Attributes that fall under “something you are” are the inherent physical characteristics of the user. Items in this category include things that we typically describe as biometrics and include items such as fingerprints, iris scans, facial recognition, and voice recognition. These are hard to fake accurately, but users are understandably hesitant to share this data with authenticators. These attributes are also subject to both false positives and false failures. Different sensors have different sensitivity levels, and conditions may prevent accurate capture of the biometric data. For the humble fingerprint sensor, this can be affected by things such as different placement of the fingerprint on the sensor, water or other contaminants on the sensor or fingerprint, or even temporary or permanent damage to the fingerprint. Because of these issues, biometrics typically

utilize a threshold value for how closely an authentication request needs to match the stored data. This leaves some room for attackers to attempt to imitate the biometric data. Additionally, if these methods are the sole method of access to a system, access can be permanently lost if physical damage occurs.

“Something you know” attributes are the standard items that most people think of when it comes to account access. Passwords, PINs, visual patterns, and security questions are all used to authenticate users under the assumption that they should be the only one who knows this information. Unfortunately, there are a lot of vulnerabilities for these methods. Passwords and PINs can be lost, stolen, or guessed. Answers to security questions can be phished or simply looked up on somebody’s Facebook page. Attackers can watch users input visual patterns, or simply guess based on the smudges present on a phone screen. Thankfully things like password managers have become more ubiquitous, making it easier to use random, secure passwords for each account, though this does greatly concentrate the risk of an attacker gaining access to the manager.

Finally, items that fall under “something you have” are physical items whose mere possession can be used to authenticate a user. Credit and debit cards are a common example of this, where a simple swipe can be used for payments. These items are commonly used for two-factor authentication, with apps on our phones providing a regularly changing PIN code that we access simply by being in possession of the phone. But just like the other methods, there are still vulnerabilities. One big one is what happens if the item is lost. If it was the sole thing allowing access to an account, we may be cut off from that account. Recovery questions/email (utilizing either “something you know” or another “something you have”) can make this situation more manageable. But a big issue comes when the item is stolen, particularly if it is not paired with another authentication method. Losing an access badge that permits entry with just a swipe could easily permit unauthorized entry into a facility.

I’ll use my work as an example. In order to enter the main building, I require an access badge that requires a PIN to function. An additional layer on top of that is that each badge is only permitted to enter certain areas, and this access whitelist is centrally controlled. This method was likely chosen as it is simple and provides “good enough” security. Badges are cheap to produce, a swipe plus PIN access system is common enough to not be excessively expensive. It also allows the security managers to track who enters through what doors and at what time in the event of a security incident. And the combination of badge plus PIN provides two-factor authentication that doesn’t permit entry simply by finding or stealing a badge. From the user side, the badge plus PIN system is easy enough to use so there’s no reason to try to subvert it to make things easier. I am by no means an expert, but it does seem to provide adequate security. The main vulnerability is human nature. People tend to be nice, and unfortunately from a security perspective that involves holding doors for people (piggybacking). This could bypass the security system permit entry simply by obtaining a badge.