Security

Dr. Abdallah Mohamed

Acknowledgement: Original slides provided courtesy of Dr. Lawrence.

Key Points

1) Privacy involves ensuring personal information is used and distributed according to a person's wishes.

2) Security encompasses the various ways for ensuring privacy and protecting digital data.

3) Security includes user identification, access privileges, and protocols and encryption.

4) Encryption encodes text so that only the intended receiver can understand it.

Privacy

Privacy is the right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.

Information technology threatens privacy due to the ease of storing, copying, and exchanging digital information that is collected from a variety of sources (government, business, etc.).

As users of services, we are often forced or must "voluntary disclose", private information that we trust the organizations will keep secure and not distribute.

Although there are numerous rules and regulations for privacy, they are **not consistent** across all countries and **cannot always be rigorously enforced.**

Privacy: Whose Information Is It?

An interesting question about privacy relates to who "owns" information in a transaction or exchange.

For instance, when you **buy groceries**, does the grocery store have the right to the information about what you purchased?

- This is **valuable information** to the merchant as they can spot trends that help in marketing and inventory management.

Beware: If you have any sort of **membership card**, your purchase information can be maintained across visits to get a profile of your purchases.

- Merchants can also use your credit or debit card information.
- Most organizations now must disclose how they will use the information and give you the **right to "opt out".**

A Privacy Success Story So Long Tele-marketers!

Before: The telemarketing industry's "self-policing" mechanism required individuals to write a letter or make an on-line payment to **stop telemarketing calls**. Individuals received numerous, unwanted calls.

Solution: The United States government set up the **Do-Not-Call** List. Anyone on the list cannot be called by a tele-marketer without incurring a fine.

Result: There are over 80,000,000 households on the list and the telemarketing industry has largely collapsed.

In Canada: The government has passed legislation creating a Do-Not-Call list similar to the United States.

- https://www.lnnte-dncl.gc.ca

Privacy on the Internet

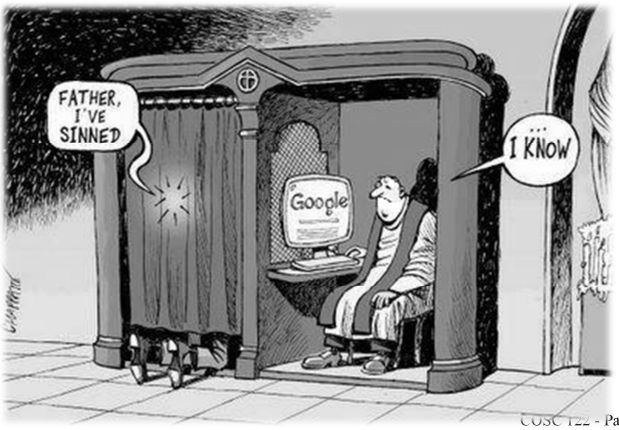
The Internet is ***not*** **an anonymous** communication system.

- **User ids, cookies, and IP addresses** can be used to track communications and interactions.
- Any **interaction** with a web site can be **logged and recorded**.
- **Email** travels (and may be logged) by numerous servers.

Privacy can only be guarded with adequate security and knowledge.

You must assume that anything you do on the web will become public.

Privacy on the Internet



Privacy Breaker: The Cookie

A ***cookie*** is a small file stored on your computer by your browser by a web site that you visit.

A cookie file allows **a site to identify you** between visits by storing information such as your user id.

Cookies can be **abused by advertisers** who store them on your computer whenever you visit a site they have ads on. They can then use the user id in your cookie to detect when you visit other sites that they provide advertising for.

Browsers now give you the option of **disabling cookies** on a per site, individual request, or overall basis.

Your Digital Footprints

Your **Internet activities are recorded** in a variety of places which results in a large digital footprint:

- **Browsers store**: Browsing history and cache, form data, cookies, etc.
  - ⇨Learn how to delete them or use Incognito mode or Anonymizer.
- **ISP stores**: Some traffic information, bandwidth usage, potentially logs of sites visited
- **Cellphone companies store**: History of calls, cell phone towers used, call detail records, text message content/detail, and IP information. Some of this information is stored for over a year and is available without a warrant.

Identity Theft

Identity theft is the crime of posing as someone else for fraudulent purposes.

