Authentication Methodologies

A computer system does not have the cues we do with face-to-face communication that let us recognize our friends. Instead computers depend on data to recognize others.

Determining who a person really is consists of two separate steps:

- Identification is the act of asserting who a person is.
- Authentication is the act of proving that asserted identity: that the person is who she says she is.

Types of Authentication

Authentication Based on Phrases and Facts: Something You Know

Password Protection seems to offer a relatively secure system for confirming identity related information, but human practice sometimes degrades its quality. Let us explore vulnerabilities in authentication, focusing on the most common authentication parameter, the password. In this section we consider the nature of passwords, criteria for selecting them, and ways of using them for authentication.

How secure are passwords themselves?

Passwords are somewhat limited as protection devices because of the relatively small number of bits of information they contain. Worse, people pick passwords that do not even take advantage of the number of bits available: Choosing a well-known string, such as **qwerty, password, or 123456** reduces an attacker’s uncertainty or difficulty essentially to zero.

Knight and Hartley [KNI98] list, in order, 12 steps an attacker might try in order to determine a password. These steps are in increasing degree of difficulty (number of guesses), and so they indicate the amount of work to which the attacker must go in order to derive a password. Here are their password guessing steps:

- no password

- the same as the user ID

- is, or is derived from, the user's name

- on a common word list (for example, password, secret, private) plus common names and patterns (for example, qwerty, aaaaaa)

- contained in a short college dictionary

- contained in a complete English word list

- contained in common non-English-language dictionaries

- contained in a short college dictionary with capitalizations (PaSsWorD) or

substitutions (digit 0 for letter O, and so forth)

- contained in a complete English dictionary with capitalizations or substitutions

- contained in common non-English dictionaries with capitalization or substitutions

- obtained by brute force, trying all possible combinations of alphabetic characters

- obtained by brute force, trying all possible combinations from the full character set

Although the last step will always succeed, the steps immediately preceding it are so time consuming that they will deter all but the most dedicated attacker for whom time is not a limiting factor.

Good Passwords

Chosen carefully, passwords can be strong authenticators. The term **"password"** implies a single word, but you can actually use a non existent word or a phrase. So **2Brn2Bti?** could be a password **(derived from "to be or not to be, that is the question")** as could "**PayTaxesApril15th.**"

Note that these choices have several important characteristics: The strings are long, they are chosen from a large set of characters, and they do not appear in a dictionary. These properties make the password difficult (but, of course, not impossible) to determine.

If we do use passwords, we can improve their security by a few simple practices:

- Use characters other than just a–z. If passwords are chosen from the letters a– z, there are only 26 possibilities for each character.
- Adding digits expands the number of possibilities to 36.

- Using both uppercase and lowercase letters plus digits expands the number of possible characters to 62.

Although this change seems small, the effect is large when someone is testing a full space of all possible combinations of characters. It takes about 100 hours to test all 6-letter words chosen from letters of one case only, but it takes about 2 years to test all 6-symbol passwords from upper- and lowercase letters and digits. Although 100 hours is reasonable, 2 years is oppressive enough to make this attack far less attractive.

