Sam Barton
GEOG 78.01: Geospatial Technologies and Society
Professor Alvarez Leon
March 7, 2022

Not So Smart: Cybersecurity of Smart Home Systems

In a world dominated by the Internet of Things (IoT), the continued human reliance on computational power and sensory devices all connected within a (wireless) network has been astounding. Sensors and networks pervade every space of society, whether it be in public restrooms detecting the need for toilet paper refills, surveillance cameras located outside the local convenience store, or conductivity-temperature-depth-satellite relay data loggers tagged on elephant seals near the continental shelf off East Antarctica (Kokubun et al., 2021). In 2008, machinic connectivity to the internet outnumbered human connectivity, a defining moment for the IoT, and this gap has only grown since then (Gabrys, p. 7). Cisco predicts there will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018 (2020). These ubiquitous sensors provide major benefits within modern life in realms such as public health, personal safety, and general efficiency. Throughout *Project Earth*, Gabrys (2016) focuses on environmental sensing, and demonstrates how sensors not only record data, but also generate new environments and environmental relations within the spaces they oversee. This brief paper will explore homes as the environment and explore the consequences of smart home systems with regards to cybersecurity.

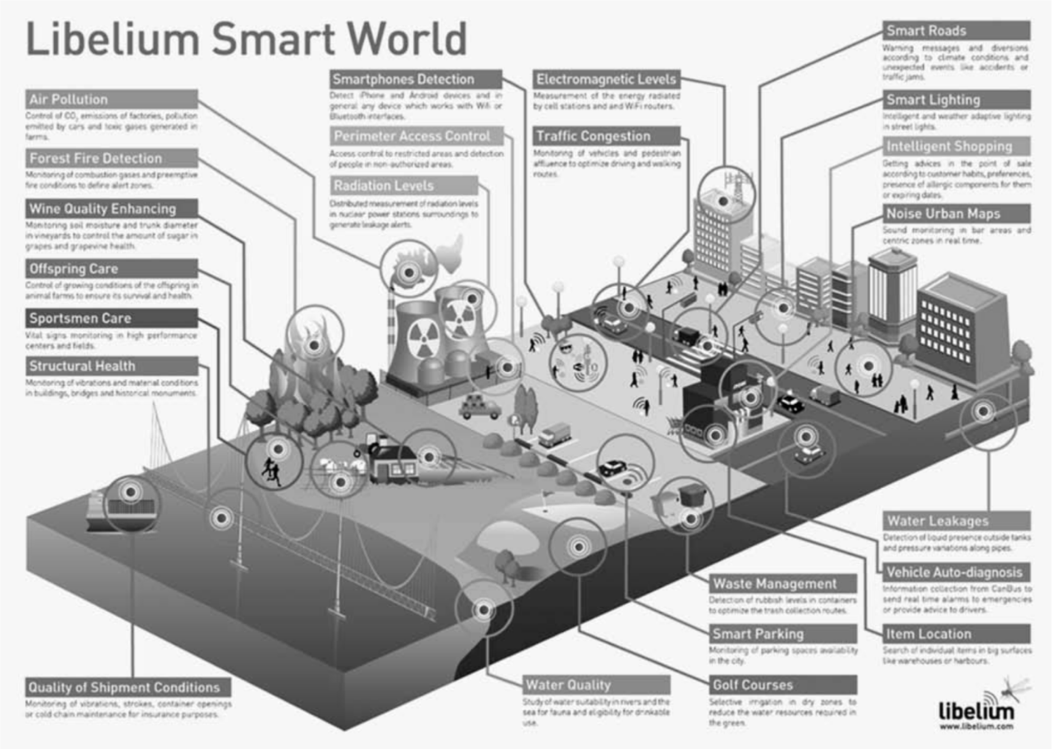
Throughout her study, Gabrys explores how wireless and embedded sensor systems have drastically developed through ecological study, and how these initial projects can serve as a basis for a widespread deployment of these systems in other, more citizen-focused contexts. She asserts that these sensor systems composed of small-scale in situ sensors and actuators which collect and transmit data throughout networked connections have produced a revolution comparable to the rise of the internet (Gabrys, 2016). However, the collection of data through sensors is not an entirely new phenomenon, and the synthesis of this data using algorithms, and computer networking principles has been the major step in creating information systems from these otherwise distinct sensors. These syntheses turn data into “high-level information” (p. 41) where the records and raw data transform into observations or experience, or in other words, this process of filtering, aggregating, and selecting transforms this sensory data into information that is relevant to humans (Gabrys, 2016). A sensory network can consist of many different tools for collecting data: these sensors can be anything from an accelerometer, pendulum resistive tilt sensor, or pressure switch to an IR reflection sensor, UV detector, or magnetic sensor. However, in connecting these various devices into a singular system, which Gabrys (2016) claims to act as a proxy for the very environments that they sense. The relationships between these different sensors and actuators are the most important attribute of the system and render it capable of advanced data visualization. With algorithmic tools such as machine learning, these systems can only get ‘smarter’ and provide more relevant information for scientists and corporations/governments.

