Authentication & Passwords

Dr Tay Kian Boon

4062/3010

Main Objectives: Computer Security

There are 7 key concepts in the field of computer security:

1. Authentication
2. Authorization
3. Confidentiality
4. Data/message integrity
5. Accountability
6. Availability
7. Non-repudiation

Main Objectives: Computer Security

There are 7 key concepts in the field of computer security:

1. Authentication (identity -solved by eg 2FA)
2. Authorization (permission -solved by Access control list)
3. Confidentiality (secrecy contents -solved by encryption)
4. Data/message integrity (unmodified-solved by MAC-msg auth code)
5. Accountability (who is responsible -solved by log trail)
6. Availability (access –solved by adding redundancy)
7. Non-repudiation (undenialibility -solved by digital signatures)

Main Objectives: Computer Security

There are 7 key concepts in the field of computer security:

1. Authentication (identity -solved by eg 2FA)
2. Authorization (permission -solved by Access control list)
3. Confidentiality (secrecy contents -solved by encryption)
4. Data/message integrity (unmodified-solved by MAC-msg auth code)
5. Accountability (who is responsible -solved by log trail)
6. Availability (access –solved by adding redundancy)
7. Non-repudiation (undenialibility -solved by digital signatures)

AUTHENTICATION

- *Authentication* is the act of verifying someone's identity, AND ESPECIALLY IMPT IN NON-MTG SETTING

AUTHORITY

- *Authorization* is the act of checking whether a user has permission to conduct some action.

CONFIDENTIALITY

- The goal of *confidentiality* is to keep the contents of a transient communication or data on temporary or persistent storage secret.

MESSAGE/DATA INTEGRITY

- When Alice and Bob exchange messages, they do not want a third party such as Mallory to be able to modify the contents of their messages.

ACCOUNTABILITY

- The goal of accountability is to ensure that you are able to determine who the attacker or principal is in the case that something goes wrong or an erroneous transaction is identified.

AVAILABILITY

- An *available* system is one that can respond to its users' requests in a reasonable timeframe

Non-Repudiation

- The goal of *non-repudiation* is to ensure undenialibility of a transaction by any of the parties involved.

AUTHENTICATION

AUTHENTICATION

- When exploring authentication with Alice and Bob, the question we want to ask is:
- if Bob wants to communicate with Alice, how can he be sure that he is communicating with Alice and not someone trying to impersonate her?

AUTHENTICATION

- Bob may be able to authenticate and verify Alice's identity based on one or more of 3 types of methods:
  - something you know,
  - something you have, and
  - something you are.

Something You Know

Something You Know: Passwords

- The first general method Bob can use to authenticate Alice is to ask her for some secret only she should know, such as her secret password.
- If Alice produces the right password, then Bob can assume he is communicating with Alice.
- Passwords are so prevalently used that we will further study how to properly build a password management system.

Something You Know: Passwords

- There are advantages and disadvantages to using passwords.
- One advantage is that password schemes are simple to implement compared to other authentication mechanisms, such as biometrics, which we will discuss later.
- Another advantage of password security systems is that they are simple for users to understand.

Something You Know: Passwords

- There are, however, disadvantages to using password security systems.
- First, most users do not choose strong passwords, which are hard for attackers to guess.
- Users usually choose passwords that are simple concatenations of
  - common names,
  - common dictionary words,
  - common street names, or
  - other easy-to-guess terms or phrases.

How Hackers Crack Your Passwords

- They don’t go to the applications and try various combo of your passwords!
- They will commonly sniff & extract the “password hash” over the internet as you log in.
  - Normally systems uses common standard hash function
- They will write or use a password cracking program with dictionary of common passwords. They will crack Offline!
- They store password hashes in dictionaries.
- If your password hash appear in the dictionary, you are toast!

Something You Know: Passwords

- Attackers interested in hacking into somebody's account can use password-cracking programs to try many common login names and concatenations of common words as passwords.
- Such password cracking programs can easily determine 10 to 20 percent of the usernames and passwords in a system.
- Of course, to gain access to a system, an attacker typically needs only one valid username and password.
- Passwords are relatively easy to crack, unless users are somehow forced to choose passwords that are hard for such password-cracking programs to guess.

Something You Know: Passwords

- A second disadvantage of password security systems is that a user needs to reuse a password each time she logs into a system—that gives an attacker numerous opportunities to "listen in".
  - IMAGINE ONE FINE DAY A KEYLOGGR WAS INSTALLED INTO YOUR PC
- If the attacker can successfully "listen in" on a password just once, the attacker can then log in as the user.

