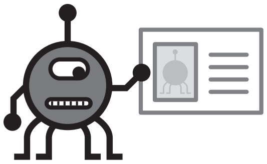

IV
Determining Identity

Summary

It’s not enough to have a secure connection between two machines. You also need to be sure that the person or computer you’re connected to is who it claims to be. This part discusses the pros and cons of the many available identification systems as well as ideal technology combinations.

Key Points

- Philosophy tells us that a person is more than just the uniqueness of his or her body.
- Technology views a person as a combination of attributes, knowledge, actions, and possessions.
- A digital identity allows the defining characteristics of a person to be rapidly accessed whenever and wherever necessary.
- When properly combined, multiple types of identification technology can improve security.

Connecting the Chapters

Modern identification systems use a combination of technologies, ranging from simple passwords to complex biometric systems (such as fingerprint or retina scanners). This part’s chapters explore the most commonly used identification technologies and concepts as follows:

- **Chapter 8, “Passwords,”** examines the words, phrases, or patterns that grant access to a system.
- **Chapter 9, “Digital Certificates and Trusted Authentication,”** covers the electronic documents that verifiably prove the bearer’s identity.
- **Chapter 10, “Portable Identifiers,”** discusses the physical items that can associate a digital identity with the bearer.
- **Chapter 11, “Biometrics,”** concerns the technologies that measure a person’s vital statistics in order to determine identity.

Introduction to Determining Identity

Throughout history, humanity has been making an ongoing effort to discover itself. We have accumulated and analyzed knowledge and wisdom for thousands of years. For the most part, the goal has been to find answers to two simple questions: "Who am I?" and "Why am I here?"

AU: No footnote for footnote 1 reference.

Sadly, little progress has been made. Although we can provide functional answers to complicated questions such as, "What keeps the earth from crashing into the sun?" we're still at a loss when it comes to those seemingly simple questions. And even then, all we really know is what we've observed, and how do we know our observations are complete? Even worse, these questions beg the shortest and most complicated question of all: "Am I?" You'd think this one would be easy. After all, the only possible answers are yes or no.[1] Unfortunately, philosophers can't agree on either one of them.

The young, brash Western philosophers shout, "Yes, I am!" After all, if there's no self, there can be no identity. If there's no identity, there can be no ownership. If there's no ownership, there can be no capitalism. If there's no capitalism, there can be no Coca-Cola, and we get very grumpy without our daily dose of caffeine. When asked to give a reason for this inarguably practical logic, Descartes succinctly replied, "Cogito ergo sum."

In contrast, the ancient Eastern philosophers believed that the self does not exist. In their view, we are all part of a cosmic unity. The sense of individuality that we call our self is just an illusion of perception. With the right frame of mind, one can see through this illusion and join completely with the singular consciousness. One might achieve such enlightenment by pondering this Zen koan: Who is the difference between one self?

The illusion of reality may be interesting to some, but try explaining it to a hungry person. Eventually, if our individual physical bodies don't get food, we starve and die. In today's world, it's understandable why Western thought is the easier of the two to swallow (sorry). That's a good thing for us, because it's the only mindset compatible with a chapter on identification technology.

Modern society blends philosophical, religious, and technical perspectives on humanity. Most of us Western thinkers assume we have a self, and that it's the only one attached to our body (schizophrenics and those who are possessed might not be so certain). When we see other bodies walking around, we assume they have unique selves too. We call these wandering self-body combinations people. Based on our assumptions, we learn to identify people by the unique features of their bodies. Faces, shapes, voices, smells, movement patterns—these are physical attributes that help us differentiate among people.

A person is more than just the uniqueness of his or her body; people can also be defined by their behavior, their knowledge, the history of their actions, and the items they possess. When this information is shared or well known, it provides an alternate means of identification that can be used in the absence of physical recognition. For example, you may be looking for somebody you've never met. You've been told that she's a tall woman (physical) wearing a leather jacket and a red scarf (possessions). She walks in a funny manner (behavior) and her name is Sarah (knowledge). By combining these factors, you can identify this unknown person with a large degree of certainty.

When you have finished mulling over these deep thoughts about the nature of identity, you may want to drop by your local bank and make a withdrawal. Afterwards, maybe you'll go shopping. During each transaction, you will have a very real need to prove your identity, especially if paying with a credit card. Philosophy won't help you here. Technology has its own way of looking at you that is neither Eastern nor Western. In today's world, your digital identity is just as important as any other self you may or may not have.

Your Digital Identity in General

Philosophy asks, what makes someone what he or she is? Is it his personality or his work? What truly defines a person? What provides every individual on this planet with a sense of distinctiveness?

