

## Q.What is an authentication factor?

### Authentication

Passwords and passphrases are one example of a form of security measure called authentication.

Authentication would be used in: ➤ a restricted area ➤ a computer system ➤ an Internet service ➤ encrypted document

An authentication factor is a procedure or chunk of information used to authenticate an individual, that is, to verify that he or she has access rights

## Q. Describe with the aid of examples the three classes of authentication factors.

### Authentication factors generally fall into one of three classes:

➤ Inherence (or human) factors — “Something you do” These include biometric measures for identifying the individual by a physical characteristic such as fingerprints, iris or retina recognition, or automated face recognition.

➤ Ownership (or technical) factors — “Something you have.” These include identity cards, communications devices such as passcode tokens, or even a traditional metal key.

Knowledge (or personal) factors — “Something you know.” These include passwords or passphrases, a PIN (personal identification number) or other passcode



## Q. Give an example of two-factor authentication using a token card.

- In the most common implementations of two factor authentication
- The token card is a compact electronic device which displays a number on a small screen. By entering this number into the system when you attempt to authenticate (login), you prove that that you are in possession of the card.
- The number displayed by the card changes frequently, usually every 30 or 60 seconds.
- To increase security, the electronic device is sometimes protected with a PIN.

**Q. Give an example of biometric authentication. Why are users often unhappy with biometric authentication?**

### **Biometrics**

- Biometric authentication satisfies the regulatory definition of true multi-factor authentication.
- Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware
- There is great user resistance to biometric authentication.
- For many biometric identifiers, the actual biometric information is rendered into string or mathematic information.
- Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved.

### **Cons:**

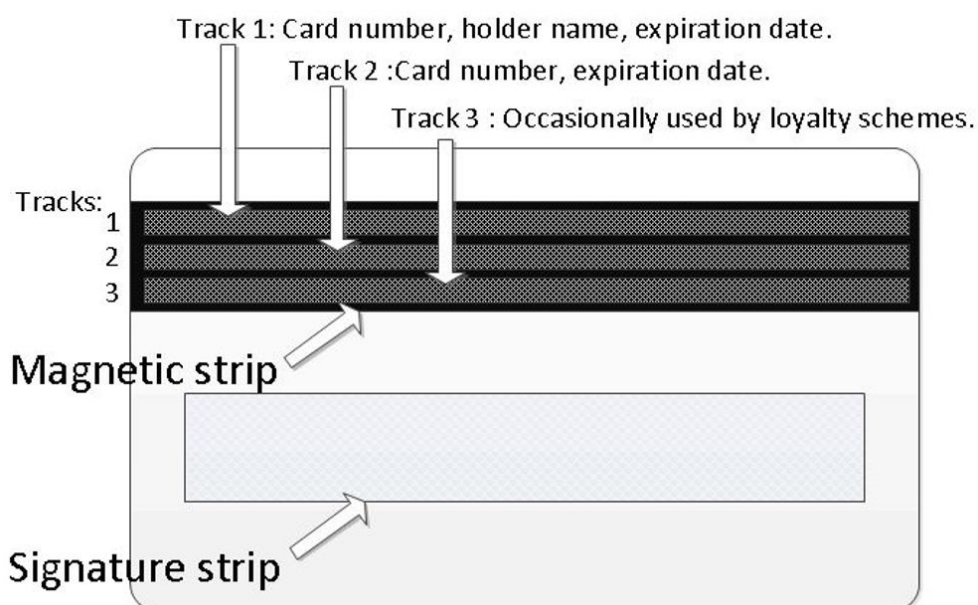
- Possibility of false positives and negatives.
- Biometric information may be mechanically copied and they cannot be easily changed. This is perceived as a disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his/her password, however, a user cannot change their fingerprint.
- A bio-identifier can also be faked. For example, fingerprints can be captured on sticky tape and false gelatine copies made, or simple photos of eye retinas can be presented. More expensive biometrics sensors should be capable to distinguish between live original and dead replicas, but such devices are not practical for mass distribution



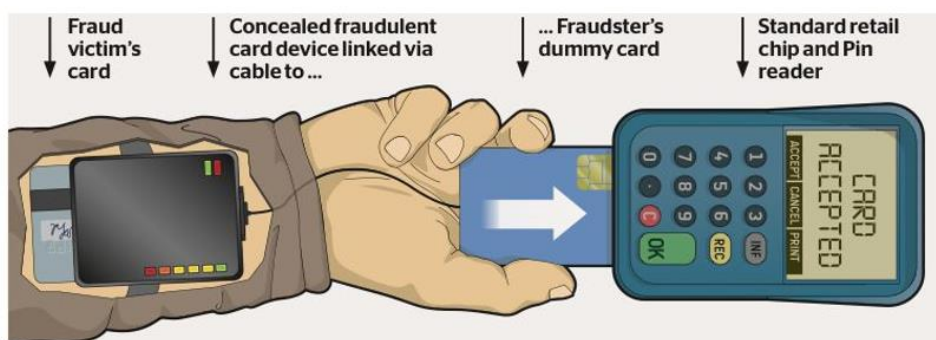
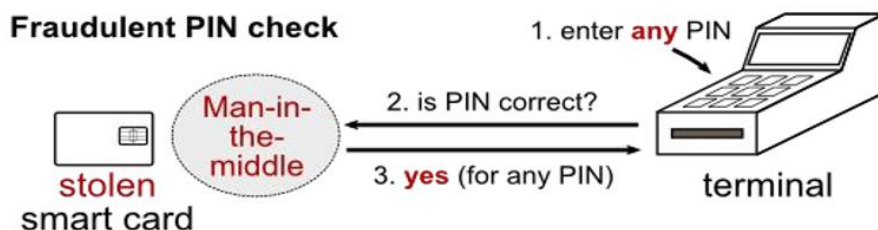
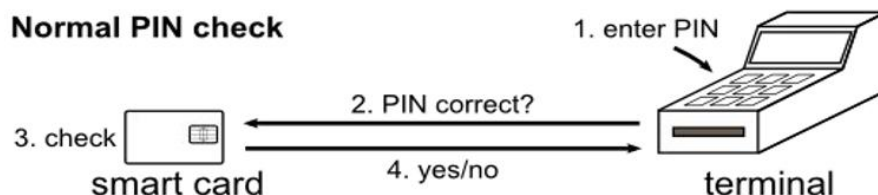
**Q. Explain how magnetic cards have inbuilt two-factor authentication that prevents card cloning.**