Something You Know: Passwords

- A one-time password (OTP) system, which forces the user to enter a new password each time she logs in, eliminates the risks of using a password multiple times.
- With this system, the user is given a list of passwords—the first time she logs in, she is asked for the first password;
- The second time she logs in, she is asked the second password; and so on.
- The major problem with this system is that no user will be able to remember all these passwords.

Something You Know: Passwords

- However, a device could be used that keeps track of all the different passwords the user would need to use each time she logs in.

- This basic idea of such a device naturally leads us from the topic of "something you know" to the topic of "something you have."

Something You Have

Something You Have:

- A second general method of authenticating a user is based on something that the user has.
  - OTP Cards (one-time password)
  - Smart Cards
  - ATM Cards

Something You Have: OTP Cards

- OTP products generate a new password each time a user log in.
- One such product, by RSA Security, is the SecurID card
- The SecurID card is a device that flashes a new password to the user periodically (every 60 seconds or so).
- When the user wants to log into a computer system, he enters the number displayed on the card when prompted by the server.

Something You Have: OTP Cards

- Server knows the algorithm that the SecurID card uses to generate passwords, and can verify the password that the user enters.
- Other variations of OTP systems as well:
- For instance, some OTP systems generate passwords for their users only when a personal identification number (PIN) is entered.
- Also, while OTP systems traditionally required users to carry additional devices, they are sometimes now integrated into personal digital assistants (PDAs) and cell phones.

Something You Have: Smart Cards

- New Gen smart cards are tamper-resistant, which means that if a bad guy tries to open the card or gain access to the info stored on it, the card will self-destruct.
- Card will not self-destruct in a manner similar to what comes to mind when you think of *Mission Impossible*.
- Rather, the microprocessor, memory & other components that make up the "smart" part of the smart card are epoxied (or glued) together such that there is no easy way to take the card apart.

Something You Have: Smart Cards

- The only feasible way to communicate with the microprocessor is through its electronic interface.
- Smart cards were designed with the idea that the information stored in the card's memory would only be accessible through the microprocessor.
- A smart card's microprocessor runs software that can authenticate a user while guarding any secret information stored on the card.
- In a typical scenario, a user enters a smart card into a smart card reader, which contains a numeric keypad.

Something You Have: Smart Cards

- The smart card issues a “challenge” to the reader.
- The user is required to enter a PIN into the reader, and the reader computes a response to the challenge.
- If the smart card receives a correct response, the user is then considered authenticated, and access to use the secret information stored on the smart card is granted.
- One problem with using smart cards for authentication is that the smart card reader (into which the PIN is entered) must be trusted.

Something You Have: Smart Cards

- A rogue smart card reader that is installed by a bad guy can record a user's PIN, and if the bad guy can then gain possession of the smart card itself, he can authenticate himself to the smart card as if he were the user.

- While such an attack sounds as if it requires quite a bit of control on the part of the attacker, it is very feasible.

Something You Have: Smart Cards

- For example, an attacker could set up a kiosk that contains a rogue smart card reader in a public location, such as a shopping mall.
- The kiosk could encourage users to enter their smart cards and PINs by displaying an attractive message such as “Enter your smart card to receive a 50 percent discount on all products in this shopping mall!”
- Such types of attacks have occurred in practice.

Something You Have: Smart Cards

- Attacks against smart cards have also been engineered by experts such as Paul Kocher, Cryptography Research-(www.cryptography.com)
- By studying a smart card's power consumption as it conducted various operations, Kocher was able to determine the contents stored on the card.
- While such attacks are possible, they require a reasonable amount of expertise on the part of the attacker.
- However, over time, such attacks may become easier to carry out by an average attacker.

Something You Have: ATM Cards

- ATM card is another example of a security mechanism based on some secret the user has.
- On the back of an ATM card is a magnetic stripe that stores data—namely the user's account number.
- This data is used as part of the authentication process when a user wants to use the ATM.
- However, ATM cards are not tamper-resistant—anyone who has a magnetic stripe reader can access the info stored on the card, without need of any additional information, such as a PIN.

Something You Have: ATM Cards

- Not very difficult to make a copy of an ATM card onto a blank magnetic stripe card.
- Since the magnetic stripe on an ATM card is so easy to copy, credit card companies also sometimes incorporate holograms or other hard-to-copy elements on the cards themselves.
- However, it's unlikely that a cashier or point-of-sale device will actually check the authenticity of the hologram or other elements of the card.

