Smart Home Technologies: Applications, Security Risks, and Scaling Challenges

Introduction

Smart Homes offer vendors and innovators new applications for already existing technologies as well as a chance to create new hardware or software built on those. Unfortunately, there is no agreed upon Smart Home definition across governing agencies or vendors (EIC 2014). A more general definition of a Smart Home could be: a home which integrates smart technologies and processes to improve residents' quality of life, sustainable use of resources, health, and security (Hafidh et al. 2017). Intertek (2003) defined Smart Homes as "[a] dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely connected, monitored or accessed" (in Alam et al. 2012). In addition, this report defines Smart Homes as providing true home intelligence. This concept is well explained by Satpathy (2006). Home intelligence allows "inhabitants to live independently and comfortably with the help of technology. In a smart home all the mechanical and digital devices are interconnected to form a network, which can communicate with each other and with the user to create an interactive space."

As will be seen in the reviews of hardware and software capabilities, there is a serious gap between the aspirations of Smart Homes proponents and the existing matrix of compliance, common protocols, security and privacy regulation, low cost manufacture, and even uniform building practices which would enable home intelligence to be provided scalably and with a reasonable expectation of safety and security. Some enablers like smart phones and IoT modules are advanced beyond industry needs. Some critical enablers like common IoT protocols, uniform construction regulations, and EU compliance frameworks prove insufficient to complete the promise of intelligent homes for all (Yan et al. 2011).

1. Smart Home Technology Enablers

Smart Homes require a vast number of diverse components in order to transfer from concept to physical reality – the most basic of which are the physical and digital aspects a Smart Home resident interacts with. Smart appliances and applications must be designed in a way that they are able to interact with other parts of the Smart Home network as well as intuitive and simple for the user. As mentioned before, these are the features Intertek (2003) describes. Other hardware components, mainly sensors and actuators, must be neither seen nor heard. These components, together with data collection/processing and decision-making capabilities, achieve the home intelligence Satpathy (2006) details.

1.1 Hardware Enablers

Though this is not a complete list, the primary hardware enablers for Smart Homes include communications systems – wired (e.g. power lines, phone lines, ISDN lines, and twisted pair cables) and wireless (radio frequency, WiFi, Bluetooth) –, sensors and wireless sensor networks (WSN), and intelligent appliances and devices (including smartphones, tablets, health monitoring devices, smart objects).

1.1.1 Communications systems

Many wired and wireless systems have the advantage that most homes are already equipped with them. This makes it possible to upgrade certain aspects of these homes to become smart. Each communications system, however, has its own disadvantages, limiting important factors like speed, range, and bandwidth (Alam, Reaz, and Mohd Ali 2012). For this reason, most Smart Homes deploy multiple overlapping communication protocols to transform the hardware on-site into an Internet of Things network for the home. This overlap creates potential security risks through added complexity: software can become obsolescent or malfunction and hardware can do the same – plus simply break. The communications within the home can be tampered with or hijacked (Ali and Awad 2018), putting Smart Home residents' personal information, privacy, health, and even financial and physical security at risk. This issue will be more thoroughly discussed in a later section.

1.1.2 Sensors

Add to this a wireless sensor network which must be integrated with the systems of control and the complexity of Smart Home ventures drastically increases. These sensors (PIR, ultrasonic, RFID, pressure, temperature, current, power, water, light) embedded throughout the Smart Home allow detection of factors like room occupancy and user location, room and body temperature, current and power usage, water usage volume, light intensity (Ruman et al. 2019).

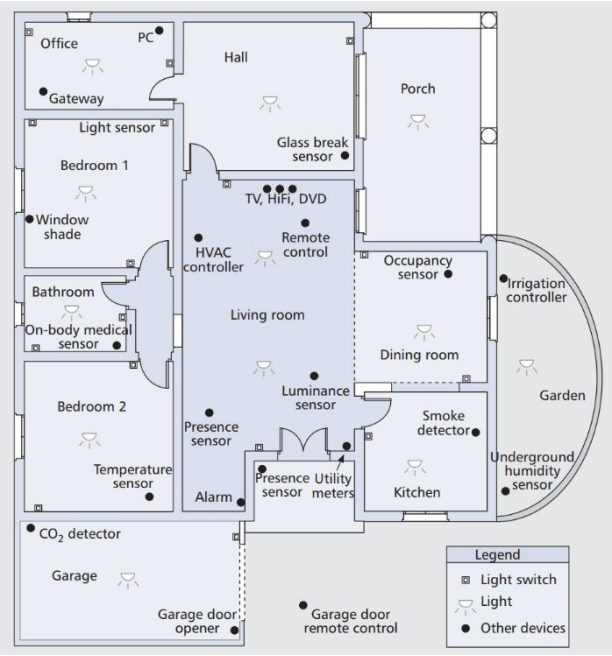

Figure 1: Example of sensor use for intelligent automation (Gomez and Paradells, 2010, p.93)

They also produce data which must be managed, stored, processed, and secured. Manufacturing chips and sensors with these data processing capabilities would be both expensive and inefficient – instead of having a centralized database that could manage and make decisions based on the data all of the sensors collect, each device would be forced to do that on its own and then somehow share the information collected with other devices inside the network. Already it becomes necessary for the Smart Home to exist not just inside the physical home. Ensuring a third-party treats residents' data responsibly and the devices that

collect it are secure becomes crucial to trustworthy Smart Home development. This necessity for interconnectedness, accessibility, and cross-communication means the inherent design and architecture of wireless sensor networks is vulnerable to a number of internal (bugs, malfunctioning sensors, accidental misuse) and external (malicious attackers, environmental events, power outages, attacks on third party developers or implementors) threats.

