On a Territorial Notion of a Smart Home

Shreenidhi Ayinala
Frisco ISD
Frisco, TX, USA
shreenidhi.ayinala@gmail.com

Renita Murimi
University of Dallas
Irving, TX, USA
rmurimi@udallas.edu

ABSTRACT

A home is an emotional investment, a retreat, a safe space. The various elements of a home create an incomparable experience from other physical spaces. Alongside these elements, a home instills belonging and familiarity, creating a bond between the boundaries of a home and the individual. However, this bond may be destroyed through the intrusion of uninvited individuals, and this intrusion is fueled by the lack of security in smart home devices. Although they provide convenience, smart home devices are capable of being breached for various reasons, some being due to vulnerable sensors, faulty data protection mechanisms, and vulnerability to malware and flaws. In this paper, we analyze a smart home based on the theory of territoriality. By incorporating the theory of territoriality, our goal is to analyze how cyberattacks on smart devices can disrupt an individual's experience of a home.

CCS CONCEPTS

• Ubiquitous and mobile computing • Theory, concepts, and paradigms • Ambient intelligence.

KEYWORDS

Smart Homes, Territory, Attacks, Taxonomy

ACM Reference format:

Shreenidhi Ayinala and Renita Murimi. 2022. On a Territorial Notion of a Smart Home**.** In *Proceedings of CySSS '22: The 1st Workshop on Cybersecurity and Social Sciences Proceedings, May 30, 2022, Nagasaki, Japan.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3494108.3522766

1 Introduction

The quest to define, measure, and develop smartness is an innate predisposition of both human and animal societies. Defining intelligence as "an agent's ability to achieve goals in a wide range of environments", [17] provided a framework for intelligence in the form of three components – an agent, the environment, and goals. Although initially narrowly defined by niche intelligence tests, Gardner's theory of multiple intelligences broadened the discourse about various kinds of intelligence [13]. Simultaneously, studies of animal intelligence have revealed remarkable insights about their prowess in adapting to their environments, instead of measuring their intelligence relative to that of other species, including humans [37]. As the measures and definitions of intelligence have progressed, so has their foray into the tools that we use.

It is no longer that we label human or animals as intelligent or smart; we now also measure tools and technology by their smartness. Ericsson first coined the term "smartphone" in 1997 for their GS88 phone, which was equipped with a 16-bit operating system, POP3 email, world clock, text messaging, and a browser among other features [9]. Codenamed as "Penelope", the GS88 smartphone never made it to market due to multiple reasons including battery life considerations and market fit. Almost a decade later, Apple's iPhones set the ball rolling on a consumer market for smart devices that combine telephony and computing capabilities – a USD 378B market as of the year 2020 [34]. Smartness, now, has become a coveted label for a plethora of devices and applications, enveloping the obvious such as computers, cars and robots [7] as well as quirky objects such as smart cat litter trays [20], smart salt shakers [12], and smart egg trays [27]. The notion of smart objects implies, at the very least, the following: computing, sensors, and connection to the Internet. These smart objects, known as the Internet of Things (IoT), encompass both consumer electronics and industrial automation tools ranging from structural health monitoring devices [33], electricity grids [31], and other public utility services, as well as infrastructure and defense [11]. For convenience and efficiency, various smart objects are bundled according to their utility or proximity as smart homes, smart buildings, and smart cities. The IoT market alone is upwards of USD 750B as of 2020 and intersects with other important technological phenomena of our time: big data, machine learning, artificial intelligence, and blockchain [14].

However, the rapid rise of smart environments is being paralleled with another rapid increase, that of attacks on smart devices. Attacks on computing infrastructure began with the benign

CySSS '22, May 30, 2022, Nagasaki, Japan
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9177-1/22/05..$15.00
https://doi.org/10.1145/3494108.3522766

malware of the eighties and have since morphed into a global enterprise for infiltrating systems, theft, and manipulation of data. The outcomes of these attacks have been varied, ranging from personal identity theft to disruption of infrastructure such as the shutdown of the electricity grid in Ukraine [19], the diversion of wastewater plant outputs [26] and tampering with medical equipment [10]. The frequency and severity of these cybersecurity incidents are increasing at an alarming rate, with recent statistics pointing to upwards of 80,000 attacks every day around the world [30]. Out of these, 40% of smart homes have at least one device vulnerable to cyber-attacks [2], and another estimate suggests that smart homes could experience more than 12, 000 attacks in a single week [6].