### Magnetic Cards

- Magnetic cards (credit cards, debit cards, ATM cards, gift cards, etc) combined with secure, encrypting card readers provide a possible solution for two-factor/strong authentication.
- Each magnetic stripe card has unique characteristics much like the card's own fingerprint called a magnetic fingerprint.
- The advantage is that a magnetic fingerprint already exists on every magnetic stripe card because it is an intrinsic characteristic and no cards would need to be re-issued.
- Each swipe of the card provides a correlative number called a dynamic digital identifier that can be scored and "matched" to the originating value to determine the cards authenticity.



**Q. Describe how the use of Smart Cards be compromised through sidechannel attacks.**



**Q. What is the principle of least privilege?**

### Principle of Least Privilege

“The principle of least privilege requires that in a particular abstraction layer of a computing environment, every module must be able to access only the information and resources that are necessary for its legitimate purpose.”

This practice is just good common sense as it prevents a number of problems, some of the benefits of such a system:

- Better Stability – users cannot break systems they do not have access to
- Better Security – Malware is limited in its propagation
- Easier to Deploy – applications designed with this in mind are easier to deploy and maintain

**Q. Describe how the “principle of least privilege” improves a system’s stability, security and easy of deployment of systems.**

This practice is just good common sense as it prevents a number of problems, some of the benefits of such a system:

- Better Stability – users cannot break systems they do not have access to
- Better Security – Malware is limited in its propagation
- Easier to Deploy – applications designed with this in mind are easier to deploy and maintain

**Q. Describe classes of weak passwords.**

It’s good practice to avoid the following common strategies when deciding on a password. ➤ Any correctly spelled English word, especially one which is likely to be recognized by operating system or application spell-checkers and so on ➤ Any correctly spelled non-English word ➤ Any part of your own name or username ➤ Any part of the name of a member of your extended family (including pets) or, worse, a colleague, your boss, or, in fact, anyone’s name ➤ Place names are often easily guessed ➤ The name of the OS you’re using, or the name of the PC you’re using or the hostname of a server you’re accessing ➤ Song, book and movie titles, famous people, cartoon characters ➤ Anything so unmemorable you have to write it down

➤ Reusing passwords

**Q. Describe how you would choose a strong password**

**Techniques that may help in slowing down password breaking** by guessing or simple dictionary attacks include the following.

- The more combinations of techniques you use in a single password, the more effective they’re likely to be
- Embed control characters or non-alphanumeric symbols
- Unorthodox caPitaliZation
- Use a personally significant acronym, e.g., ICRMFPW (I Can’t Remember My Friendly Password)
- USE A PASSPHRASE

**Q. What is the golden rule relating to the use of passwords?**

**Why do you need a good password?**

- One of the most common forms of automated attack on a corporate system is password guessing,

- while attempting to steal passwords from targeted individuals by various forms of social is also used.
- On many systems, most untrusted services are still protected primarily by passwords rather than by more glamorous methodologies such as smart cards, biometric systems, hand-held authentication and so on.
- Insecure passwording, whether as a result of bad systems practice or bad user practice, may endanger data in breach of data protection legislation, contractual obligation, or corporate policy.

### **Good User Practise**

It has been estimated by CERT-CC that “80 percent of all network security problems (are) generated by bad passwords.”

We can't actually demonstrate the accuracy of that statistic, but it does at least indicate anecdotally how seriously the security community regards the issue of password security.

**So here are some ideas that should make you less vulnerable to password-related problems as an end-user.**

### **Don't Share Passwords**

Don't share passwords unless there's a formal protocol set up to allow it. More than one person sharing an account is (except under “very” controlled conditions) a major threat to security.

- The more people with access, the greater the risk.
- Attacks on computer systems can come from inside as well as outside. This should be of particular concern to an end-user who is not cautious about sharing account information.
- If an attack is traced to a particular account, the holder of that account will be the prime suspect. Accidental or deliberate extension of access to intruders.

### **Anti-Social Engineering**

Be aware of the social engineering approach to cracking passwords. The quickest route to appropriating a password (especially a shared one) can be via a phone call and a bluff.

**Don't disclose passwords** to anyone whose identity you can't verify, or whose right/need to know is in doubt. A good rule of thumb is that anyone who contacts you in order to ask for your credentials should be treated with suspicion. However convincing their story is, verify that they are who they say they are.

### **Changing your password regularly is important.**

- How frequently you change your password will depend upon how important the information you are protecting is
- Generally, once every three months is a really good idea. That way, by the time a computer has cracked a good strong password, you will have already changed it! One of the problems with multiple passwords is remembering them all.
- Tools are available to do this
- Just remember that you need to keep your “keysafe” application on a very safe computer, and back up the password file.

### **Trojans**

“A Trojan horse, or Trojan, in computing is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it.”

Trojan horses take many forms,

and many of them are intended to steal passwords and other sensitive data.

Treat any uninvited program with suspicion, from whatever apparent source.

=====End lecture 11 notes=====