1.1.3 Smart Devices

What makes an object "smart" is its connection to the internet and its ability to be remotely controlled and accessed. In the domestic domain, potentially every device a resident interacts with could be replaced with a smart version. The most common smart appliances currently relate to

- Resource management: outlets, energy and water meters, HVAC systems, thermostats, and heaters, that can be monitored and controlled both on-site and online,
- Home automation: smart lighting, automatic temperature and blinds control, other embedded sensors and actuators, remote (health) care, energy efficiency,
- Entertainment: ambient lighting, smart audio and visual (A/V) systems, mood setting, smart home theaters,
- Security: IP connected CCTV, doorbells, smart locks, remote access security applications.

As can be imagined, what makes an object smart also makes it vulnerable to outside tampering. Bugeja, Jacobsson, and Davidsson (2017) found that overlapping communication protocols require software enabled command and control. In addition, many IoT driven smart appliances require manufacturer upgrades. Between them, this opens the door for malicious agents to exploit vulnerabilities which they can introduce by mimicking a household device, infecting a single appliance, infecting the network itself, inserting a trojan via upgrades or tricking the network into accepting a hostile upgrade from a third party (Bugeja, Jacobsson, and Davidsson 2017). This existential weakness means that every enabler represents an increased risk to the user: "smartness" provides increased access and control over previously inert objects. Increased data privacy, physical safety, social presence, and individual autonomy can be delivered by smart systems. They can also be destroyed by the same objects and networks.

Smartphones are a fundamental but not necessarily obvious technology enabler. Smartphones most often are the devices that control the features of many smart appliances, especially those that can be monitored and (de)activated outside the home. Due to the ubiquity of smart phones in smart city solutions, many of these solutions can be applied or modified for use in Smart Home environments. In their research into IoT solutions for smart cities, Dutta, Roy, and Chowdhury (2018, p.83) found that "[b]y embracing the potential of IoT and smartphones, traditional cities can be transformed to smart cities." The core of these cities will be Smart Homes which derive their functionality from the desires and needs of users, so they "have a bottom-up nature, initiated by the citizens" (Dutta et al. 2019, p.83). This bottom up functionality requires engagement with and intelligent optimization of day-to-day objects. In the kitchen you may find an appliance smart sous vide cooker, baking scale, refrigerator and freezer, oven, or microwave. Smart vacuums and mops may replace certain household tasks. Outside you may have a smart irrigation system, lawn mower, pool cleaner. Personal health monitoring and fitness devices could potentially connect to these devices to perform functions not yet devised (Dutta et al. 2019).

These objects have great potential when combined with an IoT network and a smart phone. They also represent significant risk to their users if not managed in a secure fashion.

In addition to providing upgraded convenience and capability, smart devices generate something entirely different and new compared to their analog versions: data. Some will be from sensors, some from the limited processors in the IoT. Processing this data can provide real time snapshots of what a user is doing and saying as well as their location, health, and habits. These enablers could result in unintended consequences if the data were to be accessed by unauthorized persons.

1.2 Software Enablers

High volumes of real-time data must be collected and analyzed in order to provide more efficient feedback and services for Smart Home users. In order to accomplish this, data is sent, stored, and processed in the cloud using data analytics. The cloud also allows flexible and dynamic control and access to the Smart Home environment. “Cloud computing makes it relatively easy to replicate control functionality at two or more locations that operate far from one another and hence, if one is lost, the other can step in” (Birman et al. 2011, p.17). Cloud-based applications and Smart Home solutions, together with internet access, provide Smart Home residents with reliable and accessible control of applications and appliances, as well as analysts and innovators with data and the ability to process it. Software processes are also necessary to make decisions in real time that directly affect and interact with Smart Home residents. Algorithms used for this purpose include artificial neural networks to predict future Smart Home environmental states, the C4.5 machine learning algorithm for residents’ behavior, fuzzy logic for home appliance control, image-processing methods for human activity recognition, case based reasoning, prediction algorithms, and multiagent systems (Alam et al. 2012).

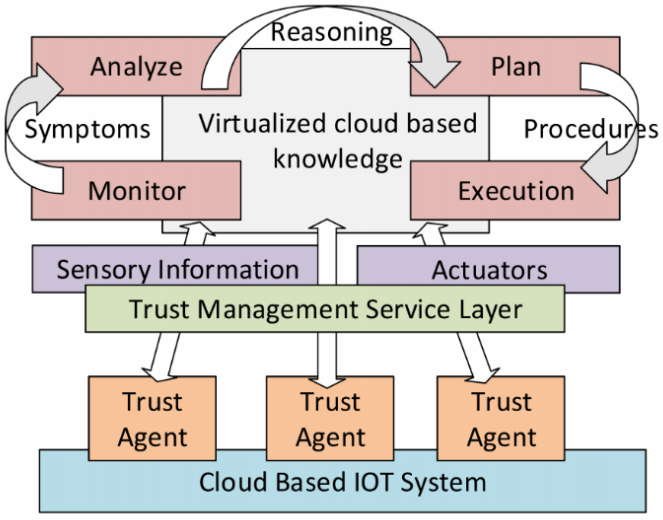

Figure 2: Example of smart home system model
(Namal, Gamaarachchi, Myoung Lee, and Um 2015)