The contributions of this paper are three-fold. First, we define the notion of a smart home based on the Porteousian theory of territoriality [28], which ascribes three distinct territorial attributes of identity, security, and stimulation to a home. Second, our paper examines the landscape of breaches on smart homes against the backdrop of the Porteousian theory of a home as a territorial construct, and offers a taxonomy of attacks on smart homes. Finally, our paper calls for the need to distinguish between smart home network that are merely net-smart instead of being smart, and emphasizes the need for holistic security and privacy-focused design and implementation of smart home networks.

Current cybersecurity research has focused largely on frameworks, solutions, and countermeasures for combating cyber-attacks at the corporate and individual levels. At the corporate level, elaborate cybersecurity awareness initiatives such as phishing campaigns and hackathons, consortia of academic, industrial, and government efforts to develop secure computing infrastructure, and vendors of cybersecurity solutions are involved in multi-pronged efforts to boost the security posture of our global computing grid. At a smaller scale, these solutions are also available to individuals for use in their personal applications such as encrypted communications and antimalware licenses. However, as our living environments become increasingly outfitted with smart objects, it is also important to think about the intermediate link between the personal and the corporate. One such link is that of the smart home, which now includes a multitude of objects that are equipped with sensors and connected online thus creating a new frontier for smart computing and simultaneously widening the cybersecurity attack surface in our environments.

Our paper focuses on the smart home and analyzes the kinds of attacks that have been propagated against smart home environments. Smart home attacks, while following the basic blueprint of cyber-attacks, are also unique in their degree of their cybersecurity vulnerability. These attacks are propagated primarily by poor device and network configuration, inadequate computing required for cryptographic protection, as well as a general lack of user awareness of the "smartness" of these devices. The rest of this paper is structured as follows. Section 2 offers an overview of the notion of a home from an anthropological point of view and situates a smart home within this viewpoint. In Section 3, we present a taxonomy of cyberattacks on smart home to illustrate how smart homes contradict the territorial expectations of a home. Section 4 presents socio-technical implications and directions for future research. Finally, Section 5 concludes the paper.

2 Expectations of a home

Jacobson defined a home as a space where "we close the door behind us when we enter our homes" [15]. Over time, homes have evolved into complex and sophisticated structures integrating technology into our daily lives. Objects such as watches, speakers, air conditioning systems, and ovens did not traditionally incorporate Internet connectivity, however, with the concept of smartness, these objects are now able to communicate with other devices, and can be remotely accessed and manipulated. Hackers are not only able to extract personal information, but are also able to spy on the occupants of the home. This violation erases boundaries, where we no longer are able to close the door to outsiders behind us.

Our paper analyzes a smart home based on the theory of territoriality, which was first proposed by Douglas Porteous [28]. Territoriality proposes the idea that individuals exert jurisdiction over his/her personal space. Individuals may exert their control by defining boundaries over a variety of entities, including his/her personal information and belongings. The Porteousian definition of a home is one that provides an individual with three essential territorial satisfactions - identity, security, and stimulation. With smart home breaches, attackers can gain unauthorized jurisdiction over these personal entities and impinge upon the aspects of identity, security, and stimulation. While identity and security are self-explanatory, stimulation is defined as the ability to manipulate and personalize the living spaces within a home. Security is directly breached when prying eyes are intruding on the enclosed areas of a home, which can lead to serious consequences to the individual's safety and privacy. Identity and stimulation are lost in the process of a breach as the intruder establishes a sense of fear and domination, diminishing any opportunities for self-nourishment or self-development.

