Cybersecurity and Our Food Systems

Nicholas Russell
Computer System Security
Professor Ming Chow
December 13, 2017

Table of Contents

Abstract

Food systems include all of the processes and infrastructure involved in feeding our populations: from growth, through consumption, to disposal. In February of 2013, the Department of Homeland Security labeled the Food and Agriculture industry as one of the sixteen national critical infrastructures. As the technologies that improve the effectiveness of these systems and their components rapidly evolve, the need to ensure their security from cyber-terrorism and exploitation becomes ever more critical. This paper will highlight some areas of concern at both the consumer and production levels. In addition, the paper will discuss recommendations for both producers and consumers to consider as our food systems become increasingly exposed to exploitable networks and technologies.

Introduction

Cybersecurity is a topic that is difficult to ignore. In recent years, we have seen a spike in highly publicized and wide-reaching attacks, like the one that took down several major websites in 2016 when our DVRs, televisions, and other IoT devices targeted the DNS provider Dyn with a DDoS attack. Twitter, amongst other high traffic websites, was affected by the attack on Dyn. However, we have yet to hear of a major cyber-attack on our food systems. Are they simply not being targeted? Perhaps their internet exposure and attack surfaces do not make them ripe for attack? Highly unlikely is the answer to both of these questions.

Each and every one of us is a participant in food systems. A food system is all of the processes and infrastructure involved in feeding our populations. This includes everything from growing and harvesting, to processing and packaging, to distribution and consumption. Such high exposure theoretically renders food systems an ideal target for any malicious actor looking to target the masses.

The internet has facilitated innovations in technologies that make the varying parts of the food system more effective than ever. Automation via networked PLC (programmable logic controllers) facilitates rapid production of foods. Connected sensors in distribution channels help ensure that food arrives safe and unadulterated for consumption, and in the most effective of

logistical manners. These systems save time and money – this is great for both manufacturers and consumers. Our homes contain smart devices involved in the food system like modern refrigerators. These devices provide a pleasant experience for those of us looking to know the conditions inside of the refrigerator without having to open the door.

Like most good things, there is a price to be paid and a degree of risk associated with this level of connectivity. However, when it comes to food, the risks associated with an attack are greater than per say the risk of your gaming system or smartphone being exploited. The results of a cyber-attack on our food systems could be at minimum economic hardship and at most life-or-death scenarios for millions. The stakes are simply too high to ignore.

To the Community

This is an important topic because we are all participants in food systems. Our public water supplies, the vegetables we purchase at local markets, and the meat we consume in meals from chain restaurants have likely all been exposed to networked technology at one point in time. As we are seeing now more than ever, connected devices are the subjects of malicious attacks each and every day. Each of us has the potential to be an unknowing victim of an attack on food systems as a result of these connected technologies. Due to the potential life-and-death nature of attacks, it is critical that we become more aware of the threats we face and assume responsibility for protecting others and ourselves from harm.

The "C.I.A. triad" is a widely applicable cybersecurity model, and represents three key principles of any secure system: confidentiality, integrity, and availability. While each of these principles can be applied at both the consumer and facilitator levels of food systems, integrity and availability are the two with obvious potential for a large impact on the wellness of our society. By ensuring technologies that play a role in our food systems practice the protection of integrity and availability, we are one step closer to protecting our families and society from the potential harm caused by a cyber-attack.

We need to ask ourselves if we are adding complexity without understanding the potential consequences of our desire for the continuous rapid technological improvements. Do I need a

networked refrigerator? Is it crucial that we automate and facilitate the remote control/monitoring of devices essential to food safety at the production level? These are questions that we need to ask ourselves. Unfortunately, it is difficult to guarantee that software connected to our food systems is completely secure when not all developers are trained in secure coding.[1] Software developers are human, and humans make mistakes – these mistakes may be either bugs or design flaws that go unnoticed until it's too late. However, each and every effort that is taken to develop strong security principles and raise awareness at both the consumer and commercial levels will offer us greater hope and peace-of-mind as it relates to the security of what is essential to our existence: food.

Cyber-terrorism meets agro-terrorism and produces potential outcomes deserving of careful attention and consideration

The Congressional Research Service defines agro-terrorism as a subset of bioterrorism and is the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining social stability.[2] In February of 2013, the Department of Homeland Security identified the Food and Agriculture industry as one of the sixteen national critical infrastructures.[3]

There are at least two large areas of concern regarding food systems: disruption of distribution and the malicious tampering/adulteration of the food supply. These two areas of concern represent the integrity and availability principles of cybersecurity's C.I.A. triad. Disruption of the integrity component could result in economic hardship in the form of lost product for consumers and households. Imagine the economic burden that arises from having to throw away spoiled goods. Disruption in the availability component could result in decreased food security, access to food, which could be detrimental to public health at a regional or socio-economic level, depending on the nature and targets/victims of an attack.

