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 private schedules 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

## Products