The World in 2050: Safety by Design

Tiana Ashley Khong

San Jose State University

Spring 2017

Abstract

This paper relates technological advances in intelligent buildings, autonomous vehicles, and smart roads to the critical need for safety service standards for consumers and users. Companies continuously compete with one another to come up with innovative technology, but in doing so, can put consumers and users at risk. The Internet of Things (IoT) and cloud service platforms make it possible to build intelligent buildings that reduce company costs and environmental impacts, produce autonomous vehicles that reduce consumer costs and risks while making lives efficient, and construct smart roads that reduce risks and increase efficiency. All of these amazing technologies can provide enormous benefits for communities, but they can also fall victim to lack of security. Hackers pose a serious threat to IoT, cloud service platforms, and devices that rely on both services to work, and all it takes is one small alteration in the programs to cause severe damage to societies all over the world. To provide a better understanding of the severity of lack of safety, I created a scenario in the not-so-distant future where hackers caused a global catastrophe. To prevent such a catastrophe to occur again, governments and technology companies from all over the world realized that innovation means nothing without safety, and worked together to establish safety-by-design service standards with the motto: "safety before innovation," leading to the blissful and progressive era of 2050. This essay will look at the inner workings and benefits of intelligent buildings, autonomous vehicles, and smart roads to allow better understanding of how IoT and cloud service platforms play a vital role in making each one possible. Explanations of their inner workings and benefits are followed by recent examples of how hackers are able to turn what seemed like fool-proof secure technology into a business and consumer nightmare, giving light to the desperate need for safety-by-design service standards.

The World in 2050: Safety by Design

In 2028, the world experienced the collapse of cloud service platforms unlike anything it had ever seen before. A few days before the Christmas holiday, two major cloud service platforms were hacked into and collapsed, resulting in hundreds of thousands of deaths all over the world, emergency responders unable to respond, hospitals shutting down, and businesses being completely out of commission for a week. The world we knew came to a screeching halt, and all it took were minor alterations to major cloud service platform programs by vindictive members of society wanting to make a political statement. Even with supposedly foolproof security in place to prevent such a cyber attack, it didn't prove to be too difficult a task for the hackers to carry out the largest cyber terrorist attack the world had ever known.

After the Internet of Things (IoT) programs were altered, the interconnected sensors and devices connected to the cloud service platforms failed, resulting in the malfunctions of autonomous vehicles worldwide and causing over two million road crashes and hundreds of thousands of deaths. Due to the prevalence of autonomous emergency service vehicles since the early 2020s, there weren't enough driver-operated emergency vehicles available for responders to help citizens. Hospitals worldwide had been completely shut down due to their building automatic systems relying on IoT and the cloud service platforms, resulting in the deaths of thousands of patients in the hospitals, and preventing hospitals from taking in new patients who desperately needed care. It took collaborating governments and technology companies a few days to gain access to the cloud service programs, and by then the damage had been done worldwide. It became clear that if we were to continue living in a world that heavily relied on IoT, we needed to adopt new service standards incorporating safety by design to prevent future failures.

Fast forward to the year 2050: it’s been 22 years since the largest cyber terrorist attack occurred, and societies are thriving all over the world. For nearly two years after the attack, governments and technology companies from all over the world worked together to develop safety-by-design service standards with the motto: “safety before innovation.” These standards require that companies incorporate security measures at the very primal stages of innovative technology to ensure the safety of consumers and societies. When a company creates innovative technology, extensive security tests must be conducted and the technology must pass with a 100% safety approval rating before it may proceed with development, accompanied by security tests at every step of the way. This has completely shifted the way companies do business, slowing down processes and innovation; but it ensures safety for customers and users. Since the new service standards were implemented, the sales and development of intelligent buildings, autonomous vehicles, and smart roads increased dramatically. People felt safe once more, allowing our cities to become more dependent on IoT, thus providing efficient and blissful lifestyles. Even though it took the catastrophe of 2028 to open our eyes to the dire need for stronger safety guidelines, we are now living in a progressive era where government and industry collaboration resulted in improved service standards.

