Section 3: Week 7: Future Needs

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 5, 2020

North Central University

# Future Needs

The Internet of Things (IoT) represents the next evolutionary step in communication and system connectivity. Naïve outsiders see this industry as a series of gimmicks, Apple watches, and smart toasters. Those statements are true, but more importantly, it also creates the missing bridge between cyber and physical systems (CPS). This capability comes from sensor and input networks that emit telemetry into ubiquitous cloud computing and machine learning platforms. Using physical motors and actuators, artificial intelligence and big data solutions can then reach back into manufacturing and safety systems. As information and decision processes transact across this bridge, it enables organizations to execute expert workflows autonomously and prevent costly failures. However, many challenges exist around ensuring the confidentiality, integrity, and availability (CIA) of all participants of this system.

## People

It can be helpful to think of identity within IoT as a profile of historical choices, stated preferences, user roles, and known associations (Wachter, 2018). When the device understands the context of the user’s profile, the experience can be customized and produce more accurate predictions. The payment for access to these inferences and decision processes comes from personal information, such as calendars, contacts, and routines (Mickens, 2018). This trade creates privacy concerns that can be subtle and barely noticed until much later.

For instance, numerous platforms integrate into open identity provides like Google and Facebook as a mechanism to simplify enrollment. However, is that the job the user intended to hire (Dai Zovi, 2019)? Through an exchange of convenience, the user becomes trackable across multiple sites and web services (Paller, Mahalik, Skoudis, & Ullrich, 2020). While the physical person wants a single sign-on experience, they also desire distinct virtual profiles across those providers (e.g., LinkedIn versus PornHub). Traditionally users have found these entanglements of context on their mobile devices, but these are not the only scenarios. Asking personal assistants, such as Siri, Alexa, and Google Home, if they spy on us, results in recommendations to review the privacy policy (Haselton, 2018). That response can be misleading since these policies exist as a liability disclaimer, not for the direct benefit of the user (Wachter, 2018).

## Process

Manufacturing facilities are evolving into massive CPS ecosystems through Industrial IoT devices feeding into complex event processing systems (Babiceanu, 2016). This approach reduces costs by increasing automation efficiencies. Reliance on automation also increases the opacity of decision-making processes and introduces additional risk vectors (Mickens, 2018). For example, an increase in network latencies might cause decision processes to act on outdated information. When perspective distortion exists between the cyber and physical structures, then accidents can follow, like autonomous vehicles not stopping or safety systems not initiating quick enough (Frodigh, 2018). CPS technologies can enter into this erroneous state due to Denial of Service states (DoS) caused by malicious actors, malware, and negligent software administrators.

## Products

According to Gartner, the trend of weak authentication controls impacts nearly 50% of all IoT vendors (Galinec & Steingartner, 2017). The Mirai malware was able to span half a million devices using a small dictionary file to brute force access (Gamblin, 2017). Although its source code has been available for several years, and its particularly noisy approach to gaining entry are discoverable, variations are still active (Kolias, Kambourakis, Stavrou, & Voas, 2017). While these programs should have encouraged a movement toward security by default, the broad industry has failed to act against even this rudimentary attack.

There is an economic incentive for businesses to churn out new IoT devices with more innovative, instead of investing in security protections for those features (Li & Liao, 2018). For many retail markets, the customer makes purchasing decisions solely on which product has the most features at the lowest price. Meanwhile, devices such as 8-bit micro-controllers, lack the computing resources necessary to support authentication, authorization, auditing, and transport encryption (Weber & Studer, 2016). Even when there are sufficient resources available, security protections can cause interoperation (interop) challenges, which leads to customers assuming that the device does not work. If the customer believes that the equipment is faulty, they leave bad reviews online, contact support, and request replacements—all of which cost the business money.

## Legal and Compliance

Creating universal regulations around security and compliance is a very challenging topic due to different political values (Matsubara, 2014). Even domestically, states like California, Delaware, and Utah have stricter expectations of privacy than federal requirements. When states redefine the minimum bar, it varies the expectation of acceptable use and results in litigation risks. Some organization approaches the problem by meeting the strictest set of requirements, but implementing the best protections might not be feasible on large codebases or for embedded systems (Weber & Studer, 2016).

When a customer purchases a traditional device, like a video player, they can exert full ownership. However, with everything as a service (XaaS), manufactures are relying on service integrations and Digital Rights Management (DRM) to retain control after the procurement (Oravec, 2017). These new licensing models enable organizations to collect monthly subscription fees and provide new features through software updates. This paradigm shift introduces dependencies, where failures in the third-party platform can cascade into the local environment. For instance, using Alexa requires installing microphones throughout the home and continuously streaming back to Amazon. After the content leaves the local network, nothing prevents the receiver from data mining for intimate conversations.