Identification and Access Control, Security Monitoring and Analysis

Threat
Permanent Denial of Service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Privacy, Data & Identity Theft

Countermeasures
Authentication, Encryption and Access Control

Threat
Man in-the-middle

Countermeasures
Authentication and Encryption, Security Lifecycle Management

Security just isn't a high priority for some connected device makers. All it takes is one compromised device to allow hackers to access personal or sensitive data, leaving the entire home network at risk.

The most common attacks on IoT devices

Data breach / identity theft
IoT devices gather lots of information about the end user. Personal information like addresses, phone numbers, health records (from wearables like smart watches) and even bank information are all handled by smart home devices. Hackers can target these devices and gain the information necessary to steal user identities.

Man-in-the-middle (MITM)
Man-in-the-Middle attacks occur when a hacker intercepts or spoofs the communication happening between two devices. This attack makes it appear as if a normal exchange of information is underway. The goal of MITM is for the attacker to gather sensitive information by eavesdropping on the targets, without revealing that they are listening.

Example:

One MITM attack that made the news was when a Samsung smart fridge was compromised and allowed hackers to gain access to Gmail login credentials. https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html

Distributed Denial of Service (DDoS)
A denial-of-service attack (DoS) is done by flooding a network or website with large amounts of data, to force websites, devices, or entire systems to shut down or become unavailable. DDoS attacks take DoS attacks one step further by using multiple computers and networks to execute the attack by flooding a targeted system or device with enough traffic to shut it down and stop it from working.

Often, hackers will gain control of IoT devices (usually without a user knowing) and harness the power of hundreds or even thousands of these compromised devices to launch DDoS attacks. (Each compromised machine is known as a "bot", and the network of compromised devices is known as a "botnet").

Example:

The Mirai botnet attack is a big example of a massive DDoS attack which left much of the eastern coast of the US without internet access.
https://www.minim.com/blog/why-minim

Permanent Denial of Service (PDoS) / phlashing

PDoS attacks damage compromised devices to the point of replacement. One example of a PDoS attack is a feed of fake data to a smart home thermostat that might cause extreme temperature fluctuations, resulting in physical damage to both the device and the home.

Securing the smart home against cyber attacks

Now that we’ve elaborated on the types of attacks that most commonly affect connected devices in the smart home, it is time to discuss solutions and the options available for implementation of protective measures.

Depending on your location and availability, it is possible to hire a company to create smart home environments. These companies will handle the setup, maintenance, followup and security of the system. These types of companies are one-stop-shops for home automation. Smarthome is such a company that operates in the USA. They provide their customers a complete smart home experience, start to finish, alongside continuous security services and maintenance. This company goes to the clients home, installs all the requested devices and provides tech support and security.

A second type of security that is available is the one provided by companies such as Allot. In this type of situation, the customer purchases the devices, integrates them in the network, and the company helps them set up the security. This is a company that provides security solutions for smart homes and IoT devices. They provide local network security, which protects home devices from attacks within the local home network. An example of this is ensuring that a single compromised device in a home network is unable to attack other devices in the network.

Allot provides a centrally-managed thin agent for existing CPE (Customer Premise Equipment), which basically refers to any type of equipment that connects to the internet. Their service secures the home network and protects the CPE against online attacks. All devices in the network are identified and connected to Allot's system. A default security policy is then applied to each device and the home network is segregated, to block malware propagation. The agent protects the CPE from security vulnerabilities that can compromise it, by employing password strength enforcement, open port analysis and protection, and unauthorized access control.

Allot provides a variety of services which focus on the client's CPEs.They provide per-device security, based on the customers existing devices. The installation is done remotely and has low CPU usage. They also provide cloud security to the network and all the devices included in it. Additionally, Allot provides its customers with an application to manage their device security. This allows the end users a simple way to manage the security of their smart home. These services are considered SaaS (Security as a Service) solutions that will monitor your IoT devices as a service using their software, and will provide additional help regarding the software. It must be noted that the subscription is to the software as a service, not to a SOC service.

There are a number of other companies that provide similar services to those provided by Allot. A few examples of these companies are Armis, Bitdefender, Forescout, OverWatch, SecuriThings, Zinkbox (now owned by Palo Alto) and others. We will, however, not elaborate on them here, to avoid unnecessary repetition.

The third option is the do-it-yourself (DIY) solution, where the customer purchases the devices from a company like Amazon ,that provides an extensive smart home department, where customers can choose the devices they need for their home, in one place. Following the purchase and setup of the network, it is up to the customer to install security measures and constantly monitor, update and upgrade their systems.

Tips on how to better defend a smart home

Change the default router name

A router's default name can provide an attacker insight that individuals would not want to be made public. Hackers can use even small bits of information like a device's name to infiltrate a network. Router traffic should be secured by using WPA2 encryption.