Remote access applications allow users to control connected aspects of their Smart Home from anywhere (as long as they are connected to the internet). Smart appliances within the network of their Smart Home can also be (de)activated remotely. Besides the aforementioned use of cloud storage, IP networks, and wireless and Bluetooth communications, software applications must be designed that allow users to access and control these smart devices (Bin et al. 2016). Many (if not, eventually, all) of these Smart

Home appliances can be controlled with a mobile or voice-control virtual assistant. Several are currently compatible with various Smart Home solutions, such as Amazon's Alexa, Google's Assistant, and Apple's Siri (Ongun et al. 2018). Each of these categories represents overlapping risks, especially the virtual assistant which have potential social media connections. As later sections will demonstrate, the overarching complexity of these systems, while necessary, also presents potential failure points which endanger user data and the security of the Smart Home (Bugeja et al. 2017).

1.3 Section Conclusion and Recommendations

In conclusion, the technology exists to produce Smart Homes but not to safeguard them against security hacks, cyber-thieves, poor construction and technological obsolescence (think Moore's Law). Smart devices and IoT modules might be the path forward, using the existing power of hardware with a common software devised by Smart Home providers. Of concern, some necessary enablers of a true cost-effective home intelligence ecosystem are not yet ready to be integrated.

Private developers could establish software protocols with built in security, perhaps taking parallel technologies like blockchain, to secure the home using personal smart devices linked to the IoT enabled hardware. Likewise, the EU or a similar regulatory authority could establish a compliance regime which mandates necessary practices like modular networking and cabling which can be swapped every 3-4 years and security processes which must be inherent to all manufactured IoT as well as operating software.

Will the widespread implementation of Smart Homes define protocols, standards, and processes that will allow functional and safe smart cities? Privacy and security concerns have already been brought to attention due to virtual assistants. So too the danger of security and safety using smart devise with IoT software for buildings. There is still little research done on these and that seems an obvious next step.

2. Smart Home Application Area(s)

As mentioned previously, Smart Homes present an opportunity to develop new systems and technologies as well as new applications for already existing ones. Smart appliances – everyday devices and objects that deliver internet connectivity, home automation, and remote access and control – working as an interconnected whole make a home "smart" (Alam et al. 2012). Smart, however, does not mean secure. Smart appliance security (or lack of it) represents the most important application area for Smart Homes (Ali and Awad 2018). As a result, technology ethicists and security experts have recommended smart appliances be purpose built with both secure networks and secure hardware (Chong et al. 2019). IoT driven smart appliances related to home security are necessary to safeguard the privacy and physical integrity of the home (Ruman et al. 2019). Whether blockchain (software), IoT (both hardware and software) or encrypted chip (hardware) driven, end to end security for smart appliances provides the critical trust and security necessary to eventually scale, manufacture, and upgrade Smart Homes (Dorri et al. 2017; Yan et al. 2011).

2.1 Smart Appliances

It is necessary to understand the qualities and functions – each of which is exploitable and each of which needs to be made secure – that make objects smart in order to discuss purpose

built secure hardware and software. Smart functionality has become more common with everyday devices and could become the standard format for most appliances present in residential homes. “There is a manifest destiny that more and more object types will become smarter […] To get the most value, interoperability standards will be needed to enable plug-and-play so that all objects obey a suite of smart object protocols” (Eguchi and Thompson 2011, p.909). In part, the world’s aging population will drive this as needs for accessibility, health support, and predictive care can be met in-home via smart appliances and applications. Alam, Reaz, and Mohd Ali (2012) argue that by 2050, 20% of the world be 60 years or older – prime candidates for Smart Homes possessing a predictive IoT network, specialty health appliances and assistive technologies. These types of appliances represent the apex of complexity and vulnerability.

Even appliances not directly related to security or processing personal information can pose potential risks. Take, for instance, a smart fridge or smart vacuum cleaner: “These devices, which include the smart refrigerator, provide mechanisms through which botnets can operate and if appropriately customized, can gather the information needed for identity crimes to be perpetrated” (Holm 2016, p.7). Taken to the extreme, well prepared and highly organized malicious agents with persistent threat capability can hijack systems, blackmail homeowners by locking down critical systems or stealing sensitive documents, hack baby monitors and social media for bullying or stalking, and even cause medical crises. Bugeja, Jacobsson, and Davidsson (2017, p.4) found creative ways to manipulate smart devices: “One attack demonstrated by researchers is to set smart lightning into a strobe pattern that can possibly trigger epileptic seizures to people.”

Inconsistent, or even nonexistent, software updates not only pose an inconvenience to users who find that their devices no longer interfaces with other applications – thereby losing the capabilities that made it smart in the first place – they represent another pathway for malicious threats. Smart thermostats, for example, can be attacked through their own firmware update scripts (Moody and Hunter 2016). Vulnerabilities which haven’t been patched provide easy access to the entire network of devices connected to the thermostat (or refrigerator, baby monitor, smart lighting, home computer, smart device, etc.). Consider that Samsung’s warranty for their smart fridge with Family Hub contains no information about its software or how it can be updated (Samsung, 2017).