In the third section of *Project Earth*, Gabrys (2016) transitions into the realm of urban sensing, analyzing the sensory systems which can build the framework of a smart and sustainable city (see Figure 1). Proposals for networked/computable cities have become staples of urban-development plans since the 1980s (Batty, 1997). Gabrys (2016) states that the hope for these ‘smart cities’ is how networked urbanisms and participatory media can achieve greener and more efficient cities which also promote rapid economic growth. These computational technologies, which are based off of digital sensors, are meant to synchronize urban processes and infrastructures to improve resource efficiency, distribution of services, and urban participation. In this system architecture, computing becomes another utility for citizens. These proposals which often monitor citizen activities convert these citizens into “unwitting gatherers and providers of data” (p. 189) which may be used for a number of purposes which are not obvious to those who are sensed (Gabrys, 2016). Furthermore, in the case of a lack of participation of from citizens, Gabrys (2016) reveals how these smart cities would totalitarian overshoot where these “dumb citizens” (p. 200) become entities subject to monitoring without actually participating in the flow if information. These systems may also operate on their own. Citizens become “data-gathering nodes” (p. 203) in a smart city (Gabrys, 2016). With these systems now being implemented in cities, dashboards, which amalgamate all of the various sensory inputs onto a single board, have become a prevalent fixture of a modern city, and they demonstrate how the city has become a platform, similar to internet. This platform is not simply an internet space, but is also an embedded, situational, cand context-focused applications that maps new digital functionalities onto urban infrastructures, processes, and exchanges (Gabrys, 2016, p. 257). Gabrys asserts that with this synchronization of information, cities can become a living organism itself.

Throughout *Program Earth*, Gabrys (2016) maintains an optimistic outlook on the types of users interacting with these computer systems, and through the case study of smart homes, this essay will conversely consider the malignant hacker interaction and the lens of cybersecurity. The smart home is one of today’s most well-known applications of the IoT ideology, and it consists of heterogenous devices ranging from electronic door locks to smart kitchen appliances which all communicate remotely with each other over the internet. Similar to fundamentals explored in *Project Earth*, devices within the smart home system collect and exchange data with each other and users with embedded sensors and internet connectivity, a network which propagates a digital space within the physical space of a home (See Figure 2). Digital Market Outlook forecasts smart home revenue to increase a staggering 478% from 2017 to 2025 (see Figure 3). However, since smart home systems collect vast amounts of personal and sensitive data, privacy protection is critically important, and the question of cybersecurity is a major one. Sensors embedded in smart appliances are highly exposed to identity theft and intruders on the network can recognize residents’ locations or other sensitive information through the exchanged data, identifying life patterns of the inhabitants, leaving them open to open harm or theft.