Parse the network into logical subnetworks
The devices on a network are able to constantly communicate with each other. A clear example of this is how Alexa can communicate with other devices and control them if needed. Of course this poses a security threat if someone were to access Alexa remotely and use her to gain control of other devices or even the home network as whole.

One way to defend a home network, and keep people from accessing sensitive information is to make boundaries inside a home network with the use of virtual LANs that logically separates which devices can communicate with each other.

Change default passwords
Many people skip this crucial step, the majority of devices come with preconfigured user names and passwords, such as admin admin, admin with the password 1234, and the list goes on. Someone with malicious intent and a little bit of knowledge can access devices in a matter of minutes or even seconds, just by trying a few of the default combinations. This is why it is so important to change the default passwords.

Using a firewall on any device possible, program or physical component
A firewall can filter the type of traffic going through the network and stop possible malicious attempts of attack from unknown sources. Installing a firewall on any device that can handle it, can assist in the protection of each device, individually, and the network as a whole.

Change the default voice command
In certain situations devices can be voice activated with simple and easy to find commands such as “ok Google” or ”hey Alexa”. It is important to personalize those commands to mitigate voice command injection attacks.

Be sure to update the devices
Updates often include security patches, to make sure the software is up to date. Additionally, it is important to check once in a while if the company is still making patches, if not, consumers should consider changing the type of service for security reasons.

Check the permissions settings in all connected devices

Often we give permission to a device to do many things outside the scope of the function it is supposed to do, for example giving the printer administrator privileges. This can pose a risk if an attacker manages to access the device, use the privileges to insert themselves into the entire network and do as they please.

Do not connect anything to your device without fully knowing what it contains

Until we are sure about what kind of device we are using, such as a flash drive, it is not a good idea to plug it in to any device we own that may be corrupted by it. Verify the source of the devices and that it originated from trusted sources.

Getting an IDS or IPS:

By installing an Intrusion Detection System or an Intrusion Preventions system, smart home users can monitor suspicious or anomalous traffic on all the devices in their network.

Access control

Limiting access and delegating permissions to a predefined set of users will restrict who can control devices and home servers. This can help mitigate exposure and an overabundance of administrative users, which can further partition the network.

Hash passwords

It is good practice to consider not saving any login data inside a network or to keep electronic copies of it, instead passwords should be hashed and only the corresponding hashes are saved on the network.

Cloud computing

Rather than basing home automation systems off of a dedicated IP address or high-end computer, many systems are based on a cloud, which is both more affordable and easier to use.

However, even though a cloud service is a good possible solution for security needs, it is crucial to check once in a while if the service is still proactively protecting your system.

Manage the risks and create a fail-safe
Create a backup for when all else fails. In some cases, no matter how well the smart household and IoT devices are protected a breach will occur. At that point, it is a good plan to have a backup, preferably one that is not connected to a network, that will contain a backup of all of the information needed and configurations that were made to the systems, or even software that will assist in a hard-reset of the devices as fast as possible, in order to buy time against the attack. It is important to occasionally check that the backup is still intact and functional.

Issues with the common approach to smart households

While researching the topic at hand we found a general lack of concern about the issue from a cybersecurity point of view. Of course there are forums like Kaspersky that post a few tips on how we, as the consumers, can defend ourselves but there is no suggestion on services.

This approach is problematic, to say the least, since very few people around the world will read these tips and even fewer will implement them.

Lack of centralized service as a solution

Smart households contain different devices, which lead to a high probability that many devices will operate on different operating systems (OS). This creates a world of problems, each unique device has its own exploits, its own source code and so on. This makes finding a way to mitigate attacks exponentially more difficult.

There are a number of premium brands of IoT devices such as Alexa (which itself has been involved in a lawsuit for recording children) or Google Home Assistant, that have their own proprietary softwares and continuously patch and update the system. These companies provide defensive software to their supported devices. But the fact remains that this kind of service is first of all, pricey, and second of all, supports only the devices belonging to the brand, and it cannot be expected from them to protect devices that belong to other companies with foreign source code that could have unknown flaws.

What about those who purchase their devices from less known vendors?
In an attempt to “get a piece of the pie”, less known companies developed their own version of devices for smart household needs, by skimping on the software developments and security, they manage to bring a competitive price to the market. The greatest issue here is most likely that the OS will be an opensource linux-based system that will come with a plethora of exploits and vulnerabilities already built in, not to mention the fact that you can forget about patching or system updates.

This brings us to the conclusion and the big question, what kind of broad solution can we use?
At this point there is no general answer from the cyber security community, as we said in the beginning of the section, most of the answers rely on the consumer being, to some extent, computer literate in order to successfully deploy at the very least some sort of solution.