It is too easy to **get personal information** for others:

- from **spam** email or bogus web sites
- from **security breaches** in registered databases
- from **accidental release** on the Internet
- from **paper records** including discarded documents

Identity theft is a growing problem because most **financial transactions** are entirely automatic. Once you have the key identifying fields for a person, ***a system assumes you are that person*** and **no manual verification is performed**.

Protecting Your Identity

It may sound paranoid, but in today's digital society, your identity is your most important asset and must be protected:

- Ensure your **computer security** including anti-virus and software is up-to-date.
- Only use **trusted software**, **email**, and **web services**.
- Be wary of **scams** that are "**Too good to be true**!"
- Chose **strong passwords** and keep them safe.
- **Shred documents** that contain personal and financial data.
- **Do not trust** an organization or person unless you have evidence that you should do so.

Identify Theft

Question: Do you know any one who has been a victim of identify theft?

A) I have been a victim

B) A member of my family has been a victim.

C) A friend has been a victim.

D) Someone I know has been a victim.

E) I do not know someone who has been a victim of identify theft.

Security

Security is the act of keeping precious data safe and only **accessible to the correct people**.

- Security is a way of enforcing privacy in digital systems.

There are many different security technologies. In general, security involves several things:

(1) User identification - verify system user is who they say they are

(2) Access privileges - only allow user to access data they have the privilege (or right) to access or update.

(3) Security or encryption protocol - stores or transmits data in such a way that only users with the correct access privileges can use it.

(1) *User Identification*

A system performs ***user identification*** to determine if the user is who they claim to be.

Technologies for user identification:

- **User id and a password**
  - **The most common form** of user identification.
  - An ***authentication system*** is used to verify the user id and password is correct.
- **Biometrics** - finger printing, voice recognition, eye scans
- **Digital access cards** and keys

Creating Good Passwords

Your password is your only form of defense against other users accessing your data and private information.

- It is crucial to select a good one because **there are techniques to "crack" passwords**, especially weak ones.

Cracking passwords:

- **Directed guessing** - use common words, names, birth dates, and other information known about the user.
- **Brute force** - try all possible character sequences to find the password (usually limited by denying access after a while)

Good passwords have **at least 6 characters** with a mixture of upper and lower case letters, numbers, and punctuation.

- It should not contain components of dictionary words or personal information.

Changing Passwords

Passwords should be changed periodically.

Although managing passwords for many different systems is cumbersome, **using a single password for everything is risky**.

A good idea is to recycle passwords by rotating through a few or making slight changes to existing ones.

Question: Why can the administrator not tell me my forgotten password?

- Answer: Passwords are encrypted when stored on the computer to prevent the administrator (and others) from knowing it.
- Administrators are only allowed to reset a password.

Password

Question: Do you have at least one bad password (a name, a birth date, a student ID, etc) for an important computer system that you use?

A) Yes

B) No

(2) *Access Privileges*

Access privileges limit access to data and software functions based on the rights assigned to the user.

The ***access control system*** verifies a user has access to the given resource before allowing them to use it.

On shared machines, your user id provides you access to some files and programs. However, you cannot typically access the files and directories of other users unless they allow you to.

Three common access privileges:

- ***read*** - can read file contents
- ***write*** - can update file contents or delete entire file
- ***execute*** - can run a program or enter a directory

These access privileges may be specified on a **per user** basis, to ***groups*** of users, or to all users (**public**).

(3) *Encryption And Decryption*

An ***encryption system (protocol)*** converts data into a form that cannot be understood by anyone but the intended user.

- ***Encryption*** transforms a data representation so it is no longer understandable to users without the decryption key.
- ***Decryption*** converts an encrypted data representation into its original form, usually using a key or private information.

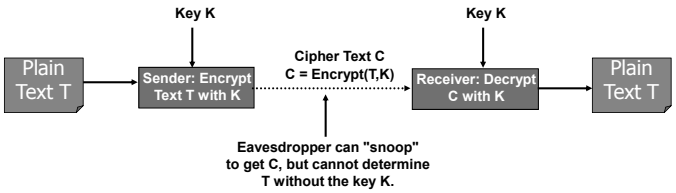
Cleartext or ***plaintext*** is the information before encryption.