The famous Roomba, a smart vacuum cleaner, represents a dual threat to the Smart Home. First, it creates a virtual map of its environment and is able to track its movement within it. As robotic vacuum cleaners continue to add more advanced sensors, lasers, and even cameras, attackers are able to access these features if they have accessed the network (Wolfe, 2017). Second, it provides interconnected access to the same networks as refrigerators and baby monitors but has additional vulnerabilities. “Using sensory channels (e.g., light, temperature, infrared), an adversary can successfully attack systems. Specifically,

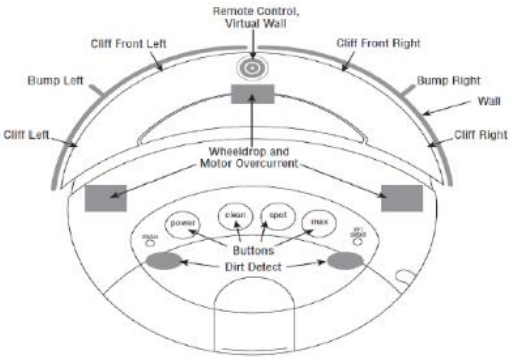

Figure 3: Diagram of Roomba sensors
(Uluagac, Subramanian, and Beyah 2014, p.3)

the adversary can (1) trigger existing malware, (2) transfer malware, or (3) combine malicious use of different sensory channels to increase the impact of the attack on CPS devices." (Uluagac, Subramanian, and Beyah 2014, p.1)

2.2 Section Conclusion and Recommendations

One solution to security risks associated with smart objects is a centralized security management system that integrates and controls all software related activity in the home. Simpson, Roesner, and Kohno (2017, p.8) concede that "quickly patching IoT devices to remove vulnerabilities is not always straightforward due to the longevity of some home appliances, the lack of software update capabilities, and the challenges of predicting a convenient time to update." Other security experts suggest that appliances could best be handled by external network operators, as the services they provide are ubiquitous and already present in a majority of homes (Batalla, Vasilakos, and Gajewski 2017). Augmenting device-level protection with software defined networking (SDN) technologies allow network monitors to "dynamically block/quarantine devices, based on their network activity and on the context within the house such as time-of-day or occupancy-level" (Sivaraman et al. 2015, p.1). It is obvious however, that due to the enormous risk connected smart objects pose to personal, health, and financial security, more needs to be done to secure them:

There is a general need for the integration of security in design. Risk analysis perspectives are typically put on the connected home from the outside, i.e., risk analysis is not included in the design and development phases of Smart Home automation systems and technologies. Security in design is crucial for mitigating the threats posed at IoT- connected homes, especially in terms of malware mitigation, access control, and privacy disclosure. Such sound security management must also contribute to the overall system requirements, something that is facilitated for during system development. (Jacobsson, Boldt, and Carlsson 2016, p.7)

Centralized power sources and security systems also represent threats if not mitigated with disaster recovery and cloud-based reboot options due to the permanent risk of failure. "Even decentralized control systems still have the problem that the cable or power supply is a single point of failure, and this is the downside to control" (Roshan and Ray 2016). If a server goes down, that means people could potentially be left without lights, heating, security, and access to other smart devices and objects simply because they've lost their internet connection (Hern 2017). These devices must be designed with a failsafe in mind.

3. Challenges to Large-scale Smart Home Deployment

There exists the technology to produce Smart Homes right now, there is no real ability to scale production in a safe, secure, economically viable fashion. Unless these open challenges to scalability are remedied, Smart Homes represent a significant threat to the privacy as well as personal and financial security of their owners (Zeng, Mare and Roesner 2017).

3.1 Overview of Open Challenges

The open challenges that should be addressed first include the interoperability of hardware and software systems, the economic viability of manufacturing secure, resilient sensors and devices, core compliance to international privacy and security regulations and the overall

integration of appliances, networks, electric grids and sensors into a cohesive working unit that provides low effort no effort security for the homeowner.

Hardware issues include sensor reliability and endurance as well as range limits associated with smart devices (Apthorpe, Reisman, and Feamster 2017). Software in some cases remedies these concerns but poses data privacy, security and interoperability limits (Zhang et al. 2017). Fundamentally, these challenges stem from unresolved confidentiality and privacy concerns related to gaps in uniform manufacturing, communication, and command and control systems of smart sensors, smart appliances and Smart Home management systems.

Fundamentally, there exists the working technology to build a scalable Smart Home that can stay secure and resilient long term. At this time no one manufacturer or distributor owns all the patents necessary to deliver an entire home purpose built and designed as a cohesive unit. That means that every Smart Home will be cobbled together by architects and engineers who have to create management solutions that integrate potentially incompatible systems and safeguard the data and security of those systems from the smallest external sensor channels to the cloud based agents managing grids, IoT network updates, and external security programs.

3.2 Hardware and Manufacturing Challenges

The problem of scalability is in part related to wide scale of actual things – the hardware – that make up a Smart Home. Smart Home devices range from tiny sensors that determine body temperature or light intensity to smart grids which service entire residential or commercial areas. A Smart Home requires integration of hundreds of various sized devices, which complicates the large-scale deployment of Smart Homes (Hui, Sherratt, and Sanchez 2017).

