Applications of Information and Communication Technologies (AICT)

(CSC – 107)

Dr. Rizwan A Khan


CyberSecurity
Security & Privacy

1. Privacy

- **Privacy** : Keeping your data secure or not allowing to be seen by un wanted person.

- Some of the devices that we use daily are vulnerable (unsecure) and have our private **data**:
  - Laptops
  - Desktops
  - Phones
  - .

- Data is a collection of files and are of course just 0s and 1s

1. Privacy : Data

- What kind of files do we have on our devices:
  - Images (vacations, home, office, friends ….)
  - Videos (home function, entertainment …)
  - Financial documents
  - Academic documents
  - Audio files
  - .

1. Privacy : Deleting files (vulnerabilities in files)

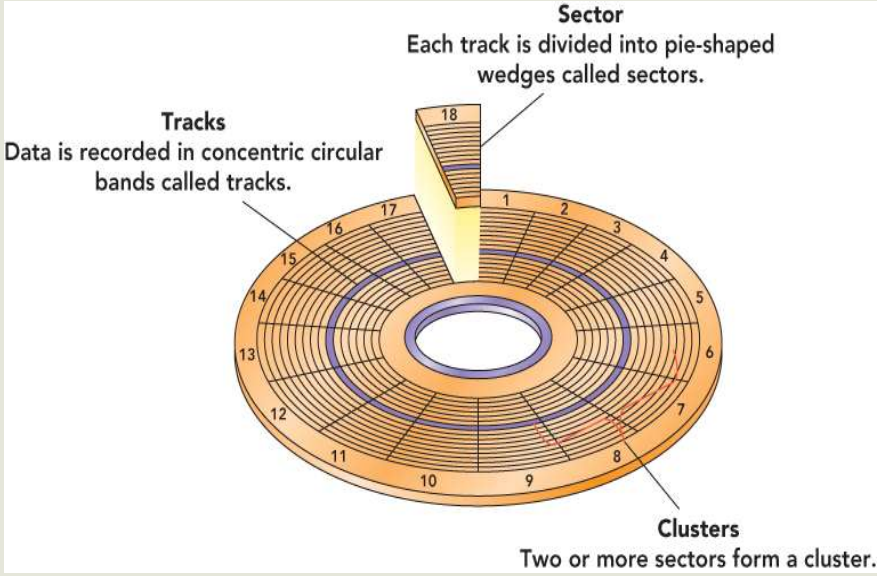
- You are cautious about data and anything that is not required you delete it.

- What happens when data is deleted?
  - Files are stored on HDD or SSD
  - They disappear once file is deleted
  - Where those 1s and 0s are gone?
  - Is there any mechanism to wipe them out from physical device?

1. Privacy : Deleting files (vulnerabilities in files)

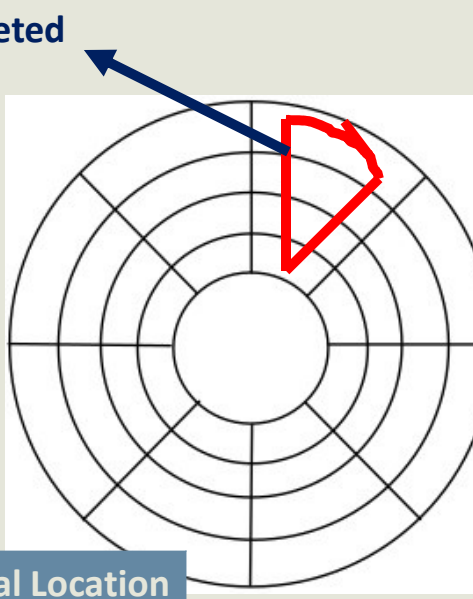
- **Operating system** keeps track of data being stored on physical media.
- It records file address (location / lookup table)

File name	Physical Location (byte number)
myImage.jpg	123
myDocument.doc	890
…	…
…	…



1. Privacy : Deleting files (vulnerabilities in files)

- What is it mean to delete file?
- Graphically file disappears.
- It may goes to trash can / bin. But file can be retrieved from bin.
- Ok you clear bin as well. What happens to those 1s and 0s?
- It turns out OS does nothing to file on physical media, it just deletes entry in location table
  - Data is not destroyed on physical disk



File name	Physical Location (byte number)
~~myImage.jpg~~	~~123~~
myDocument.doc	890
…	…
…	…

1. Privacy : Deleting files (vulnerabilities in files)

- 1s and 0s are still on physical media, till it gets over written by some other data pattern.