Cipher text is the information in encrypted form.

A ***cryptosystem*** is a combination of encryption and decryption methods.

A ***one-way cipher*** is an encryption system that cannot be easily reversed (used for passwords).

Cryptosystem Diagram Sender to Receiver



Caesar Cipher

The ***Caesar cipher*** was used by Julius Caesar to encrypt messages sent to his generals.

- Encryption Algorithm: Shift each letter over K places, wrapping around to the start of the alphabet as necessary.
- Decryption Algorithm: Go back K letter places in the alphabet, wrapping as necessary.

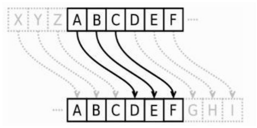
Example (K=3):

- `Plain text  =` **`ABCDEFGHIJKLMNOPQRSTUVWXYZ`**
- `Cipher text =` **`DEFGHIJKLMNOPQRSTUVWXYZABC`**

Example (K=3):

- Plain text = `HELLO WORLD.`
- Cipher text = `KHOOR ZRUOG.`

Question: Pick a partner and exchange a short encrypted message (then decrypt).



Security Caesar Cipher

Question: Decrypt the following Caesar cipher message:

SLFN D

A) PICK A

B) VOIQ G

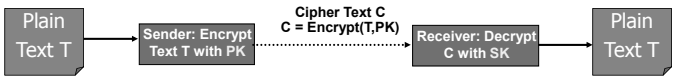
C) PICK G

D) PICK D

Public Key Cryptosystems

Public key cryptosystems use two keys: one public (PK) and one private (SK). The keys are designed so that senders can send a message encrypted using the public key and only the receiver (who made the keys) can decrypt the message.

Diagram:



RSA Public Key Cryptosystem Selecting a Key

The RSA public key cryptosystem relies on prime numbers.

Any number can be factored into primes in only one way.

A key is chosen with special properties such as:

- Must be the product of two different prime numbers p and q.
- p and q must be about 64 or 65 digits long to produce a 129-digit public key.

If *p* and *q* are kept secret, the code cannot be cracked.

- If the key is large enough, factoring to find *p* and *q* can't be done in any reasonable amount of time even by software.

System Backup

A ***system backup*** is a copy of valuable data and software that is used to **restore a failed system.**

Performing regular system backups is important, even for personal data, that may get lost due to system and natural disasters.

Mission-critical data is frequently backed up to multiple different sites to handle major natural disasters.

System redundancy is a good thing to insure the system continues to operate properly. Redundancy can be in the form of software backups or hardware components (multiple drives).

Backing Up a Personal Computer

What to backup:

- All personal data including documents, pictures, and music.
- Software settings such as Internet favorites.
- Do not backup operating system or programs as they can be re-installed from source CDs.

How to backup:

- **Simple**: Use a duplicate device such as a USB key or extra hard drive and copy files to it periodically.
- **Offsite**: Burn a CD or DVD with files and store in another place.
- **Online**: Use cloud services (DropBox, Google).
- **Sophisticated**: Install and configure backup software that regularly saves data to another drive or CD/DVD.

Backup

Question: The last time I backed up the important files on my computer or laptop was…

A) Last week
B) Last month
C) Last semester
D) Last year
E) Never … do you mean the computer can lose my files?

Conclusion

Preserving our ***privacy*** is especially important in our digital world because of the amount of information collected and the simplicity that it can be exchanged.

Security protocols and systems are designed to restrict access to systems and data to the appropriate individuals.

- Security involves user identification (authentication system), access privileges (access control system), and encryption.
- We must use good passwords to protect our privacy.

Various encryption protocols provide data security. RSA public encryption is a strong encryption scheme.

We must backup our data and system in addition to securing it.

Objectives

- Discuss some issues with maintaining privacy in a digital world.
- Define cookie and explain how it can invade your privacy.
- Define identity theft and list some precautions to avoid it.
- Define security and list three components of security.
- Define: user identification, access privilege, authentication system, access control system
- Define: encryption system, encrypt, decrypt, plain text, cipher text, cryptosystem, one-way cipher
- Draw a diagram and explain how encryption/decryption works.
- Be able to encode and decode a Caesar cipher.
- Explain the key idea of public (RSA) key encryption.
- Define: system backup, redundancy