Authentication Based on Biometrics: Something You Are

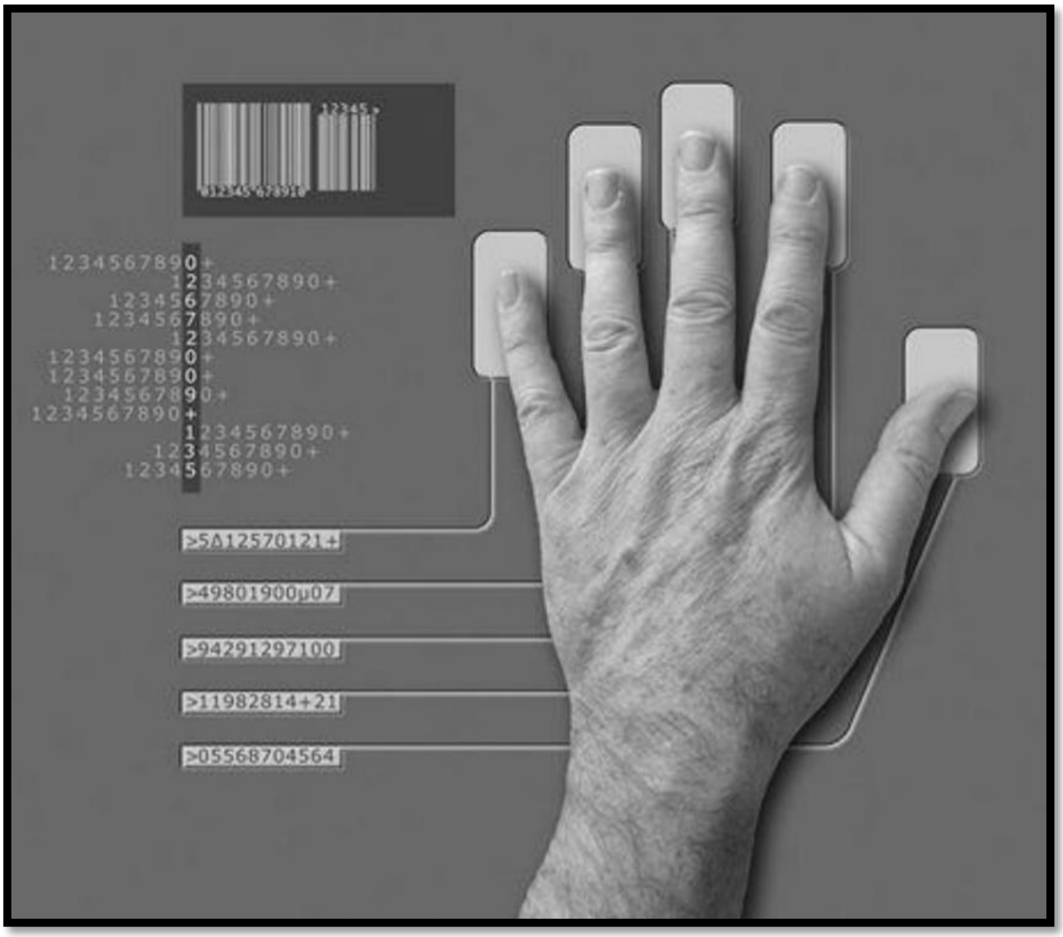
Biometrics are biological properties, based on some physical characteristic of the human body. The list of biometric authentication technologies is still growing. Now devices can recognize the following biometrics:

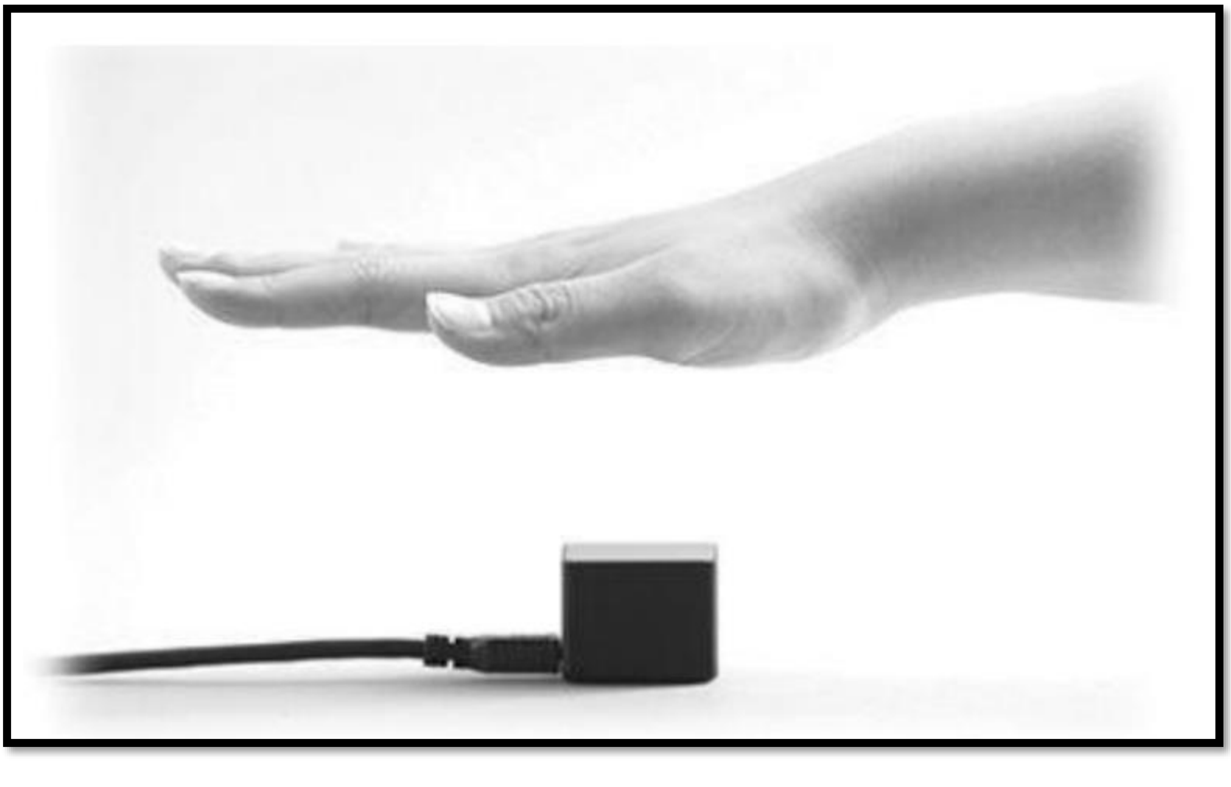
- fingerprint
- hand geometry (shape and size of fingers)
- retina and iris (parts of the eye)
- voice
- handwriting, signature, hand motion
- typing characteristics
- blood vessels in the finger or hand
- face
- facial features, such as nose shape or eye spacing