The Merriam-Webster dictionary defines cyber-terrorism as terrorist activities intended to damage or disrupt vital computer systems. This a generalist definition in comparison to others that stipulate that the acts be motivated by ideologies or politics.[4] On December 17, 2014, the U.S. Government asserted their belief that North Korea was behind the cyber-attack on Sony Studios that caused economic hardship for both Sony and theaters across the country when the movie was

forced to an early digital release and limited theater release. It is commonly believed that this act was politically motivated due to the film's depiction of North Korea's leader Kim Jong Un. However, as we have come to learn from other attacks and acts of violence in our modern world, things are not always as clear and understandable as we would like to believe. What we are able to count on is the unexpected in our world.

Other acts of violence have manifested themselves using devices that have been available to us for centuries. Guns, bombs, and more recently weaponized-vehicles have all been widely available around the world for generations. The Internet is still relatively new and even more so is the concept of the Internet of Things. Are we potentially building modern tools of terror to be used against our society? It is possible considering that the motor vehicle was never intended by its creators to be used as a weapon and means of inflicting mass harm in the hands of a malicious operator. Those looking to inflict economic hardship through exploitation have the ability to turn computer code, something so commonly used for good, into a weapon at the expense of innocent individuals and businesses in our society.

What is to stop these malicious actors from turning your innocent intentioned refrigerator against you? You may end up with spoiled milk or salmonella from spoiled chicken. Max Kilger, a cybersecurity researcher at University of Texas-San Antonio is quoted saying, "If I was being malicious, I might turn your refrigerator off," … "If I were being more terror-minded, I might tap into your refrigerator, turn it up to the temperature where certain key foods would spoil and turn. Then I would be sure to mask the temperature on the display, so it looks like 34 degrees when it is in fact 49, and then turn it back down—preferably all in the middle of the night. Now you have a nice case of food poisoning."[5] This is an example of a potential vulnerability at the consumer level. It is safe to assume matters could become even worse. What would the repercussions be on our society and the stress of our healthcare systems if cyber attackers were to exploit networked components in a food production facility and harm thousands?

Area of concern: networked production processes like food irradiation and potential vulnerabilities

Food irradiation is a technology that is commonly agreed to extend the shelf life of food and improve its safety for the consumer. The process of food irradiation removes microorganisms and insects that may cause disease or other harm to consumers. One of three FDA approved methods either involving gamma rays, X-rays, or via electron beams irradiates food. While some find fault in the use of this process, the FDA has evaluated irradiation for more than 30 years and deems it safe for a variety of foods. Critics of irradiation cite its ability to adversely alter a food's taste and potentially encourage manufacturers to take shortcuts in the realm of sanitation due to the belief that the process will subdue any safety defects that may have otherwise resulted.

Firms like Nordion develop complex and network connected systems designed to irradiate foods such as fruits and vegetables, meats, and spices. Nordion claims to have developed more than half of the world's large-scale irradiators. Informational videos on the firm's site depict the general process, which shows totes designed to carry foods and other products requiring irradiation through the system. Nordion boasts that its JS-10000, the "workhorse of industrial irradiators", integrates Programmable Logic Control (PLC) and Supervisory Control and Data Acquisition (SCADA) allowing for real-time status monitoring and easier handling of "difficult-to-dose" products.[6] The JS-10000's data sheet also notes that the system features network connectivity with options for remote diagnostics and troubleshooting.

Area of concern: cyber-attacks that result in consumers making misinformed purchases with big impacts

Attacks resulting in the misrepresentation of foods and other consumables raise concerns for both the availability and integrity dimensions of the C.I.A. triad. Today, we purchase food and beverage consumables more than ever online. Amazon Fresh and popular services like Blue Apron have finally brought technology within reach of our taste buds.

Individuals with unique dietary requirements as the result of food allergies are especially endangered by the risk of mislabeled food and beverage product information. An estimated 15 million Americans live with food allergies. Viewed another way, roughly 4% of adults and 8% of children in the United States have allergies.[7] A consumer with a nut allergy may see falsified information on a service like Amazon or a hacked menu board at a restaurant leading them to make a seemingly insignificant purchase that may affect their lives forever. In our fast-paced world, we place our trust blindly in companies and people that would otherwise give us no reason not to trust them. What happens when not even they know they cannot be trusted? It is safe to assume that most, if not all, business owners and their managers would prefer not be at the center of an attack. What happens when their products and services are the subject of intentional and malicious mislabeling via compromised technology? The consequences could mean life and death for someone.