Identification technology asks, who are you? Tell me who you are. Can I believe that you are who you say you are? How can I trust you? How can I determine your identity with accuracy? How do I know you are not pretending to be someone else? Will anybody vouch for you?

Although philosopher might wax eloquently about the nature of identity, technology does not treat such matters esoterically. Technology is forced to view the defining qualities of a person in a clinical manner through precise and accurate measurements that can be consistently repeated. Computers simply do not have the capacity to factor in the immeasurable. For example, no accurate way exists to measure all the changes in a person's body and behavior due to stress. Computers therefore cannot predict the effect a person's level of stress will have on their voice and body patterns. To a computer, a person under high stress may appear to have a completely different identity.

Using technology for identifying people isn't perfect, but it's a necessary component of a modern society. Technology can provide trustworthy methods for proving identity in a global society where it's often impossible to personally verify if someone is who he or she claims to be. For example, if you purchased a cell phone and a service account, the service provider checked your credit report before they decided to extend you the credit of using their phone service. These typical authentication methods prove that as the global economy grows, the world is getting smaller. Technology provides the necessary means for achieving this.

In another example, when a person becomes financially independent, he or she also begins to build a digital financial identity. Computers record the details of every banking and credit transaction, all of which are collected, organized, and analyzed by several different organizations. In some cases, information is collected from external sources, such as government records. Organizations also exchange information in order to build more accurate and extensive digital profiles. The centralization of this information makes it easy for vendors to obtain digital profiles whenever they need to verify the identity and financial status of a customer. This most frequently happens when a vendor wants to extend credit to a customer.

The Perils of Digital Identity

Most of the time, consumers enjoy the benefits of convenience that come with centralized digital identities. The problems only happen when someone uses the F word, *fraud,* which has become a major problem in the last decade. Criminals have realized it is easier to steal digital money than it is to steal the green variety. The key to virtual robbery is virtual impersonation. Grab somebody's digital identity, and you can take his or her digital assets.

Identity theft is accomplished by obtaining the few pieces of information needed to establish a trusted digital identity. This is not difficult to do. You would be surprised how much of the necessary information is contained in your junk mail. For example, your name, address, and date of birth are often found on common credit card offers, most of which end up in your garbage. Intercepting the right piece of real mail can provide a thief with even more information, such as your bank account numbers and your social security number. Public records can be used to fill in the gaps (see Figure IV-1).

Instant Approval!!!

The credit check process begins when a consumer gives a vendor or store clerk certain bits of critical information about himself. This information is required to verify his digital identity. It usually includes his home address and phone number, date of birth, and social security number.

Once the consumer's identity has been established, a summary score is displayed to the vendor. This score is a dynamic view of the consumer's financial history. The score quickly informs the vendor whether the consumer is a high, medium, or low credit risk. The vendor then makes an instant decision about taking the consumer on as a customer.

This system has its strong and weak points. The speed of information retrieval is a tremendous asset to many creditors. In addition, the credit scoring system provides an accurate evaluation of a consumer's ability to take on additional debt and pay bills on time. But errors do occur. It is unfortunately the consumer's responsibility to ensure that the information is accurate. The trouble is that in many cases, the consumer either has no control over the information or is unaware that the information even exists. It is also difficult, if not impossible, for a consumer to control the way their digital profile is used.

Once these pieces of information are assembled, the holder can begin impersonating the unlucky victim. The information can be used to open credit card accounts, activate cell phones, and even lease automobiles. Identity theft is a federal crime. That said, justice is served far less often than necessary. Identity thieves are difficult to catch, and it's equally difficult to obtain substantial proof for prosecution.