Authentication with biometrics has advantages over passwords because a biometric cannot be lost, stolen, forgotten, or shared and is always available, always at hand, so to speak. These characteristics are difficult, if not impossible, to forge.

Examples of Biometric Authenticators

Many physical characteristics are possibilities as authenticators. In this section we present examples of two of them, one for **the size and shape of the hand**, and one **for the patterns of veins in the hand**.


12345+
912345 678910
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
1234567890+
>5Δ12570121+
>49801900µ07
>94291297100
>11982814+21
>05568704564



Problems with Use of Biometrics

Biometrics come with several problems:

- **Biometric recognition devices are costly**, although as the devices become more popular, their cost per device should go down. Still, outfitting every user's workstation with a reader can be expensive for a large company with many employees.

- **Biometric readers and comparisons can become a single point of failure.** Consider a retail application in which a biometric recognition is linked to a payment scheme: As one user puts it, ***"If my credit card fails to register, I can always pull out a second card, but if my fingerprint is not recognized, I have only that one finger."*** (Fingerprint recognition is specific to a single finger; the pattern of one finger is not the same as another.) Manual laborers can actually rub off their fingerprints over time, and a sore or irritation may confound a fingerprint reader. Forgetting a password is a user's fault; failing biometric authentication is not.

- **All biometric readers use sampling and establish a threshold for acceptance of a close match.** The device has to sample the biometric, measure often hundreds of key points, and compare that set of measurements with a template. Features vary slightly from one reading to the next, for example, if your face is tilted, if you press one side of a finger more than another, or if your voice is affected by a sinus infection. **Variation reduces accuracy**.

- Although equipment accuracy is improving, false readings still occur. We label a **false positive or false accept** a reading that is accepted when it should be rejected and a **false negative or false reject** one that rejects when it should accept. Often, reducing a false positive rate increases false negatives, and vice versa. The consequences for a false negative are usually less than for a false positive, so an acceptable system may have a false positive rate of 0.001 percent but a false negative rate of 1 percent. However, if the population is large and the asset extremely valuable, even these small percentages can lead to catastrophic results.

Authentication Based on Tokens: Something You Have

Something you have means that you have a physical object in your possession. One physical authenticator with which you are probably familiar is a key. When you put your key in your lock, the ridges in the key interact with pins in the lock to let the mechanism turn. In a sense the lock authenticates you for authorized entry because you possess an appropriate key. Of course, you can lose your key or duplicate it and give the duplicate to someone else, so the authentication is not perfect. But it is precise: Only your key works, and your key works only for your lock.

Other familiar examples of tokens are badges and identity cards. You may have an "affinity card": a card with a code that gets you a discount at a store. Many students and employees have identity badges that permit them access to buildings. You must have an identity card or passport to board an airplane or enter a foreign country. In these cases you possess an object that other people recognize to allow you access or privileges. Another kind of authentication token has data to communicate invisibly.

Examples of this kind of token include credit cards with a magnetic stripe, credit cards with an embedded computer chip, or access cards with passive or active wireless technology. You introduce the token into an appropriate reader, and the reader senses values from the card. If your identity and values from your token match, this correspondence adds confidence that you are who you say you are.

Active and Passive Tokens

As the names imply, passive tokens do nothing, and active ones take some action. A photo or key is an example of a passive token in that the contents of the token never change. (And, of course, with photos permanence can be a problem, as people change hair style or color and their faces change over time.)