Something You Are

Something You Are: Biometric

- The third general method of authenticating a user is based on something that the user *is*.
- Most of the authentication techniques that fall into this category are biometric techniques, in which something about the user's biology is measured.
- When considering a biometric authentication technique as part of your system, it is important to consider its effectiveness and social acceptability.

Something You Are: Biometric: 1. Palm Scan

- The first biometric authentication technique that we consider is a palm scan in which a reader measures the size of a person's hand and fingers, and the curves that exist on their palm and fingers.

- It also incorporates fingerprint scans on each of the fingers.

- In this way, the palm scan technique is much more effective than simply taking a single fingerprint of the user.

Something You Are: Biometric: 2. Iris Scan

- 2nd technique used: scan their iris.
- Here, a camera takes a picture of a person's iris and stores certain features about it in the system.
- Studies show iris scan more socially acceptable than the palm scan.
- In the palm scan technique, the user is required to actually put her hand on the reader for a few seconds, while in the iris scan, a camera just takes a quick picture of the user's iris.
- The iris scan is less intrusive since the user does not have to do anything except look in a particular direction.

Something You Are: Biometric: 3. Retina Scan

- Another biometric technique is a retinal scan, in which infrared light is shot into a user's eyes, and the pattern of retinal blood vessels is read to create a signature that is stored by a computer system.

- In a retinal scan, the user puts his head in front of a device, and then the device blows a puff of air and shoots a laser into the user's eye.

- A retinal scan is more intrusive than an iris scan or a palm scan.

Something You Are: Biometric: 4. Fingerprint

- In fingerprinting, the user places her finger onto a reader that scans the set of curves that makes up her fingerprint.
- Fingerprinting is not as socially accepted as other biometric identification techniques since people generally associate taking fingerprints with criminal activity.
- In addition, fingerprinting provides less information than a palm scan.

Something You Are: Biometric: 4. Voice

- Voice identification is a mechanism in which a computer asks a user to say a particular phrase.

- The computer system then takes the electrically coded signals of the user's voice, compares them to a databank of previous signals, and determines whether there is close enough of a match.

- Possible Problem?

Something You Are: Biometric: 4. Face

- Facial recognition involves a camera taking a picture of a person's face and a computer system trying to recognize its features.

Something You Are: Biometric: 5. Signature

- Another technique, signature dynamics, records not only a user's signature, but also the pressure and timing at which the user makes various curves and motions while writing.

- The advantage of signature dynamics over simple signature matching is that it is far more difficult to replicate.

Something You Are: Biometric: Disadvantages

- Key disadvantages to these biometric authentication techniques are
  - the number of false positives,
  - number of false negatives generated,
  - their varying social acceptance, and
  - key management issues.

Something You Are: Biometric: Disadvantages

- A *false negative* occurs when a user is indeed an authentic user of the system, but the biometric authentication device rejects the user.
- A *false positive* occurs when an impersonator successfully impersonates a user.
- Social acceptance is another issue to take into account when considering biometric authentication techniques.
- All the biometric authentication techniques discussed here are less socially accepted than entering a password.

Something You Are: Biometric: Disadvantages

- The final disadvantage for biometric authentication techniques is the key management issue.
- In each of these biometric authentication techniques, measurements of the user's biology are used to construct a key, a supposedly unique sequence of zeros and ones that corresponds only to a particular user.
- If an attacker is able to obtain a user's biological measurements, however, the attacker will be able to impersonate the user.
- For example, a criminal may able to "copy" a user's fingerprint by re-creating it with a wax imprint that the criminal puts on top of his finger.

Something You Are: Biometric: Disadvantages

- If you think of the user's fingerprint as a "key," then the key management issue in this case is that we cannot revoke the user's key because the user cannot get a new fingerprint—even though her original fingerprint has been stolen.
- By contrast, the keys in password systems are generated from passwords, and users can easily have their passwords changed if they are ever stolen or compromised.
- Biometric authentication becomes ineffective once attackers are able to impersonate biometric measurements.

Gummy and Conductive Silicone Rubber Fingers

— Importance of Vulnerability Analysis —

Tsutomu Matsumoto

Yokohama National University
Graduate School of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
tsutomu@mlab.jks.ynu.ac.jp

Matsumoto Fingerprint Paper-Asiacrypt2002

- Biometrics are utilized in individual authentication techniques which identify individuals by checking physiological or behavioral characteristics, such as fingerprints, faces, voice, iris patterns, signatures, etc.
- Biometric systems are said to be convenient because they need neither something to memorize such as passwords nor something to carry about such as ID tokens.
- In spite of that, a user of biometric systems would get into a dangerous situation when her/his biometric data are abused.
- For example, you cannot change your fingerprints while you can change your passwords or ID tokens when they are compromised.