As defined by the Institute of Customer Service, “service standards are important to customers, potential customers, employees, and management for they help define what customers can expect and to remind businesses of the challenges and obligations they face” (“Setting Customer Service Standards,” 2015). With the development of IoT, innovative technologies provide new, beneficial services to the community. But if innovation continues to outweigh safety, a global disaster similar to the above scenario is inevitable, which is why it’s crucial for innovators to adopt safety-by-design service standards. By putting safety before innovation, we are getting the maximum benefits of a world run by IoT: technological advances continue to improve our lives, and we feel secure knowing safety is priority. If safety-by-design service standards are not adopted, then with every step forward we take with a technological advance we take two steps back when the lack of safety is exposed. Let’s look at intelligent buildings, autonomous vehicles, and smart roads to understand the importance of adopting safety-by-design service standards.

The world is becoming more reliant on IoT and cloud computing, with many intelligent buildings being built to service the community by reducing costs, risks, and environmental impact, and improving the internal environment of the buildings. It’s also possible to convert already-existing buildings into intelligent buildings. Either way, the process requires constant cooperation and collaboration from all the stakeholders involved, including building management, operations, suppliers, customers, and especially the information technology (IT) department. When setting up an intelligent building, it’s important for the stakeholders to consider and prepare for technological and security changes early in the development to allow for such changes to occur smoothly without much interruption.

By combining a building automation system (BAS) with IoT, companies can use the building’s sensors to store data on the cloud using a cloud-based building-analytic system. Once a building's BAS is combined with IoT, data from the sensors is sent to the cloud, where it is stored and analyzed, and then sent back to a dashboard which is accessed by the stakeholders, helping them make effective and efficient decisions to reduce costs. Since the BAS connects with IoT, the data that is stored and analyzed allows the BAS to take predictive measures by sensing minor issues that could result in a failure, reducing risks. The occupants of the building are still able to control functions of the intelligent building such as lighting, equipment, heating, and air while they are there, which allows an ideal and comfortable environment. But once they leave, the BAS sensors will detect the empty space and turn everything down, reducing costs and the negative impact on the environment (Walden, 2016).

It’s easy to brush off the idea of a hacker wanting to gain access into a building's BAS just to control heating and lights. But what people might not think about is that by gaining access into the building’s BAS, a hacker can gain access to confidential information. IBM’s security research group conducted an ethical hacking exercise just to see how vulnerable intelligent buildings really are. During this exercise, the group discovered issues in the BAS architecture that allowed them to gain access not only to the BAS, but to a central server as well. The security issues that lead to this realization included exposed administration ports on routers and identical passwords for multiple systems. Not only did the group gain access to one BAS, they also gained access to multiple buildings across the company. After the exercise, the team’s lead, Paul Ionescu, discussed how companies could take action to increase their BAS security and stated that roughly 29% were in the process of improving their cybersecurity (Millman, 2016).

Twenty-nine percent is a very small amount, considering how many companies heavily rely on IoT services and devices to store their data. Companies investing in intelligent buildings reap benefits such as reduced costs, risks, and environmental impacts, but in doing so it’s important to incorporate safety-by-design service standard. What good are the benefits if a hacker is able to gain access to the BAS, resulting in access to confidential information that can harm the company and its consumers? When constructing the BAS, it’s important for the IT department to integrate safety by testing the security each step of the way until accomplishing a 100% safety rating. In doing so they are ensuring the company’s and consumers’ data is safe, while creating an innovative building to better service the internal and external communities.

Autonomous vehicles – also known as driverless cars – and smart roads are systems that are already being integrated into our lives, and much of the technology found in autonomous vehicles can be found in recently manufactured vehicles driven by people. A person-operated vehicle that has collision avoidance, drifting warning, and self-parking features is just a few steps away from being an autonomous vehicle. Autonomous vehicles use sensors and cameras to communicate with each other in real time to detect objects such as other vehicles, cyclists, pedestrians, stop lights/signs, and other stand-still objects to prevent collisions ("When Cars Drive Themselves," 2017). They can also communicate with each other through collected data that is sent and stored in the cloud using a cloud-based analytic system. This data could include weather conditions, speed limits, and road collisions detected by other vehicles ("Smart Roads," 2016).

To better assist autonomous vehicles, smart roads are being built, and just like autonomous vehicles, the roads are embedded with sensors. This interactive road technology sends data to a cloud-based analytic system to be stored, analyzed, and transmitted to autonomous vehicles ("Smart Roads," 2016). The sensors will be able to detect weather conditions and surrounding objects, and work in conjunction with smart traffic signals to enable autonomous vehicles and smart roads to communicate with each other and provide a safe environment for travelers and pedestrians (Igbenoba, 2016).