Assuming that these can be effectively integrated and secured, they must still be built, deployed in the home and made functional long term. Mass producing this number of devices and ensuring they can withstand various environmental and thermal conditions would be critical to ensure uninterrupted service (Zheng et al. 2018). These devices communicate inside a network and often with each other. Some utilize Bluetooth which limits their range; others communicate via WiFi which would require ubiquitous and extremely reliable internet connection (Müller, Waldvogel, and Kaiser 2017). Sensors are of particular concern because they must be small and light enough that they can be seamlessly incorporated into intelligent objects and home infrastructure. They must also have sufficient battery life to stay active when needed but stay dormant when not needed in order to prevent downtime sensor noise (El-Sayed W., El-Bakry, El-Sayed, S. 2019). These represent significant manufacturing hurdles on their own. Another hardware challenge is found in Moore's law.

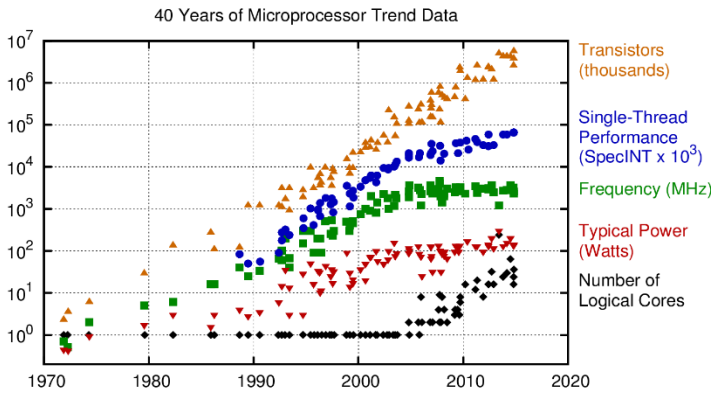

Figure 4: Moore's Law (Rupp 2015)

How often would Smart Home components (wires, sensors, devices) have to be replaced after being improved, and who would be responsible? Who would absorb the cost? In areas prone to natural disasters (hurricanes, earthquakes, tornadoes), is it possible to ensure devices and communications systems are resilient enough to withstand them? (Laplante, P., Voas, and Laplante, N. 2016)

3.3 Interoperability and compliance

All of these point to a common theme: Smart Home devices need to be easily upgradable and replaceable. This means they need to be of low cost and high flexibility when working with other members of the IoT to insure scale. A lack of interoperability is the next obstacle standing in the way of large scale Smart Home deployment. Various technologies in various domains must conform to respective sets of standards (such NIST or HIPAA in the United States or the GDPR in the EU). However, there are currently no cohesive, cross-agency standards for Smart Home solutions (Theoharidou, Tsalis, and Gritzalis 2017). These different standards result in entirely different kinds of objects duplicating the same data or perform the same job but on different communication bandwidths or with different sensors. The potential data leakage if these are not all combined, validated and secured would be immense.

But as previously stated, there is no uniform regulation to validate what will work and to penalize manufacturers who fall short of the mandate. In addition, Moore's law guarantees that either regulatory bodies will lag behind technological changes, or – in the case of overarching compliance regimes like the European Union's GDPR – the burden to properly update individual technologies may represent a direct threat to the economic viability of sensor and appliance production (Seo et al. 2018).

Along the lines of compliance, Smart Home technologies and the agents that sell them may potentially break various data and privacy protection laws as Smart Home solutions and objects become available across borders. The European Union wrote the GDPR into effect in 2016, but other nations like the USA must interpret the language of potentially outdated data protection laws in order to apply to them to Smart Homes. Technologies available in different countries have the additional hurdle of being compliant with multiple, possibly conflicting, sets of standards. This means that regulatory standards must be also made interoperable and cohesive. While the IoT network might be the obvious place for a manufacturer to look, the proposed security fixes in Section 2 represent an entirely meta-national issue of data movement in the internet and cloud. Enormous amounts of data must be secured and stored in an originating country, potentially one different than where the Smart Home is located, and possibly transferred to a different one. With that movement comes competing privacy laws (Seo et al. 2018).

3.4 Trust and Privacy

Trust is another important aspect of Smart Homes. People must be able to live without fear. Since we have exposed and discussed the potential for malicious agents to hijack sensors and IoT networks for sabotage, theft and stalking, there is legitimate concern that the same virtual assistant which records the user in order to offer better service can be manipulated to provide false information, deliver bullying messages, or simply provide users' most private information to external parties without consent. In the same way, residents' smart lighting system monitors their movement to better predict which room needs light in order to save energy costs. But these movements also represent a direct threat to physical security if stolen or shared with malicious agents. Both smart devices may require such protocols and they may

have legal contracts which stipulate the sharing of data to the manufacturer, the security provider, and third parties that provide firmware updates or data processing capabilities. How can a homeowner truly trust that these devices have been calibrated in a way that does not infringe on their privacy and safety? (Gkotsopoulou et al. 2019)