We understand at least one method by which an attack renders information adulteration possible – it's called XSS (Cross-site Scripting). As a matter of fact, this has happened to Amazon before. In 2010, Dirk Wetter proved in his research article that Amazon could experience this type of attack on their site. He goes on to note that Amazon had corrected the issue within days of his uncovering it.[8] The danger of XSS is that malicious actors can alter information (wording/images) on a website resulting in a consumer unknowingly purchasing food or other consumables that are dangerous for the intended recipients. An XSS attack also has the ability to render a particular page/site unavailable if the attacker so desires – here lies a clear potential to affect the availability dimension of the C.I.A. triad.

The XSS attack type was discovered several years ago and for the most part is addressed in many modern applications. However, we've recently been reminded that not all sites and applications have caught up. Akamai, a leader amongst CDN service providers, announced in their quarterly (2017 Q1) *State of the Internet Security Report* that XSS attacks now account for 10% of all attacks on web applications.[9] The report continues to note that this number is up 3% from the prior quarter.

Area of concern: networked refrigerators and other smart devices interacting with food systems in the home

The internet is working its way into your private kitchens with appliances that want to do more than ever – introducing the smart refrigerator. It is important that we consider the impact of connecting devices integral to food systems to the internet where they may become vulnerable to attack.

LG is one manufacturer producing refrigerators that contain computers and software applications designed with the intention of making our lives simpler. One application LG plans to roll out in a refrigerator that was slated for production in late 2017 tracks the expiration dates of items inside. The prototype of this particular refrigerator runs on Windows 10 while production models are expected to use WebOS.[10] It is not outside of the realm of possibility to ponder a scenario where a malicious actor may find and exploit the refrigerator's software and alter the expiratory date of a highly perishable item resulting in food borne illness for an unsuspecting and trusting user.

Wal-Mart is testing an application that will allow consumers to order groceries on their website and have those groceries delivered directly to their refrigerator. This concept, unimaginable a decade ago, is made partially possible in thanks to the assistance of a smart lock on the exterior door allowing physical access for the delivery person. To alleviate any anxieties that may result from a complete stranger inside your home and refrigerator, Wal-Mart has partnered with IoT security firm August to facilitate cameras that allow you to watch as the delivery occurs.[11] What could possibly go wrong? Take a moment to consider the integrity principle of the C.I.A. cybersecurity triad. The integrity component is compromised if a malicious actor were to gain access to your delivery information potentially introduce something harmful to the contents of your refrigerator. It seems reasonable for consumers to assume that the infrastructure and software that facilitates a service of this nature from firm as large and trusted as Wal-Mart would not be vulnerable to compromise. Perhaps many will indeed make this assumption and are likely safe in doing so. However, can we make the same assumptions of other new players in the market offering similar services as popularity grows and the laws of economics take hold? These new players and Wal-Mart alike may only be as strong as their weakest segments of code in applications with potentially millions of lines.

Wise parties will carefully consider the benefits and drawbacks of networked technologies that integrate into food systems at home. These appliances have served us well for generations prior to their connection to the Internet and resulting automation. Careful consideration of the benefits paired with an elemental understanding of the cybersecurity risks is necessary for consumers to protect themselves and their families. In the very least, consumers that decide to move forward as pioneers of these connected appliances should not soon forget how to safely monitor the traditional functions of these appliances and the foods and other consumables they interact with.

Recommendations that raise cybersecurity awareness for all food system participants

An elemental understanding of cybersecurity and its potential impact on the devices we decide to integrate into our food systems is critical in protecting our populations while safely improving and modernizing food systems. Consumers and producers/facilitators alike need to take a proactive role in further communicating the real concerns and work together to foster the cybersecurity principles of integrity and availability (C.I.A.) in these connected and thus inevitably vulnerable devices.

While federal agencies, such as the FDA, may work to propose guidelines designed to address these concerns, we cannot simply rely upon regulation that moves slower than threats that are evolving daily. Professor Ming Chow, a computer science lecturer at Tufts University, has said "Politicians have little knowledge of tech and encryption. Technologists have little understanding of policy" … "Every stakeholder needs to be sitting at the same table. The consequences of not getting it right is that no one wins."[12] All participants must be proactive in securing the integrity of technology that plays a role in our food.

Attacks against our food systems may be complex but are more likely to be simpler in nature. Consider the theories of the principle of least effort. The principle postulates that people, animals, and even well designed machines will naturally choose the path of least resistance or "effort". As a result, older and considerably simpler methods of cyber-attack are likely to be exploited and need only find a single vulnerability in the entire attack surface to be successful.