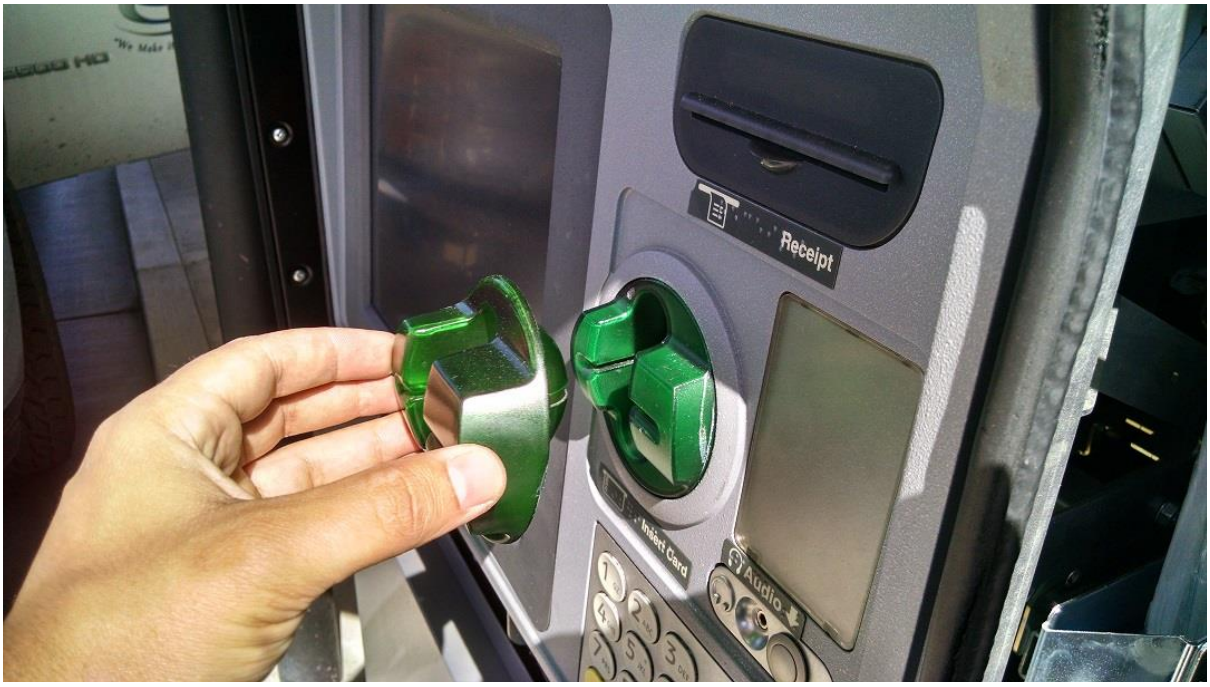
An active token can have some variability or interaction with its surroundings. For example, some public transportation systems use cards with a magnetic strip. When you insert the card into a reader, the machine reads the current balance, subtracts the price of the trip and rewrites a new balance for the next use. In this case, the token is just a repository to hold the current value. Another form of active token initiates a two-way communication with its reader, often by wireless or radio signaling. These tokens lead to the next distinction among tokens, static and dynamic interaction.

Static and Dynamic Tokens

The value of a static token remains fixed. Keys, identity cards, passports, credit and other magnetic-stripe cards, and radio transmitter cards (called RFID devices) are examples of static tokens. Static tokens are most useful for onsite authentication: When a guard looks at your picture badge, the fact that you possess such a badge and that your face looks (at least vaguely) like the picture causes the guard to pass your authentication and allow you access.

Tokens are vulnerable to an attack called **Skimming**. Skimming is the use of a device to copy authentication data surreptitiously and relay it to an attacker. Automated teller machines (ATMs) and point-of-sale credit card readers are particularly vulnerable to skimming.

At an ATM the thief attaches a small device over the slot into which you insert your bank card. Because all bank cards conform to a standard format (so you can use your card at any ATM or merchant), the thief can write a simple piece of software to copy and retain the information recorded on the magnetic strip on your bank card. Some skimmers also have a tiny camera to record your key strokes as you enter your PIN on the keypad. Either instantaneously (using wireless communication) or later (collecting the physical device), the thief thus obtains both your account number and its PIN. The thief simply creates a dummy card with your account number recorded and, using the PIN for authentication, visits an ATM and withdraws cash from your account or purchases things with a cloned credit card.



To overcome copying of physical tokens or passwords, we can use **dynamic tokens**. A dynamic token is one whose value changes. Although there are several different forms, a dynamic authentication token is essentially a device that generates an unpredictable value that we might call a pass number. Some devices change numbers at a particular interval, for example, once a minute; others change numbers when you press a button, and others compute a new number in response to an input, sometimes called a challenge. In all cases, it does not matter if someone else sees or hears you provide the pass number, because that one value will be valid for only one access (yours), and knowing that one value will not allow the outsider to guess or generate the next pass number.