Therefore, hiding the sensors' identity within the network is a high priority in the domain of smart home infrastructure. Typical home area networks are connected by a protocol called ZigBee, a bidirectional radio protocol, because it provides low data transmission communication, and thus a large battery life. However, its designated architecture has left it vulnerable to attack as all appliances are connected via a single controller. Other communication methods are Bluetooth and WiFi which also have their own benefits and drawbacks. There is a positive relationship between employing numerous network technologies and the difficulty of hacking such a system, but there is a tradeoff: maintaining such a system requires a broad range of expertise (Moderesi and Symons, 2020). There are numerous studies exploring the other ways to increase the resilience of smart home systems, and the technical intricacies regarding these techniques are out of the scope of this essay (see Yazan et al., 2021; Sarhan, 2020; Bugeja et al., 2021; Modaressi & Symons, 2020).

While *Project Earth* has provided the technological utopia of a sensor-equipped world without any maligning factors, this essay, through the study of smart home systems, has begun to reveal the one of the vulnerabilities that this changing world will host: the issue of cybersecurity. Cybersecurity should be at the forefront of design-thinking regarding sensor-based networks and will become only more prevalent with the increasing international reliance on a 'smarter' world.



Libelium Smart World

Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

libelium
www.libelium.com

Figure 1–Program Earth p. 240

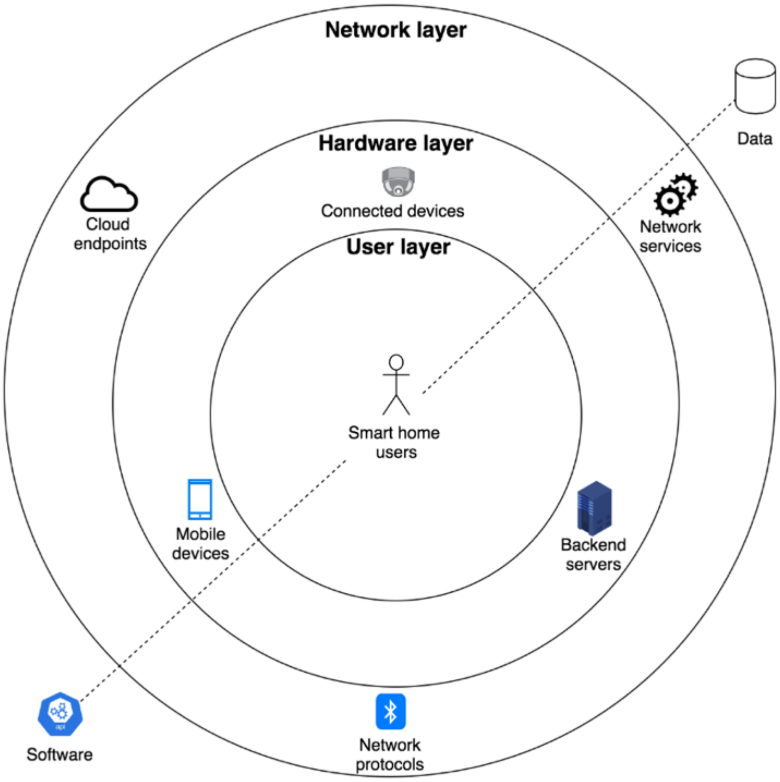


Figure 2: Smart Home Abstraction from Bugeja, Jacobsson, and Davidsson (2021)