Proving Your Identity

Illustration by SageSecure

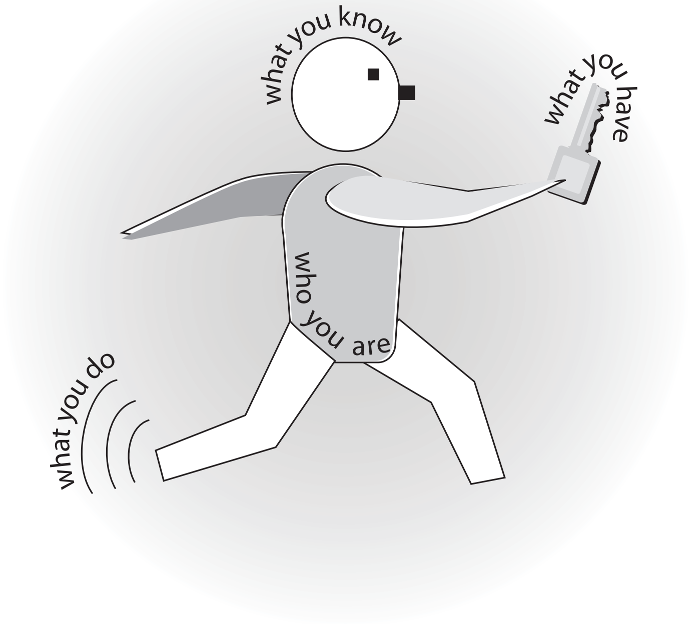

Figure IV-1

Catching the perpetrators of identity theft crimes is complicated by the fact that most people do not realize they are being victimized until months after the crime has occurred. Usually, the first indication of a problem is a call from an unfamiliar creditor trying to collect money. The victim's response is that the creditor has made a mistake. "I don't have a cell phone account with that company. How can I owe them any money?" The cell phone may only be the tip of the iceberg. Credit cards, lines of credit, and other financial services may have been abused. Crimes may even have been committed in the victim's name, and he or she can look forward to weeks of frustration tracking down and clearing every identity abuse. Years after the fact, he or she will continue to have trouble obtaining legitimate credit due to damage done by the thief.

By the time the dust settles and police reports have been filed, the relatively anonymous criminal is long gone. No perpetrator is apprehended and no record exists for how all this occurred, so who gets stuck with the fraudulent charges? In the best-case scenario for the victim, the credit lender or the vendors take the hit. However, the additional costs of fraud absorbed by vendors each year are ultimately passed onto the consumer.

Digital Identity: The Secure Way

Identity theft is a disaster. What can be done about it? As we've stated before, it's not possible to provide total security for anything, but it is possible to raise the bar way above the heads of most criminals. A good security system is too complex or costly for the average crook to crack. In the case of secure identification, raising the bar involves using a combination of techniques for establishing identity.

Earlier in this chapter, we showed you how a person could be viewed as a collection of physical attributes as well as a set of knowledge, behavior, possessions, and history. These are called *identification factors*, and modern security theory has organized them into the following four categories (see Figure IV-2):

- *What you know* refers to specific *knowledge* that can help someone prove his or her identity. This needs to be knowledge that uniquely relates to a particular individual. The most common example is a password. Other examples include personal history details, such as a mother's maiden name, elementary school teachers, or pet names. Government-issued identification numbers are also frequently used. The lesser known the information, the more secure it is as an identification factor.

  Counterpoint: Many supposedly private bits of data are actually not as private as you'd think. A large amount of personal historical information is publicly available or otherwise easy to discover.

- *What you have* refers to items that are in one's *possession*. These portable identifiers include physical keys, documents, clothing, jewelry, vehicles, and residences. Items that are easy to carry and difficult to duplicate are the most appropriate to use as a basis for identification. Unique documents, such as birth certificates, passports, and government identifications are designed to make duplication incredibly difficult. Credit cards and keys are easier to duplicate, but more convenient for daily transactions.

  Counterpoint: If an item is lost or duplicated, somebody else can use it to impersonate the original owner. Physically protecting the identifying item becomes critical and makes the item less convenient to use.

- *What you are* refers to physical *attributes* unique to one's physical and biological makeup. Examples of these traits include fingerprints, hand topography, hand geometry, and retina/iris patterns. Each one is extremely difficult to duplicate and very specific to a person. Biometric systems are used to record and compare these physical traits.

  Counterpoint: Biometric systems use computers, which can be tricked or bypassed. It's easy to mistake the precision of a biometric system for accuracy. For example, biometric fingerprint scanners may mistakenly grant access to a gel mold of an authorized fingerprint.

- *What you do* refers to unique patterns of *action* that a body generates. This includes handwriting, typing, speech, and movement patterns. These