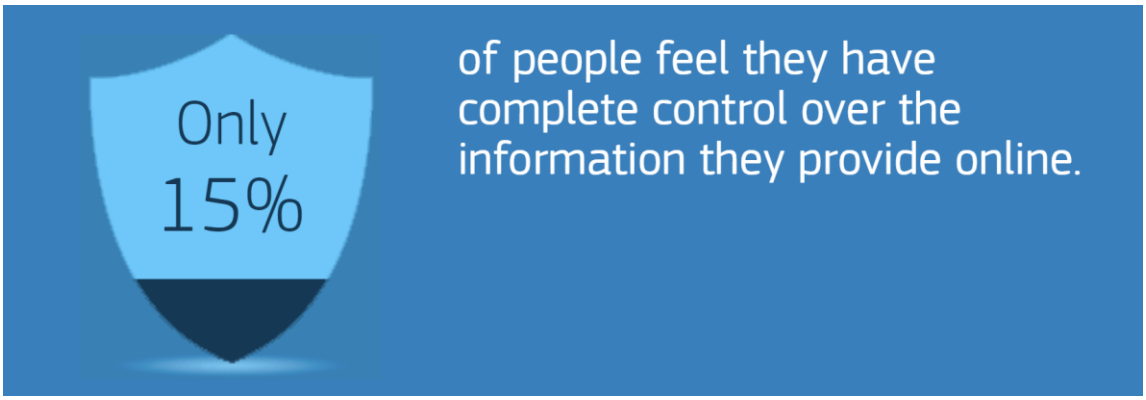

Figure 5: EU GDPR trust statistic (European Commission, 2016)

How is this information used? How is it stored? These questions represent significant legal and regulatory hurdles to long term scale of Smart Homes because competing jurisdictions could allow unscrupulous manufacturers to exploit gaps in security and data control to build a low cost and, as a result, low security Smart Home. It is this potential for rushing production without properly testing security and securing data that could erode trust in the same way that the 2017 Equifax breach had. Consider how Equifax posed the situation to its members regarding a data breach that released the personal information of roughly 147 million customers: “Equifax denies any wrongdoing, and no judgment or finding of wrongdoing has been made” (Equifax, 2017). Marcus (2018, p.555) notes that the current solutions for dealing with data breaches are inadequate: “Private litigation like consumer class actions and shareholder lawsuits each face substantive legal and procedural barriers. States have their own data security and breach notification laws, but there is currently no unifying piece of legislation or strong enforcement mechanism.” While this proves more integration of standards will help improve trust, for Smart Home providers, the economic loss from even a single breach might be X in direct legal damages and 10X to 20X in lost revenue due to lack of consumer trust (Sharf, 2014).

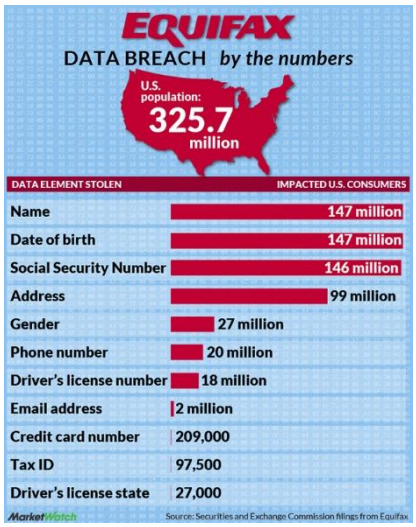

Figure 6: Equifax Data breach
(SEC in MarketWatch, 2018)

Unless providers of Smart Homes take a progressive and highly adaptive approach to securing consumer data which includes security by design appliances, data protection at both an IoT and cloud level and a comprehensive engagement with regulatory authorities to help shape future policy, then lack of trust will prevent even legitimately secure homes from being sold *en masse*. In part, these issues exist because manufacturers view a Smart Home as a technology project rather than a place which represents the safe space for a data producing users who require both security and comfort. Timo et al. (2018, p.1629) argue that the "smart home so far has targeted the home primarily as a technological space, rather than a place formed by routines and interaction. By becoming more sensitive to the routines and practices of users" both the technological hurdles and data compliance concerns could be effectively addressed.

3.4 Section Conclusion and Recommendations

To sum up in a quote, the functional issues with scaling are tied to a lack of interoperable capability of smart devices and systems. Blumendorf (2013, p.156) confirms that "[t]he utilized ICT systems – hardware and software – as well as the building itself will need to be able to evolve over time and to adapt to changing needs." These needs range from accessibility to uninterrupted and reliable service, from real-time decision making to confidentiality of personal data.

These devices and systems are also not configured and designed with security as more than an afterthought. Smart appliances, software vulnerabilities, and insecure internal Smart Home networks (including WSN) are not correctly secured and therefore act as low hanging fruit for attackers wanting to collect personal information, cause financial or personal harm to Smart Home residents, or for unlawful surveillance purposes. Because there is no industry- or agency-wide consensus on Smart Home definitions, protocols, and standards, it is not possible to manage or monitor the design, construction, and implementation of these homes and their associated devices. There is no wide-spread or functional way to ensure manufacturers avoid putting Smart Home residents at risk.

As previously discussed, the many current obstacles standing in the way of large scale Smart Home deployment are diverse but closely related. A conclusion one could draw from this report is that a potential solution would be a top-down approach guided by industry experts in security, sustainability, design, and engineering to provide a framework and systems architecture in order to solve many of these problems. Regardless, the only way to resolve them is through unified administrative and manufacturing efforts.

Conclusion and Recommendations Regarding Smart Home Technologies

Smart Homes represent a technological leap forward which promises to provide users with unprecedented control over their daily lives. At the heart of a Smart Home will be the Internet of Things connecting various intelligent appliances, a smartphone (or similar device), cloud driven software, and outside services such as a smart grid. Each of these also represent a direct threat to the home itself and the users within it. The hardware and software linked together to provide unparalleled access to user data for positive predictive applications can also be exploited by malicious actors for theft, criminal mayhem, blackmail, and even terrorism. They can be subverted for stalking, home invasion or simple data theft like the Equifax data breach. Unsecured Smart Homes represent a significant danger to user privacy and security.