Cybercrime is more than stealing sensitive information and breaching computers: the emotional and psychological effects are significant [1, 5, 16]. Instead of stealing information, a hacker's intention may be to cause discomfort through acts such as cyberstalking, which then can lead to actions such as doxing, defamation, microtargeting, and blackmail. In [4], the authors found that victims of cyberattacks felt a range of emotions during or after a breach including fear, panic, betrayal and bodily reactions such as tense muscles, fast breathing, or a trembling voice. Further, cyberattacks could lead to unconstructive action tendencies such as the need to isolate oneself or stop utilizing internet-connected devices, as well as constructive action tendencies such as changing privacy settings or attempting to regain control of the device. For a legal perspective of cyber breach-induced harms, the reader is referred to [3, 8, 35]

3 Taxonomy of attacks on a smart home

More and more of the products that we utilize on a daily basis are becoming technologized. For example, the original purpose of a refrigerator is to store food at a cold temperature and slow down the activity of bacteria. Smart refrigerators, however, not only store food but have screens in which consumers can pull up a recipe, connect to the Internet, send and receive notes, and remotely place orders to replenish the contents. Watches, speakers, toothbrushes, and light bulbs have been programmed to perform activities that traditional versions of these products could not perform. Examples of popular devices that are equipped with sensors include Amazon's Alexa, Phillip Hue's Light Bulb, and Fredi's baby monitor. Although these advancements produce convenience and easier access, they pose serious security risks. To better understand how to prevent breaches of smart devices, it is imperative to take note of the vulnerabilities that exist. To achieve this, we researched past attacks of a selected number of devices and categorized them based on their vulnerabilities. We chose a total of eighteen distinct smart home devices to research - air conditioners/HVAC systems, baby monitors, photo frames, doorbells, light bulbs, refrigerators, routers, ovens, washers, thermostats, vacuum cleaners, voice assistants, wearable technology, plugs, smart buildings, elevators, TVs, and vehicles. We found that attacks on smart home devices fell into one of three categories – sensors, data protection, and malware. However, some of these attacks could fall into more than one category. Below, we describe attacks in each category.

Sensors in smart home devices: Sensors in home IoT devices span the gamut, ranging from applications such as baby monitors, light bulbs, thermostats, vacuum cleaners, voice assistants, and TVs. These sensors are responsible for tasks such as sensing motion, sound, and temperature while communicating with other components of the device and are also capable of being hacked through their Internet connection capabilities. For example, in 2020 a US-Chinese university team manipulated voice assistants to unlock devices, take repeated selfies, make fraudulent calls, and make it read the user's text messages [36]. They were able to achieve this via a SurfingAttack, which allows hackers to send ultrasonic commands through glass or wood. In the Fredi baby monitor attack, hackers utilized the P2P cloud feature to gain easy access/interaction with the device's camera, exposing the victims to be spied on by the hacker [24]. The security issue with the P2P cloud feature is it opens multiple ports, making it difficult to track what moves through them. Last but not least, in 2017, hackers breached a casino's fish tank's thermometer to obtain access to their network [32]. Specifically, the fish tank utilized sensors that were connected to a PC and had access to the network and data.

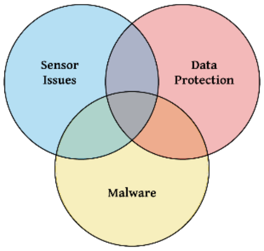

Figure 1: Taxonomy of attacks on smart home devices

Data protection issues: The data protection section encompasses IoT devices that have vulnerable encryption mechanisms, authentication mechanisms, and any other methods of protecting a device. Devices that fall under this category include doorbells, refrigerators, plugs, ovens, washers, and routers. Encryption and authentication mechanisms include multi-factor authentication (MFA), two-factor authentication (2FA), "pass the hash" encryption, SSL authentication, end-to-end encryption, key management, etc: the purpose of these methods is to protect data and verify ownership of an account, and if weak, these mechanisms may be bypassed. For example, a study identified encryption issues in the TP-Link Kasa Smart Plug [18]. Due to weak encryption, hackers could take control of the plug and the electricity going through the plug. In the same study, the Meross plug was found to expose wi-fi passwords due to weak encryption. In 2015, security researchers discovered a man-in-the-middle (MiTM) vulnerability in Samsung's refrigerator [23]. Even though secure sockets layer (SSL) was implemented, the MiTM vulnerability occurred due to the failure to authenticate SSL certificates, allowing hackers to monitor networks for Gmail credentials. Bitdefender IoT's research team identified a security vulnerability in the August Smart Pro Lock, allowing them to eavesdrop on network traffic and intercept passwords[29]. This vulnerability was caused due to the encryption key being hardcoded into the app. This not only exposed the encryption key, but the key itself utilized a simple ROT-13 cipher, allowing attackers to easily crack it.

