**Presentation Extra Notes**

* **What's Smart Home Security -**
* A Real Smart Home thinks as you do, it will anticipate your needs, doing what is needed when it’s needed. Depending on your presence, the weather, and time of day, it will do all the tasks you usually would, so you don’t have to.
* **Features -**
* Smart home Security uses a very effective internet connection
* Technology come together with technologies to make your home a better place to live in.
* It also looks after the home using CCTVs and report anything suspicious in your area.
* **Lighting**

As lighting is an integral part of a building. The user would be able to choose the time of activation, for example, in the home 7pm when it starts to get dark might be a sensible option. If the user wishes to further customise the lighting settings there should be an option available to implement motion detection, which would involve a person actually stepping into a room, in order for the lights to be activated. This could include a specific room in the home or all the rooms. In a voice controlled format the user could check if the lights were on in any room of the house by speaking into a Bluetooth headset. The system could then ask the user is the lights are in the required state.

* **Security**

With the advancements of smart technology, it makes sense to include security features. The user would be able control the arming and disarming of the alarm, as well as edit specific settings of the alarm, such as the key code. The user could also have the option to configure intrusion detection settings. This would work firstly by outside lights detecting motion and then the system would warn the security personnel or house owner of any windows or doors being forced open, through the use of electronic sensors that are connected to the system.

* **Temperature**

The user would be able to control the heating and cooling of the home, through the use of both time and parameter-based functions. The user may choose for the heating to come on when outside conditions drop below a certain temperature, there would be heat-sensitive sensors placed outside to detect varying conditions.

* **Appliances**

The power supply to all appliances in the home could be controlled using the smart system. In a large home this would be a very convenient feature because there may be a lot of electrical appliances that are left on standby, hence the system should contain a feature, which searches all power supply links in the home to determine where energy can be saved.

* **Entertainment**

For a fully capable smart home, entertainment features would be an innovative feature to include. The most widely used aspect of entertainment features would probably be the ability for subtle music to air throughout the household, this would be very welcoming especially if a resident has had a stressful day at work.

* **System Status**

It is worth having an option to verify the current status of the system. This kind of feature would provide the user with the ability to scan the entire system or just parts of it for errors.

* **Vehicle Detection**

When a vehicle approaches the driveway of a home, the system should be able to alert the homeowner. This is only possible if certain types of smart home technologies are used. It would work very well with a Bluetooth headset because the system announce the arrival of the visitor to the homeowner. It would also work well with more long-range wireless standards, such as, GSM (Global System for Mobile Communications) because the homeowner could receive an SMS (Short Message Service) when someone arrives at the home, which is especially useful when away from the home.

* **Phone set-up**

A home-based system should be able to initiate with a mobile-phone when the house is empty. The system should provide the ability for the user to enter the name and model number of the phone so it can be verified for use. The user will be able to communicate with the system when approaching home to switch the television or the oven on and any other electrical appliances the house owner may wish to make use of.

* **Wake up**

A useful feature in a home-based smart system would be alarm clock functionality, for example, the user would be able to choose from a selection of wake up sounds from more pleasant sounds to more piercing types. At the weekend the more pleasant ones are likely to be selected.

Smart Home technology can bring a valuable extra dimension to home security by utilising conventional security systems and the latest smart systems which talk to each other to provide drastically improved security far greater than the sum of its component parts.

A smart security installation will typically integrate a conventional burglar alarm, lighting control system, gate and door entry systems, external garden security sensors and the TV systems in the house. Through this level of integration the smart home knows when you are at home or away and adjusts lighting, shading and energy use settings automatically and alerts you of intruders in the grounds proactively allowing you to move to a safe area or alert the police before anyone breaks in to the house.

We believe in providing peace of mind for our clients whether they are at home or away and we can provide comprehensive solutions independently or in conjunction with your other security contractors

* **Benefits -**
* A smart home security offers a lot more by turning lights off, if no-one is at home and turning on, if there is someone at home this can be efficient and also save electricity.
* If there is any emergency then there are fire detectors and heating pipes which are are all connected to the smart home security, this will also notify you on your email as well as send you a text on your phone.
* It also lights up a way for you to walk safely to the exit with getting into any trouble.

**1. Proactive Instead of Reactive**

Standard security systems alert you when a problem is underway or has already taken place, such as a break-in, fire, or carbon monoxide leak. These react rather than offering ways to prevent such incidents from occurring, or notifying you sooner.

Smart security systems, on the other hand, are proactive, featuring a wide range of capabilities to further protect your home. For example, alerts can be received from anywhere via your smartphone, iPad, and/or desktop computer, providing critical updates on recent activities in and around your home. If the back door was left open by mistake, for instance, you’ll be notified, so you won’t have to worry about anyone wandering around while you’re sleeping or at work. If your toddler makes his or her way to the front door in the middle of the night, you will be alerted, too, as motion sensors will be activated.