*SECURITY ASSESSMENT OF BIOMETRIC user identification systems should be conducted not only for accuracy of authentication, but also for **security against fraud!***

-Matsumoto

Matsumoto Fingerprint Paper

- Therefore, biometric systems must protect the information for biometrics against abuse, and they must also prevent fake biometrics.

Fingerprints can be Cloned!

- “We have used the moulds, which we made by pressing our live fingers against them, or by processing fingerprint images from prints on glass surfaces, or by processing impression of inked fingers.
- We describe how to make the moulds, and then show that the gummy fingers and conductive silicone fingers which are made with these moulds, can fool the fingerprint devices.”

-Matsumoto

Final Notes on Authentication

Final Notes on Authentication

- Combining various authentication techniques Is more effective than using a single authentication technique.
- We have discussed some disadvantages of using biometric authentication alone.
- However, if you combine biometric authentication with another technique, such as a password or a token, then the authentication process becomes more effective.
- The term *two-factor authentication (2FA)* is used to describe the case in which a user is to be authenticated based upon two (independent) methods.
- ATM cards- another example of two-factor authentication at work.

Final Notes on Authentication

- ATM cards have magnetic stripes that have the user's name and account number.
- When the card is used, the user is required to enter not only the card into the teller machine, but also a PIN, which can basically be thought of as a password.
- In such an example of *2FA*, the bank requires the user to be authenticated based upon two methods—in this case, something that the user has and something that the user knows.

Final Notes on Authentication

- There are other factors that can be taken into account when conducting authentication. E.g. Alice's location.
- Alice may carry around a cellphone that has a GPS chip inside of it.
- When Alice stands in front of an ATM requesting to withdraw money, Alice's bank could ask her cellphone company's computer system where she currently is.
- If the cellphone company's computer responds with a latitude and longitude that corresponds to the expected location of the ATM, the bank can approve the withdrawal request.

Final Notes on Authentication

- However, if Alice's ATM card and PIN were stolen by a bad guy who is trying to withdraw money, then taking Alice's location (or specifically, the location of her cell phone) into account could help thwart such a fraudulent withdrawal request.

Final Notes on Authentication

- If Alice's cellphone is still with her, when an attacker attempts to use her card at an ATM, the location of the ATM will not correspond to the location of Alice's cell phone, and the bank will deny the withdrawal request (unless, of course, Alice and her cell phone are being held captive in front of the ATM).

- In this example, it is advantageous for Alice to keep her cellphone and her ATM card in different places; she should not, say, keep both of them in her purse.

Final Notes on Authentication: Internet

- In all the examples discussed so far, we have talked about people authenticating people or people authenticating themselves to computers.
- In Internet, computers are also interacting with other computers. The computers may have to authenticate themselves to each other because all computers cannot be trusted equally.
- There are many protocols that can be used to allow computer-to-computer authentication, and these protocols will, in general, support three types of authentication: client authentication, server authentication, and mutual authentication.

Final Notes on Authentication: Internet

- *Client authentication* involves the server verifying the client's identity,
- *Server authentication* involves the client verifying the server's identity, and
- *Mutual authentication* involves the client and server verifying each other's identity.
- TLS/SSL used in https support client, server, and mutual authentication over the internet.

Final Notes on Authentication: Internet

- Whether client, server, or mutual authentication is done often depends upon the nature of the application and the expected threats.

- Many e-commerce web sites provide server authentication once a user is ready to make a purchase because they do not want the client to submit a credit card number to a spoofed or impostor web site.

- Spoofed web sites are a significant security threat because they do not cost much to set up.

Final Notes on Authentication: Cellphone

- On the other hand, in older cell phone networks, only client authentication was required.
- Cell phone towers (servers) would only check that a phone (client) that attempted to communicate with it was owned by an authentic customer.
- The phones did not authenticate the cellphone towers because cell phone towers were costly to set up, and an attacker would require significant capital to spoof a cell phone tower.
- On the other hand, the cell phones themselves were much cheaper, and hence wireless carriers only required phones to be authenticated.
- Today, the cost of cell phone base stations is significantly cheaper, and modern-day cell phone networks use mutual authentication.