Malware: Attacks in this category cover third-party vulnerabilities, malware, CVEs and exist in a range of smart devices such as air conditioners/HVAC systems, digital photo frames, wearable technology, smart buildings/homes, elevators, and vehicles. Flaws, vulnerabilities, and malware affect the integrity, confidentiality, availability of a device as well as expose sensitive data. For example, in 2008, a third-party vulnerability lead to the exploitation of Samsung's SPF-85H8 8-Inch digital photo frame [38]. An installer disc, used to access the digital photo frame, harbored a sality worm. The sality worm is a type of malware that targets Windows executable files along with security products and attempts to download additional files from a predefined remote web server. Another example of a third-party vulnerability was found in the breach of FitBit's wearable technology [21]. Breaches of Fitbit-like wearable devices can potentially cause negative consequences for the security of a home's network. In 2016, hackers utilized leaked email addresses and passwords from third-party websites to log in to Fitbit accounts, however, there was no evidence to prove that Fitbit's servers/networks were breached. By obtaining customer credentials, hackers were able to change account details and request replacements. In 2020, researchers exploited Phillips Hue's lightbulb due to a CVE-2020-6007 vulnerability in their ZigBee low-power wireless protocol [25]. This vulnerability allows hackers to conduct a remote code execution, which allows them to attack other smart devices in the network while utilizing the light bulb as a host.

4 Discussion: Enabling a territorial smart home

A home calls for the territorial affordances of identity, security and stimulation. Below, we discuss the implications of these three aspects of territoriality, and call for a distinction between being net-smart and smart.

Identity: The identity of a smart home is intertwined not only that of the smart devices within the home, but also with the identities of the people within the home. Separating the two creates scenarios that isolate the technology from the human. Designing smart homes with careful consideration of how the smart devices interact with the people in the home allows for a consideration of parameters that influence the identity of people in the home. Consequently, this leads to an evolving notion of the identity of the smart home that is predominantly influenced by the people, and is not affected when the smart devices get replaced, fail, or are hacked.

Security: The territorial notion of a smart home is tied to that of security of its occupants. Whereas smart devices such as home security cameras are more closely affiliated with the construct of providing security for a home, other devices such as smart light bulbs, smart ovens, and smart baby monitors need to also be tasked with providing (cyber) security for the home. The breach of any of these devices in a smart home network poses threats not only to the functionality of the device being breached, but also to that of other devices on the network. An attacker could infiltrate a smart home device, gain lateral access to other smart home devices on the network, and manipulate them for altered functionality or data exfiltration, while also connecting these compromised devices to botnets [22]. Thus, a smart home should reflect the need for protecting people's need for privacy, security, and defense from virtual intruders.

Stimulation: Porteous's definition of stimulation refers to the activities undertaken by an individual within the home that result in personalization, and consequent defense of the personalized space. Smart homes offer opportunities for personalization at several levels – device, network, and user - by incorporating cognitive mechanisms for adapting to the environment within the home.