There is a lack of subscription-based SOC services that doesn’t involve SaaS or buying the house as a package that individuals may acquire for the purpose of securing the IoT device and smart households networks on a day-to-day basis. There is a need for a service that would provide 24/7 monitoring of smart home systems, detect and prevent breaches in real time, not only after-the-fact. There are many cybersecurity companies in general that include IoT protection services, and only a select few really focus on IoT. We were able to find very limited security options for smart home clients, not to speak of SOC services for individuals.

We must note that there are companies that design and implement solutions for smart homes as a whole, but only if the entire smart home is installed by them and their proprietary devices, only then will they provide monitoring services.

On the other hand, in the cases of macgyvering smart households that were designed or built by individuals, they unfortunately do not have access to such oversight systems and they will have to resort to finding a platform or a software service to defend their networks in general and IoT devices in particular.

If a consumer is searching for a service that works with a variety of devices that will provide sufficient protection without the requirement to subscribe to a software or purchasing the smart home in a package, they may have to wait a while.

Difficulties in integrating and protecting smart homes

There are currently no survey or experience-based platforms that a consumer can use to compare the kind of services, which can help them make well-informed decisions, and understand the full scope of protection and services they are considering to purchase or subscribe to. In researching smart home security services, the most common results are ads and sites that are trying to market certain services, for monetary purposes. This means that someone who is searching for a specific service will be barraged with bios, articles and ads, without really knowing if these are the best suited for their needs, since there is no platform where customers can share their experiences on this topic and recommend companies and services.

Consumers looking for IoT protection can become overwhelmed with the plethora of services available, and not knowing which one to choose. This could lead to frustration and for the consumer halting their search for cybersecurity solutions, while leaving their homes, devices and networks vulnerable to attacks. This makes it harder for companies to protect systems by association, for example, the Mirai attack that disrupted the internet for an entire country by using IoT devices and flooding traffic to DNS servers such as Dyn and making it impossible accessing sites like Netflix and Amazon (and that’s only a small example of the destruction that can occur as a result of neglecting security in IoT devices).

Conclusion

Smart households were invented to make our lives easier, they were designed to provide benefits such as comfort, protection and automation. Alongside their many benefits and convenience, they can expose us to a world of possible threats ranging from data theft to, in extreme cases, causing bodily harm.

It is crucial to be aware of the advantages and risks, when considering going forward with implementing these kinds of technologies into our day-to-day lives. It is important to consider whether the pros outweigh the cons, and if the installation and adaptation of smart homes and IoT devices will end up being a blessing or a burden on the consumer.

As cybersecurity analysts, we have much more to learn regarding the safety aspects of smart households and how we can mitigate potential threats to devices or even people using the smart homes and smart home devices.

Reference Links

https://en.wikipedia.org/wiki/Home_automation#Applications_and_technologies

https://www.investopedia.com/terms/s/smart-home.asp

https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html - hack into smart fridge

https://www.enginess.io/insights/what-is-smart-home-technology#:~:text=Smart%20home%20technology%20is%20the,Home%20entertainment%20systems
https://www.tandfonline.com/doi/full/10.1080/09613218.2017.1301707

https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#:~:text=PALO%20ALTO%2C%20Calif.,of%20granular%20user%20access%20permissions.

https://usa.kaspersky.com/resource-center/infographics/smart-homes

https://www.kaspersky.com/blog/mwc2018-insecure-iot/21343/

https://www.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home

https://www.bobvila.com/slideshow/the-10-biggest-security-risks-in-today-s-smart-home-53081

https://outline.com/ggKJdD

https://www.security.org/home-automation/

https://www.smarthome.com/

https://www.bitdefender.com/box/

https://securithings.com/horizon-solution/

https://www.armis.com/

https://www.nozominetworks.com/?gclid=Cj0KCQjwhr2FBhDbARIsACjwLo2sIORzbikuWx6eAFVHaF5e_GmoPAye5RqRC3K0bTa5kiJ7xNPAQ8waAtvAEALw_wcB

https://www.paloaltonetworks.com/network-security/iot-security

https://overwatchsec.com/

Example:

In 2019, a hacker took over the smart house of a Milwaukee couple and terrorized them. The hacker changed the temperature of the house to 90°F, by manipulating their thermostat, played loud music and disturbing videos on their media systems and spoke to them via their security camera. It is believed that the attacker gained access by using compromised passwords, rather than breaching their security network.
https://cisomag.eccouncil.org/hackers-take-over-smart-home/ -

https://www.shodan.io/ - search engine of internet-connected devices that are exposed or not configured securely