Integrating autonomous vehicles and smart roads provides enormous benefits. Every year over one million people die in road crashes globally ("Annual Global Road Crash Statistics," 2016), nearly all of which are a result of human error. All it takes is a few seconds of distraction, a vehicle defect or malfunction, or a consumer neglecting to take their vehicle in for a routine checkup to result in a road crash. Autonomous vehicles will be able to detect if there is a problem with the vehicle, alert the owners and manufacturers, and prohibit the use of that vehicle until the problem is dealt with. Along with the safety benefits, autonomous vehicles would create a stress-free environment for consumers. One would be able to talk, text, play games, or do work on their laptops while on their way to their destination (Igbenoba, 2016). Parents could program the vehicle to drop off the kids at school and then come back to take them to work or run errands. It would mean that only one vehicle would be needed for a whole family, reducing traffic and costs in fuel and insurance (Kroenke & Boyle 123-125, 2016). But with all these benefits, there is still a major concern with safety.

In a recent experiment, reporter Andy Greenberg offered to test drive an autonomous vehicle while two researchers hacked into the car's systems to see how much of the vehicle they could control. Within no time the researchers had hacked into the computer's air conditioning, stereo, and even the accelerator. This experiment showed just how powerless a driver could be if their autonomous vehicle was hacked into (Hempfield, 2017). This is where the safety-by-design service standards would come into effect. Safety would have to be at the heart of developing autonomous vehicles and smart roads. If companies such as Tesla and Ford are planning for a world where every consumer or family has an autonomous vehicle, there is a critical need for enforced safety service standards. No consumer in their right mind will buy an autonomous vehicle if hackers can easily gain access to the vehicle's computer systems, or gain access into the smart roads computer systems, potentially wreaking havoc on the city. In order for consumers to feel comfortable purchasing autonomous vehicles and for cities to develop smart roads, there must be a large-scale recognition of safety-by-design service standards requiring 100% safety ratings at every stage of development.

As innovation continues to drive technology at impressive rates, there is a risk of safety being ignored as companies compete to get the newest technology in the hands of consumers to stay ahead of competitors. Safety-by-design service standards are essential to consumers, but are often overlooked until a disaster occurs, prompting actions to be taken to prevent it from happening again. This cannot be the case if we wish to have a world where people and businesses heavily rely on IoT. Intelligent buildings, autonomous vehicles, and smart roads are just a few of the emerging technologies that can only succeed if technology companies adopt safety-by-design service standards – safety before innovation.

References

"Annual Global Road Crash Statistics." *Association for Safe International Road Travel*. 2016. http://asirt.org/initiatives/informing-road-users/road-safety-facts/Road-crash-statistics. Accessed 10 Mar. 2017.

Hempfield, Clarence. *Why a Cybersecurity Solution for Driverless Cars May Be Found Under the Hood*. 18 Feb. 2017. https://techcrunch.com/2017/02/18/why-a-cybersecurity-solution-for-driverless-cars-may-be-found-under-the-hood/. Accessed 1 Mar. 2017.

Igbenoba, Antonette. *Autonomous Vehicles and the Internet of Things*. 10 Nov. 2016. https://informationcounts.com/autonomous-vehicles-and-the-internet-of-things/. Accessed 15 Mar. 2017.

Kroenke, David M., and Randall J. Boyle. *Using MIS*. 3rd ed., Pearson Education, 2016.

Millman, Rene. *How Vulnerable Are Smart Buildings to Cyber Attacks?***.** IFSEC Global. 29 Mar. 2016. https://www.ifsecglobal.com/how-vulnerable-are-smart-buildings-to-cyber-hacks/. Accessed 11 Mar. 2017.

"Setting Customer Service Standards." *The Institute of Customer Service*. 8 Jun. 2015. https://www.instituteofcustomerservice.com/research-insight/guidance-notes/article/settinG-customer-service-standards. Accessed 25 Feb. 2017.

"Smart Roads." *IoT Mashups*. 2016. http://www.iotmashups.com/iot-examples/smart-roads/. Accessed 16 Mar. 2017.

Walden, Leroy. *The Internet of Things and Intelligent Facilities Management.* HPAC Engineering. 7 Nov. 2016 http://hpac.com/internet-things/internet-things-and-Intelligent-facilities-management. Accessed 9 Mar. 2017.

"When Cars Drive Themselves". *The New York Times*. Updated 14 Apr. 2017. https://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html?_r=0. Accessed 7 Apr. 2017.