Net-smart versus smartness: While the current tendency is for smartness to be defined in terms of computing capacity and the ability to connect to the Internet, it is unlikely that this definition of smartness will be sustainable. Technology has always been present in the human home, whether in terms of the tools of prehistoric societies, the clocks of medieval times, or the computers in our homes. The technology of older times was undoubtedly smart and complemented human existence for efficiency. However, none of these were subject to the scale and severity of attacks that our current technology is facing. It is, therefore, important to make a distinction about what smartness truly entails. If it is merely the gathering, collection, and processing of data on a global network such as the Internet, such technology is merely "net-smart". In contrast, a truly smart network would aspire to some of the abilities of cognitive smartness, which includes security as the primary underlying principle. A home with a wide cyber-attack surface might be net-smart, but in the absence of holistic security and privacy for its inhabitants, ceases to display smartness. Current research in cognitive security is an important step in that direction, and smart homes stand to benefit immensely from the developments in that area. said information for all three versions of

5 Conclusions

Conventional definitions of smart homes focus merely on the technologies that convert hitherto un-networked objects such as blenders, refrigerators, air conditioning systems, and other objects around the home into IoT devices that are capable of providing online access to the functionality and data collected by these objects. However, a home that does not meet the primal expectations of people from their homes ceases to be smart, in spite of the technologies that connect the myriad objects in the home to the Internet. In this paper, we studied the notion of a smart home from the Porteousian definition of a home as providing three levels of territoriality – identity, security, and stimulation. Although the ubiquity of networks continues to expand, we still expect our home to offer privacy, security, and the ability to personalize it. Smart homes require ongoing rigorous examination to evaluate how well they conform to our expectations of privacy, security, and stimulation offered by technologies present in our homes.

REFERENCES

[1] Ioannis Agrafiotis, Jason Nurse, Michael Goldsmith, Sadie Creese and David Upton. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." Journal of Cybersecurity 4 (1).

[2] Avast Smart Home Security Tech Report. (2019). Retrieved January 20, 2022 fromhttps://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

[3] George Ashenmacher. (2016). Indignity: Redefining the harm caused by data breaches. Wake Forest L. Rev. 51 (2016): 1.

[4] Sanja Budimir, Johnny Fontaine, and Etienne Roesch. (2021). Emotional experiences of cybersecurity breach victims. Cyberpsychology, Behavior, and Social Networking, 24(9), 612-616.

[5] Daphna Canetti, Michael Gross, Israel Waismel-Manor, Asaf Levanon, and Hagit Cohen. (2017). How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. Cyberpsychology, Behavior, and Social Networking 20(2), 72-77.

[6] James Coker. (2021). Smart Home Experiences Over 12,000 Cyber-Attacks in a Week. Retrieved January 20, 2022 from https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/

[7] Federico Cugurullo. (2020). Urban artificial intelligence: From automation to autonomy in the smart city. Frontiers in Sustainable Cities, 2, 38.

[8] Justin Dion and Nicholas M. Smith. (2019). Exploring Private Causes of Action for Victims of Data Breaches. W. New Eng. L. Rev. 41 (2019): 253.

[9] Ericsson. Innovation with impact. Retrieved January 20, 2022 from https://www.ericsson.com/en/about-us/company-facts/innovation-history.

[10] Iliya Fayans, Yair Motro, Lior Rokach, Yossi Oren, and Jacob Moran-Gilad. (2020). Cyber security threats in the microbial genomics era: implications for public health. Eurosurveillance 25(6), 1900574.

[11] Paula Fraga-Lamas, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo, and Miguel González-López. (2016). A review on internet of things for defense and public safety. Sensors 16(10), 1644.

[12] Mahita Gajanan. (2017). This smart salt shaker wants to change the way you season food. Retrieved January 20, 2022 from https://time.com/4773835/smalt-salt-shaker-bluetooth/

[13] Howard Gardner and Thomas Hatch. (1989). Educational implications of the theory of multiple intelligences. Educational Researcher, 18(8), 4-10.

[14] Globe News Wire (2021). Retrieved January 20, 2022 from https://www.globenewswire.com/news-release/2021/04/08/2206579/0/en/Global-IoT-Market-to-be-Worth-USD-1-463-19-Billion-by-2027-at-24-9-CAGR-Demand-for-Real-time-Insights-to-Spur-Growth-says-Fortune-Business-Insights.html

[15] Kirsten Jacobson. (2009). A developed nature: A phenomenological account of the experience of home. Continental Philosophy Review, 42(3), 355-373.

[16] Ido Kilovaty. (2021). Psychological data breach harms. N.C. J.L. & Technology.