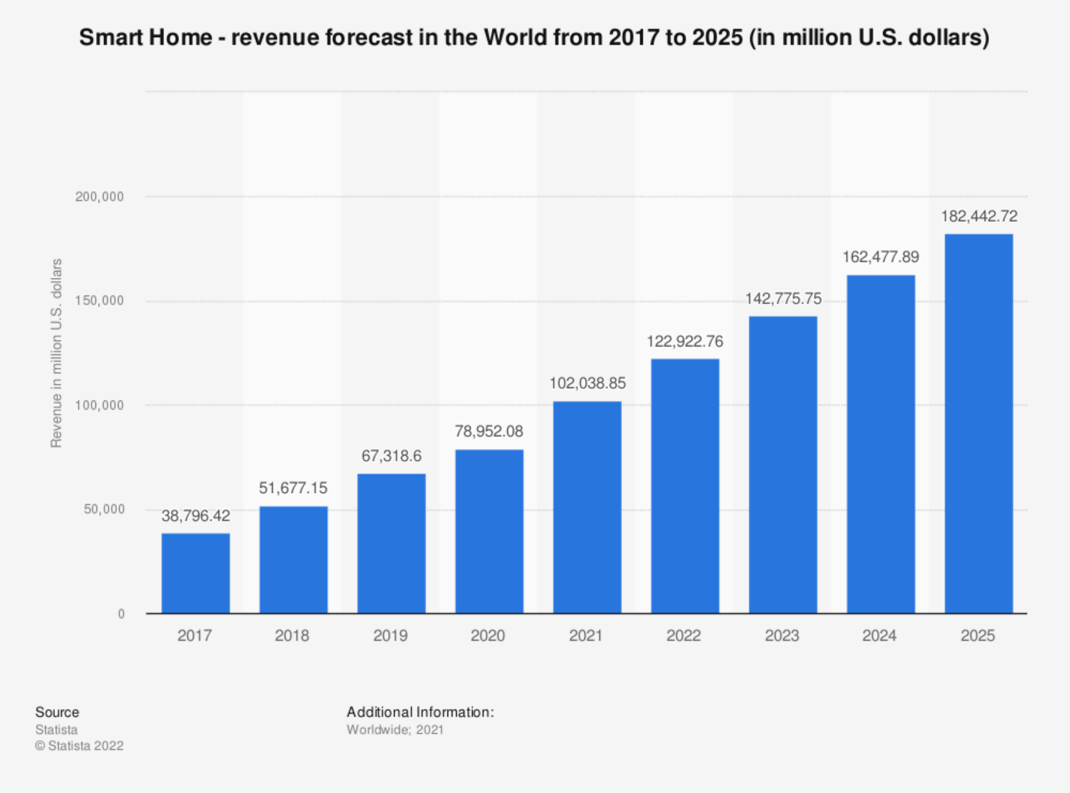


Figure 3: World Smart Home Revenue Forecase from Statista (2021)

Bibliography:

Batty. (1997). The computable city. International Planning Studies, 2(2), 155–. https://doi.org/10.1080/13563479708721676

Bugeja, J., Jacobsson, A., & Davidsson, P. (2021). PRASH: A Framework for Privacy Risk Analysis of Smart Homes. *Sensors*, *21*, 6399. doi:10.3390/s21196399

Cisco. (March 9, 2020). *Cisco Annual Internet Report (2018–2023)*. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

Gabrys, Jennifer. (2016). Program Earth: Environmental Sensing Technology and the Making of a Computational Planet. University of Minnesota Press.

Kokubun, N., Tanabe, Y., Hirano, D., Mensah, V., Tamura, T., Aoki, S. and Takahashi, A. (2021), Shoreward intrusion of oceanic surface waters alters physical and biological ocean structures on the Antarctic continental shelf during winter: Observations from instrumented seals. Limnol Oceanogr, 66: 3740-3753. https://doi.org/10.1002/lno.11914

N. Dou, Y. Mei, Z. Yanjuan, & Z. Yan. (2009). The Networking Technology within Smart Home System - ZigBee Technology (Vol. 2). doi:10.1109/IFCSTA.2009.129

Modarresi, A., & Symons, J. (2020). Technological Heterogeneity and Path Diversity in Smart Home Resilience: A Simulation Approach. *Procedia Computer Science*, *170*, 177–186. doi:10.1016/j.procs.2020.03.023

Q. I. Sarhan. (2020). Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform. *IEEE Access*, *8*, 128362–128384. doi:10.1109/ACCESS.2020.3008610

Statista. (June 14, 2021). Smart Home - revenue forecast in the World from 2017 to 2025 (in million U.S. dollars) [Graph]. In Statista. Retrieved March 07, 2023, from https://www.statista.com/forecasts/887554/revenue-in-the-smart-home-market-in-the-world

Yazan, A., Bsoul Abdel, A. R., Mohammed, A. Z., & Samer, S. (2021). Cybersecurity of Smart Home Systems: Sensor Identity Protection. *Journal of Network and Systems Management, 29*(3). https://doi.org/10.1007/s10922-021-09586-9