Identity Theft

Illustration by SageSecure

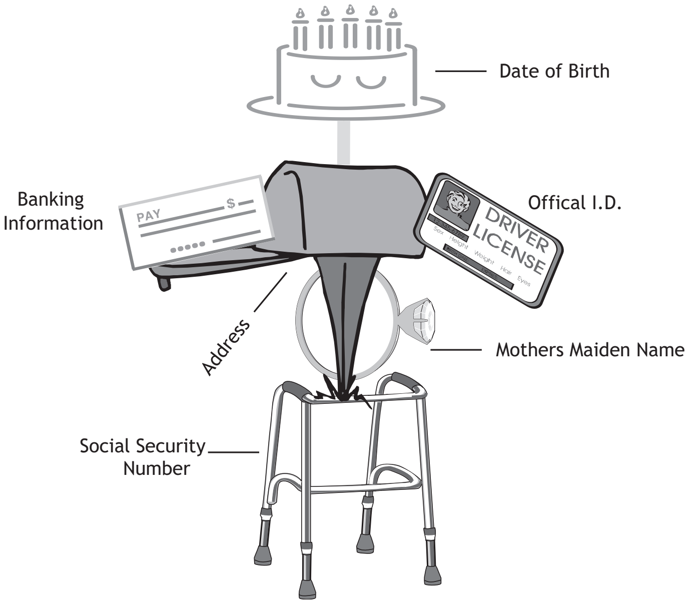

Figure IV-2

characteristics are far less consistent than direct physical traits, as they are easily influenced by external factors. For example, an awkward writing surface can make a signature unrecognizable, and loud background noise can do the same to a voice. Even under good conditions, the patterns exhibit a wide variance. As a result, systems that capture and compare these traits often have a large tolerance for variations. Such tools are also considered biometric systems.

Counterpoint: Forgers and impersonators take advantage of the tolerance for natural variations, knowing that "close enough is good enough" in many cases. A signature is an example of an easy-to-forge pattern that is commonly used as a critical identification factor in many situations (for checks, credit cards, and so on).

How Many Factors?

A determined intruder can fake any of the four identification factors, but faking more than one factor simultaneously is a significantly harder task. A security system that requires validation of all four factors is difficult to fool. Of course, this assumes that the identification system as a whole isn't the weakest link. To that extent, we can call the security level of the system itself the *fifth factor*.

Ideally, every critical system should require users to satisfy all four identification factors. In reality, this is hard to implement. Each identification factor requires a different type of verification infrastructure. Combining all four into a single system requires complete control over the operational environment. Without total control, compromises are made based on the nature of the environment and lead to weaknesses in the entire identification system.

For example, a high-security system might require an ID card, a voiceprint, a handprint, and a password. This might be easy to implement if you're securing the door to a facility. The environment can be physically secured, preventing intruders from attacking the identification system. But what if you're securing a network with remote users? Are you going to equip every desktop and remote user with a hand/card/voice scanner? If so, how are you going to protect the identification system? What will prevent an intruder from compromising a remote computer and capturing or replaying the identification information? Can you physically protect your remote users from being forced to log in at gunpoint?[2] The identification system can only be as secure as the weakest link.

Designing an effective identification system requires balance and consistency. The importance of ensuring identification needs to be weighed against the practical needs of the business. It's useless to worry about secure identification if an unidentified person can obtain the same information through other channels. For example, if an intruder can gain physical access to the network and critical computers, the intruder can bypass all the identification systems by directly accessing the desired data or observing the data in transit.

Similarly, the use of identification technology needs to be consistent throughout the system. Inconsistencies create opportunities for intruders. One of the most inconsistent systems in common use is the credit card. A credit card with a photograph has all four identification factors: what you have (the card), what you do (the signature), what you know (the card number, expiration date, and billing address), and what you are (the picture). This four-factor system seems secure, until you realize that only one factor is necessary in most situations. If you're at a restaurant or a retail store, only possession is necessary, because most waiters and register operators will not closely check the signature. Online or over the phone, neither possession nor a signature is needed, just the knowledge of the card number and other card details. Criminals only need to obtain the card number, expiration date, and billing address or the card itself to gain full use of the credit account. As a result, credit cards are an extremely easy and effective vehicle for fraud.

In most cases, two properly and consistently implemented factors will provide enough security. A password combined with either a physical item or a biometric

[2] Most sane managers probably don't worry about remote users being held at gunpoint. After all, few organizations are involved in anything that would attract gun-toting criminals. Furthermore, intruders rarely need to resort to such extreme measures.

measurement raises the bar adequately against most intruders. A three-factor system, however, that combines passwords, biometrics, and physical identifiers is considered even more secure. "What you do" patterns (other than signatures) are generally used as a fourth or optional factor in ultra-high security systems that have very controlled environments.

New consumer computing devices will make implementing multiple-factor systems easier and more convenient without sacrificing the security of the entire identification system. Devices such as laptops, keyboards, and mice are already integrating fingerprint scanners and card readers. Combination devices are being developed that look like credit cards but can also read fingerprints and generate pass codes. These devices will be responsible for integrating biometrics into many aspects of daily life.

Final Thoughts

The rest of the chapters in this part examine the major technologies used for identification: passwords, digital certificates, physical identifiers, and biometrics. We'll also look at systems for centrally managing and controlling complex identification systems across a networked environment. Understanding these technologies will help you design or improve a comprehensive identification system within your own organization.