[17] Shane Legg and Marcus Hutter. (2007). Universal intelligence: A definition of machine intelligence. Minds and Machines, 17(4), 391-444.

[18] Angelica Leicht. (2020). Warning! These smart plugs can be hacked and start fires. Retrieved January 20, 2022 from https://www.komando.com/security-privacy/smart-plugs-hacked/757290/.

[19] Gaoqi Liang, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems. 32(4), 3317-3318.

[20] Litter Robot. https://www.litter-robot.com/

[21] Marianne McGee. (2016). Fitbit Hack: What Are the Lessons? Retrieved January 20, 2022 from https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793

[22] Renita Murimi. (2019). Use of Botnets for Mining Cryptocurrencies. In Botnets (pp. 359-386). CRC Press.

[23] Colin Neagle. (2015). Smart refrigerator hack exposes Gmail login credentials. Retrieved January 20, 2022 from https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html

[24] Pierluigi Paganini. (2018). Vulnerabilities in Fredi Wi-Fi baby monitor can be exploited to use it a spy cam. Retrieved January 20, 2022 from https://securityaffairs.co/wordpress/73848/hacking/fredi-wi-fi-baby-monitor.html

[25] Pierluigi Paganini. (2020). Hacking Wi-Fi networks by exploiting a flaw in Philips Smart Light Bulbs. Retrieved January 20, 2022 from https://securityaffairs.co/wordpress/97392/hacking/philips-smart-light-bulbs-hack.html.

[26] Srinivas Panguluri, William Phillips, and John Cusimano. (2011). Protecting water and wastewater infrastructure from cyber attacks. Frontiers of Earth Science 5(4), 406-413.

[27] Katie Pilkington. (2013). Quirky Egg Minder review. Retrieved January 20, 2022 from https://www.cnet.com/reviews/quirky-egg-minder-review/

[28] J. Douglas Porteous. (1976). Home: The territorial core. Geographical Review, 383-390.

[29] Molly Price. (2020). August smart locks could be giving hackers your Wi-Fi credentials. Retrieved January 20, 2022 from https://www.cnet.com/home/security/august-smart-locks-could-be-giving-hackers-your-wi-fi-credentials/

[30] Purplesec (2021). Retrieved January 20, 2022 from https://purplesec.us/resources/cyber-security-statistics/

[31] Morello Rosello, Claudio De Capua, Gaetano Fulco, and Subhas Chandra Mukhopadhyay. (2017). A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and IoT in the electric grid of the future. IEEE Sensors Journal 17(23), 7828-7837.

[32] Alex Schiffer. (2017). How a fish tank helped hack a casino. Retrieved January 20, 2022 from https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

[33] Carmelo Scuro, Paolo Sciammarella, Francesco Lamonaca, Renato Sante Olivito, and Domenico Luca Carni. (2018). IoT for structural health monitoring. IEEE Instrumentation & Measurement Magazine. 21(6), 4-14.

[34] Dwight Silverman (2021). Apple back on top: iPhone is the bestselling smartphone globally in Q4 2020. Retrieved January 20, 2022 from https://www.forbes.com/sites/dwightsilverman/2021/02/22/apple-back-on-top-iphone-is-the-bestselling-smartphone-globally-in-q4-2020/?sh=390d13a54ca7

[35] Daniel Solove and Danielle Citron. (2017). Risk and anxiety: A theory of data-breach harms. Tex. L. Rev., 96, p.737.

[36] Sophos (2020). Siri and Google Assistant hacked in new ultrasonic attack. Retrieved January 20, 2022 from https://nakedsecurity.sophos.com/2020/03/02/siri-and-google-assistant-hacked-in-new-ultrasonic-attack/

[37] Edward Thorndike. (1998). Animal intelligence: An experimental study of the associate processes in animals. American Psychologist, 53(10), 1125.

[38] Trend Micro. (2008). Yet Another Digital Picture Frame Malware Incident. Retrieved January 20, 2022 from https://www.trendmicro.com/en_us/research/08/l/yet-another-digital-picture-frame-malware-incident.html