Builders and providers must immediately begin to build security into every device, to provide cohesive interoperability standards which are secure by design and which engage the cloud, internet, and third party data streams (from smart grids, cable television, etc.) through secured channels with inbuilt threat assessment. Intelligent objects are both innovation enablers and security risks. If they are to provide the promised future of smart living, they need to be managed intelligently through common global standards focused on data privacy, multi-layer security, and quality manufacturing.

References

Alam, M.R., Reaz, M.B.I., Mohd Ali, M.A., 2012. A Review of Smart Homes — Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* [online], 42(6), 1190-1203.

Ali, B., and Awad, A., 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* [online], 18(3), 817.

Apthorpe, N., Reisman, D., and Feamster, N., 2017. A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. *ArXiv* abs/1705.06805(2017). Available from: http://arxiv.org/abs/1705.06805 [4 October 2019].

Aminikhanghahi, S., Wang, T., and Cook, D.J., 2018. Real-time change point detection with application to smart home time series data. *IEEE Transactions on Knowledge and Data Engineering* [online], 31(5) (2018): 1010-1023.

Batalla, J.M., Vasilakos, A., and Gajewski, M., 2017. Secure Smart Homes: Opportunities and Challenges. *ACM Computing Surveys* [online], 50(5).

Birman, K.P., Ganesh, L., and Renesse, R.V., 2011. *Running Smart Grid Control Software on Cloud Computing Architectures* [online]. Cornell University.

Blumendorf, M., 2013. Building sustainable smart homes [online]. *First International Conference on Information and Communication Technologies for Sustainability*, 14-16 February, 2013, Zurich, SUI. Zurich: ETH.

Bugeja, J., Jacobsson, A., and Davidsson, P., 2017. An analysis of malicious threat agents for the smart connected home [online]. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 13-17 March 2017, Kona, HI, USA. Kona: IEEE.

Chong, I., Xiong, A., and Proctor, R.W., 2019. Human factors in the privacy and security of the internet of things. *Ergonomics in Design* [online], 27(3), 5-10.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: The case study of a smart home [online]. *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 13-17 March 2017, Kona, HI, USA. Kona: IEEE.

Dutta, J., Roy, S., and Chowdhury, C., 2019. Unified framework for IoT and smartphone based different smart city related applications. *Microsystem Technologies* [online], 25(1), 83-96.

Eguchi, A. and Thompson, C., 2011. Towards a Semantic World: Smart Objects in a Virtual World. *International Journal of Computer Information Systems and Industrial Management Applications* [online], 3(1), 905-911.

El-Sayed W.M., El-Bakry, H.M., El-Sayed, S.M. 2019. Integrated data reduction model in wireless sensor networks. *Applied Computing and Informatics* [online].

Environmental Industries Commission, 2014. *Getting the green light: Will smart technologies clean up our city environments?* [online]. London: EIC.

Equifax, 2017. *Equifax Data Breach Settlement* [online]. Available from: https://www.equifaxbreach settlement.com/ [6 October 2019].

European Commission, 2016. Data protection: Better rules for small business [online]. Brussels: European Commission. Available from: https://ec.europa.eu/justice/smedataprotect/index_ en.htm [11 Oct 2019].

Gkotsopoulou, O. et al., 2019. Data Protection by Design for Cybersecurity Systems in a Smart Home Environment [online]. *2019 IEEE Conference on Network Softwarization (IEEE NetSoft)*, 24–28 June 2019, Paris, France. Paris: IEEE.

Gomez, C. and Paradells, J., 2010. Wireless Home Automation Networks: A Survey of Architectures and Technologies. *IEEE Communications Magazine* [online], 48(6), 92-101.

Hafidh, B., Al Osman, H., Arteaga-Falconi, J.S., Dong, H., and El Saddik, A., 2017. SITE: The Simple Internet of Things Enabler for Smart Homes. *IEEE Access* [online], 5(1), 2034-2049.

Hern, A., 2017. How did an Amazon glitch leave people literally in the dark? *The Guardian* [online], 1 March 2017. Available from: https://www.theguardian.com/technology/2017/mar/01/ amazon-web-services-outage-smart-homes [3 October 2019].

Holm, E., 2016. The role of the refrigerator in identity crime. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* [online], 5 (1), 1-9.

Hossain, M., Fotouhi, M., and Hasan, R., 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things [online]. *2015 IEEE World Congress on Services*, 27 June – 2 July 2015, New York, NY, USA. New York: IEEE.

Hui, T.K.L., Sherratt, R.S., and Diaz Sanchez, D.D., 2017. Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems* [online], 76(1): 358-369.

Jacobsson, A., Boldt, M., and Carlsson, B., 2016. A risk analysis of a smart home automation system. *Future Generation Computer Systems* [online], 56(1), 719-733.

Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G., and Wulf, V., 2017. The catch (es) with smart home: Experiences of a living lab field study [online]. *2017 CHI Conference on Human Factors in Computing Systems*, 6-11 May, 2017, Denver, Colorado, USA. New York: ACM.

Laplante, P.A., Voas, J., and Laplante, N., 2016. Standards for the Internet of Things: A case study in disaster response. *Computer* [online], 49(5), 87-90.

Li, M. et al., 2018. Smart Home: Architecture, Technologies and Systems. *Procedia Computer Science* [online], 131(1), 393-400.