**2. Monitor More Than Just Your Home**

As aforementioned, smart security systems can notify you regarding various activities on your property. Cameras can view what’s happening when you’re not there and enable you to monitor your home, as well as your loved ones inside, ensuring their safety at all times.

You can receive a text message when your teenage son walks through the front door at 2:31 p.m. after getting off the school bus, for example. You can even check in again throughout the afternoon via security camera to ensure he's doing his homework rather than playing video games or spoiling his dinner.

**3. Stay in Control**

Smart technology doesn’t just stop at security. Home automation functions enable you to control various aspects of your home, too—such as adjusting your thermostat and turning on or off the lights, coffee pot, or other appliances. If you ever forget to switch your bedroom light off in the morning before heading to work, for example, you can correct your mistake, from anywhere. All you need is a smartphone, iPad, or desktop computer.

**4. Save Money on Energy Bills**

According to 2015 statistics from the nonprofit National Academies of Sciences, Engineering and Medicine, 27.3 percent of energy usage in the U.S. residential sector is for heating, 11.8 percent is for cooling, and 7.2 percent is for lighting. That's a combined total of 46.3 percent.

Automating your home can save a significant amount of money on your energy bills. Rather than adjusting your thermostat before you leave for the day and once you arrive home that evening, you can schedule a temperature change according to the local weather forecast. You can do the same for lighting, scheduling them to turn off or on at certain times, without you having to lift a finger.

**5. Increase the Value of Your Home**

Online tech resource CNET reported how people are willing to spend more on a home equipped with smart security and automation features in a 2015 article, citing a joint survey with real estate agency Coldwell Banker.

“81 percent of current smart-home device owners say they would be more willing to buy a home with connected tech in place,” it states.

Furthermore, as millennials age and become homeowners, it’s especially important to pay close attention to their preferences. The article reveals that nearly half of millennials already own smart home products. Sellers should consider this when searching for ways to increase their home’s values, as “smart” features are becoming more and more expected home components.

* **Challenges -**
* The challenges faced when a burglar breaks into your home the smart home security will make sure it looks like someone is at home so that the burglar has no choice but to retreat.
* Not only that by there are also CCTVs looking out around the house to make sure that it is perfectly safe and secure. And if someone breaks in the smart home security reveals the burglar’s position through a CCTV camera and can be taken down by calling for help.

Developing for the smart home is a challenge. That challenge is compounded when trying to provide secure communications between a home network and the Internet. The abundance of smartphone apps that allow remote access to home automation devices further intensifies these challenges especially given the attention it draws to hackers. Hackers have had particular interest in this segment of IoT, putting the security of consumer products in the spotlight. Barely a week goes by without a news report of yet another security breach at a major company or government agency.

The increase in security concerns stem from a growing number of threats on outdated systems and protocols that haven’t evolved to meet the sheer volume of connected devices. Platform security weaknesses can ruin consumer confidence in their smart home, and cause them to switch between device carriers or abandon their system altogether. Given the reach of the new IoT ecosystem, cybersecurity is growing and becoming more critical than ever, and companies from many industries are rushing to meet higher standards of security.

As homes become smarter—with security systems, thermostats, and lights that talk to one another and are all controlled with the touch of a finger—consumers demand that the highest level of home intelligence comes with the highest level of security. Device manufacturers need to be vigilant about consumer fears and consider the security of their own devices, but also about the security of all the devices in the ecosystem.

Fears of device hacking or security breaches in an ever-expanding internet of things (IoT) world and within a marketplace that does not have an industry standard for data transmission and instruction are not without merit. The IoT landscape, all of which is potentially hackable, includes a vast number of devices. All devices, whether professional- or DIY-installed, communicate with each other and the internet, via one or more wireless protocols, such as Z-Wave; others include ZigBee, Bluetooth, and Wi-Fi. The protocols themselves generally feature built-in security of various levels. However, the methods that individual brands and smart home systems use to transmit data and instructions via these protocols, both inside and outside the home, can vary greatly in sophistication and unfortunately, in attention to security. At times, for manufacturers, the security process can feel overwhelming and they may be unsure where to begin.

**The potential for IoT Smart Home Attacks**

These types of hacks are easy to imagine. On a micro level, consumers worry about hackers getting ahold of their personal information or data about their home and using that data against them to break in, steal identities, or find out when no one is home. The fear is that hackers can break into your home by “virtually picking” your smart lock or access your smart devices and spy on your family. The far more likely and more serious attack is on the macro level. With the increased amount of sensors and data that hackers could potentially collect an attack could hit the cloud and access a large number of connected devices at once, like 1000 air conditioners for example, to affect not just one person but the entire power grid. In a recent and real-world example, hackers activated emergency sirens all across Dallas, TX and made residents think the city was under attack.