Conclusion

Innovations in the role that technology plays in our food systems will inevitably continue to progress. We are not able to yet fully understand what impact of these future developments and their impact on the security of our food systems. It is, however, safe to assume that whatever is to come will likely use more software and boast the ability to connect to the internet. These new connected devices will aim to improve our quality of life and enhance our access to more high quality and nutritious foods. This greater level of connection will come at cost – reduced security due to existing and future vulnerabilities putting our food systems at risk.

As a society, we must remain cautious, yet supportive, of meaningful efforts to modernize components of our food systems. This is a responsibility that must be shared at all participation levels, from consumer to producer and ultimately government. Cautious participants will weigh the benefits and drawbacks of technologies that they consider implementing. They will also routinely re-evaluate the ongoing impact of these technologies as they are inevitably exploited. The C.I.A. triad of cybersecurity is a good starting point when determining what questions should be asked. In particular, it is wise to consider what will be the impacts on the integrity and availability components of the triad as a result of these technologies. Existing systems need to be frequently considered and scrutinized in the same manner.

Cyber-attacks will inevitably continue to plague our modern society. The effects of such attacks may have economic and health/safety consequences. Like many other threats, they will continue to manifest themselves in new forms. Many will also continue to exploit existing methods that may have been overlooked in software that is rapidly produced and continuously patched. For this reason, we must acknowledge that there is no resounding solution to protecting our food systems from cyber-attacks that have potential to impact few to many. The most advisable approach is to continuously increase awareness of the threat potentials across the board. We need to empower all parties to make informed decisions regarding cybersecurity that will ultimately lead to greater safety for all.

References

1. Zorabedian, J. (2017). What Developers Need to Know About the State of Software Security Today. [Blog] Veracode. Available at: https://www.veracode.com/blog/secure-development/what-developers-need-know-about-state-software-security-today [Accessed 8 Dec. 2017].
2. Monke, J. (2007). Agroterrorism: Threats and Preparedness. [online] Congressional Research Service, p.1. Available at: https://fas.org/sgp/crs/terror/RL32521.pdf [Accessed 8 Dec. 2017].
3. Hardy K., Williams G. (2014) What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism. In: Chen T., Jarvis L., Macdonald S. (eds) Cyberterrorism. Springer, New York, NY
4. Department of Homeland Security (2015). Food and Agriculture Sector-Specific Plan. p.6. Available at: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf [Accessed: 8 Dec. 2017]
5. Witman, S. and Witman, S. (2017). *The hackers in your yogurt*. [online] Quartz. Available at: https://qz.com/940825/the-food-industry-has-embraced-smart-technology-which-means-its-incredibly-vulnerable-to-hackers/ [Accessed 8 Dec. 2017].
6. Nordion. (2017). JS-10000 Hanging Tote Production Irradiator [online] Available at: http://www.nordion.com/gamma-technologies/js-10000-hanging-tote/ [Accessed 8 Dec. 2017].
7. National Institute of Allergy and Infectious Diseases, National Institutes of Health. Report of the NIH Expert Panel on Food Allergy Research. 2006. Retrieved from www3.niaid.nih.gov/topics/foodAllergy/research/ReportFoodAllergy.htm
8. Wetter, D. (2010). Research: Remarkable 2nd order XSS @ Amazon or How to hack Amazon with a book. [online] Drwetter.eu. Available at: https://drwetter.eu/amazon/storedXSS-vuln.at.amazon.html [Accessed 8 Dec. 2017].
9. Akamai (2017). Akamai's State of the Internet / Security [online] Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf [Accessed 8 Dec. 2017]

10. Barry, K. (2017). Finally: A fridge with Alexa that orders groceries for you. [online] USA TODAY. Available at: https://www.usatoday.com/story/tech/reviewedcom/2017/01/04/finally-a-fridge-with-alexa-that-orders-groceries-for-you/96155086/ [Accessed 8 Dec. 2017].
11. Monica, P. (2017). Walmart to deliver food to you and put it in the fridge. [online] CNNMoney. Available at: http://money.cnn.com/2017/09/22/technology/future/walmart-home-delivery-groceries/index.html [Accessed 8 Dec. 2017].
12. Pagliery, J. (2017). Congress puts terrorism and tech in the spotlight. [online] CNNMoney. Available at: http://money.cnn.com/2015/12/08/technology/encryption-congress-commission/index.html [Accessed 8 Dec. 2017].
13. Perrin, Chad. "The CIA Triad". Available at: https://www.techrepublic.com/blog/it-security/the-cia-triad/ [Access 8 Dec. 2017]