Lobaccaro, G., Carlucci, S., and Löfström, E., 2016. A Review of Systems and Technologies for Smart Homes and Smart Grids. *Energies* [online], 9(5).

Manvell, D., 2015. Utilising the strengths of different sound sensor networks in smart city noise management [online]. *EuroNoise Conference 2015*, 31 May – 1 June 2015, Maastricht, NED.

Marcus, D.J., 2018. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke Law Journal* [online], 68 (555), 555-593.

Moody, M. and Hunter, A., 2016. Exploiting known vulnerabilities of a smart thermostat [online]. *14th Annual Conference on Privacy, Security and Trust (PST)*, 12-14 Dec. 2016, Auckland, New Zealand. Auckland: IEEE.

Mulholland, K., Pitt, M., and McLennan, P., 2016. Changing Societal Expectations and the Need for Dynamic Asset Lifecycling and Obsolescence Management [online]. *CIB World Building Congress 2016: Advancing products and services*, 30 May – 3 June 2016, Tampere, FIN.

Müller, R., Waldvogel, M., and Kaiser, D., 2017. HomeCA: Scalable Secure IoT Network Integration [online]. Konstanz: University of Konstanz.

Namal, S., Gamaarachchi, H., Myoung Lee, G., and Um, T.W., 2015. Autonomic Trust Management in Cloud-based and Highly Dynamic IoT Applications [online]. *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*, 9-11 Dec 2015, Barcelona, ESP. Barcelona: IEEE.

Ongun, T., Oprea, A., Nita-Rotaru, C., Christodorescu, M., and Salajegheh, N., 2018. The House That Knows You: User Authentication Based on IoT Data [online]. *2018 ACM SIGSAC Conference on Computer and Communications Security*, 15-19 October, 2018, Toronto, CAN. New York: ACM.

Owens, J.C., 2018. The Equifax data breach, in one chart. *MarketWatch* [online], 10 Sep 2018. Available from: https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07 [12 Oct 2019].

Roshan, R. and Ray, A.K., 2016. Challenges and risk to implement IOT in smart homes: an Indian perspective. *International Journal of Computer Applications* [online], 153(3), 16-19.

Ruman, R.M., Das, M., and Mahmud, S.M.I., 2019. IoT based smart security and home automation system. *Asian Journal For Convergence In Technology (AJCT)* [online], 5(1).

Rupp, K., 2015. *40 Years of Microprocessor Trend Data* [online]. Vienna. Available from https://www.karlrupp.net/2015/06/40-years-of-microprocessor-trend-data/ [11 Oct 2019].

Samsung, 2017. *22 cu. ft. Capacity Counter Depth 4-Door Flex™ Refrigerator with Family Hub™ (2017)* [online]. Available from: https://www.samsung.com/us/support/service/warranty/RF22M9581SR/AA [6 October 2019].

Satpathy, L., 2006. *Smart housing: Technology to aid aging in place: New opportunities and challenges*, Dissertation (M.S.), Mississippi State University.

Seo, J. et al., 2018. An Analysis of Economic Impact on IoT Industry under GDPR. *Mobile Information Systems* [online], 2018(1).

Sharf, S., 2014. Target Shares Tumble As Retailer Reveals Cost Of Data Breach. *Forbes* [online]. 04 August 2014. Available from: http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach [06 October 2019].

Simpson, A.K., Patel, S.W., Roesner, F., and Kohno, T., 2017. Securing vulnerable home IoT devices with an in-hub security manager [online]. *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. 13-17 March 2017, Kona, HI, USA. Kona: IEEE.

Sivaraman, V. and Vishwanath, A., 2015. Network-level security and privacy control for smart-home IoT devices [online]. *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)*, 19-21 Oct. 2015, Abu Dhabi, UAE. Abu Dhabi: IEEE.

Theoharidou, M., Tsalis, N., and Gritzalis, D., 2017. Smart home solutions: privacy issues. *In*: Van Hoof, J., Demiris, G., and Wouters, E.J.M. *Handbook of Smart Homes, Health Care and Well-Being* [online]. Zurich: Springer, 67-81.

Uluagac, A.S., Subramanian, V., and Beyah, R., 2014. Sensory channel threats to cyber physical systems: A wake-up call [online]. *2014 IEEE Conference on Communications and Network Security*, 29-31 October 2014, San Francisco, CA, USA. San Francisco: IEEE.

Wolfe, J., 2017. Roomba vacuum maker iRobot betting big on the 'smart' home. *Reuters* [online], 24 July 2017. Available from: https://www.reuters.com/article/us-irobot-strategy-idUSKBN1A91A5 [06 October 2019].

Ye, Y., Qian, Y., and Sharif, H., 2011. A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid [online]. *Faculty Publications in Computer & Electronics Engineering (to 2015)*. 89(1).

Zeng, E., Mare, S., and Roesner, F., 2017. End user security and privacy concerns with smart homes [online]. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 12-14 July, 2017, Santa Clara, CA, USA. Santa Clara: USINEX.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., and Shen, X., 2017. Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine* [online] 55(1), 122-129.

Zheng, P, Sang, Z., Zhong, R.Y., and Xu, X., 2017. Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering* [online], 13(2), 137-150.

Zhou, B. et al., 2016. "Smart home energy management systems: Concept, configurations, and scheduling strategies." *Renewable and Sustainable Energy Reviews* [online], 61(1): 30-40.