There are three layers of connected networks that are pertinent to overall security: the wide area network (WAN), i.e. the Internet; the local area network (LAN) or “home network”; and the personal area network (PAN), which consists of the end-node devices. Several issues can arise when designing genuinely secure solutions within these varied communication pathways. Security attack threats, cryptographic computation power, available network bandwidth, available code space, firewall policies, and efficient battery operation are only a few, and must all be taken into consideration.

**Your lines of defense**

Among the various smart home protocols, Z-Wave is the longest established, and as a result, has invested the most focus on cyber protection and recently introduced the new security framework, Z-Wave Security 2 (S2). Z-Wave has always used AES-128 levels of encryption.

However, prior to S2, Z-Wave was built on application layers, meaning that the decision was on the manufacturers to implement the security and not all manufacturers have the same level of expertise or appreciation for the importance of security to do it well. For example, if a manufacturer is building a lock, they may only be concerned with building a reputable lock or shrug at the idea that a hacker could “turn a light switch on and off.” However, if a nefarious hacker is able to control a light switch, he may also know if you are home or not. It matters.

S2 prevents a hacker’s ability to do this entirely by eliminating application layers and replacing them with an entire protocol. Instead of saying: “Send command to this and this,” it says: “Send secure.” Now, all transmissions are sent safely. Hackers cannot circumvent the security application layer. The heavy lifting is built directly into the protocol and manufacturers can rest easy, focus on building a reputable product, and not have to be security experts. Sigma Designs, the manufacturers of Z-Wave chips, has done it for them…with the help of a few really smart friends.

**Insight from cyber security community**

Who are these friends? To reach this level of security, Sigma Designs stepped outside the box. The company worked with a community that can often get a bad rap, the hacker community, to create the Fort Knox of smart home protocols. Sigma opened its code entirely to the hacker community for their thoughts, additions, and input. Cooperation led to a level of security that is bar none by targeting security measures in the S2 Framework that preempt the common hacking methods "man-in-the-middle" and “brute-force” attacks. Man-in-the-middle attacks are well-described by their name; the hacker tries to intercept communications between two points and alter them. Likewise, "brute-force" attacks are just as they sound; automated, exhaustive attempts to try every possible data combination to break into the system. Consistent, pervasive encryption is the only real deterrent against these breaches and hijacks. Soon, all smart home systems, regardless of brand or protocol, will be expected to include pre-emptive measures against these attacks.

While neither of these scenarios are common occurrences, their threat remains very real. Z-Wave has taken additional steps to prevent them by monitoring periodical heartbeat signals from all Z-Wave network nodes. This detects jamming as soon as the attack is initiated, and requires S2 encryption for all commands to the door lock. In this way, it is impossible for an intruder to capture the network key via logging. Z-Wave’s S2 key exchange uses Diffie-Hellman key exchange and out-of-band authentication.

The Diffie-Hellman key exchange method adds an additional step to the security process, by allowing two nodes to establish a shared secret key for communication over an insecure network, using a one-way function. An illustrative example of how this key exchange works would be two paint colors mixed together; it is nearly impossible to separate them. A similar mathematical one-way function would be raising large prime numbers to the power of large numbers. Given sufficiently large numbers, even today’s supercomputers will have a hard time reversing this operation.

In addition to the hacker community, Sigma worked hand-in-hand with security architecture experts to implement higher levels of security without negatively impacting other device features, like battery life, with the launch of S2. Features of the new security protocol include secure communication for both individual devices and cloud communications; a QR or PIN code requirement on the device itself when new local devices are added into the network so there's no window of unencrypted activity for hackers to exploit; and for cloud-accessible systems, the S2 technology routes all communications through a secure transport layer security (TLS) tunnel. All of this added security comes without diminished battery life capabilities.

The S2 framework is currently available for implementation and has been made mandatory on all devices submitted for Z-Wave certification. Existing devices will continue to be backwards compatible with the new S2 smart devices.

Rock-solid protection against most cyber intrusions will one day be a given; the market will demand it. In the meantime, Security 2 (S2) is the direct path for consumer IoT developers to ensure a secure device and make sure it interoperates with an equally secure ecosystem.

**Johan Pedersen, Product Marketing Manager, Sigma Designs**

**Image Credit: Bergserg/ Shutterstock**

* **Moral and Critical issues -**
* There may be hackers that try to bypass the security to tap into the CCTV cameras, or snoop into the browser history to collect valuable information.
* If there is a power outage in the vicinity, the home becomes vulnerable to robbery, safety, health, electrical hazards , etc.
* If there is no back-up power supply in case of an outage, this could lead to appliance in the house to be useless and not functional.