- If there is some adversary with right software, data (theoretically) can still be recovered from HDD / SSD.

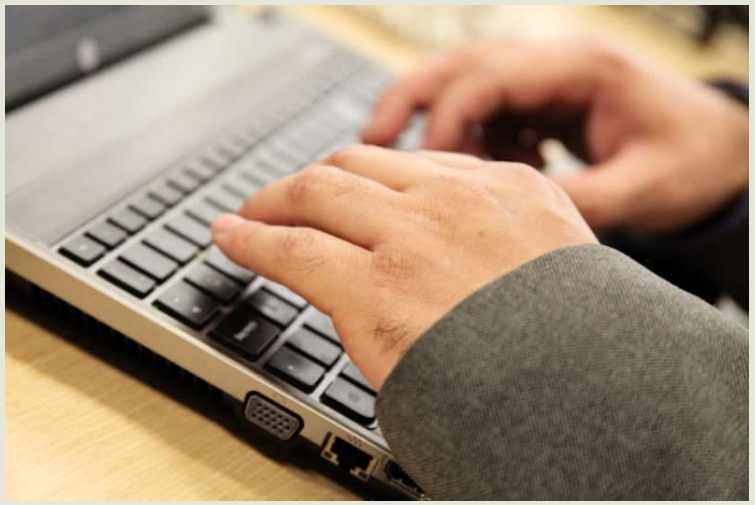
- What are **benefits and draw backs** of just forgetting entry in location table:
  - Can recover accidently deleted files. **(benefit)**
  - Its speed efficient to just delete entry from location / lookup table rather than wiping out data from each location of physical media. **(benefit)**
  - Adversary can recover private data. **(drawback)**

Internet Security

2. Vulnerabilities in browsing internet

- Internet users spend an average of **2 hours and 22 minutes** per day only on social networking in 2019[1]. And now?

- Time spent on internet surfing: **6 hours 49 minutes**[2]



- We use browsers for surfing:
  - Chrome
  - Edge
  - Firefox
  - Safari
  - .

1 Review42
2 Thenextweb.com

2. Vulnerabilities in browsing internet

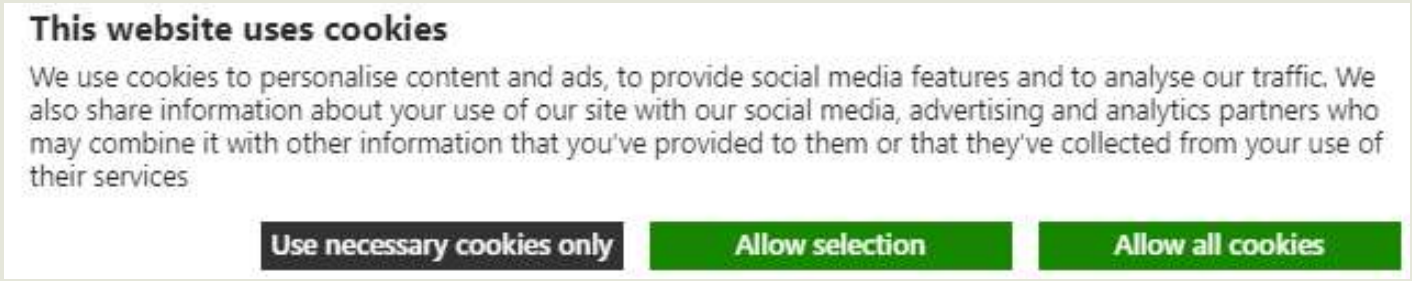
- All recent web browser uses **COOKIES**

- **Cookies** are text files with small pieces of data like
  - username
  - Password

- **HTTP cookies** are used to identify specific users and improve web browsing experience. No need to enter same information again and again.
  - **Example:** logging in Gmail account, social media accounts etc.

2.1 Cookies

- Web server puts these cookies on computers after user **authenticates** (more on this later) him/her self on that server.



- That cookie usually doesn't contain username or password, instead it just contains big random number.
- When returned to that server again, the browser presents that cookie to remind specific user(no need to enter my name, email ID, password, etc.).

2.1 Cookies : HTTP header

- Data stored in a cookie is created by the server upon connection. This data is labeled with an ID unique for specific user.

```
HTTP/1.1 200 OK
Set-Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

  - HTTP 200 OK → all is ok
  - Cookie → key : value (pair)

- Big random number **uniquely identifies specific user.** The same **number will never be sent** to another user.

2.1 Cookies : HTTP header

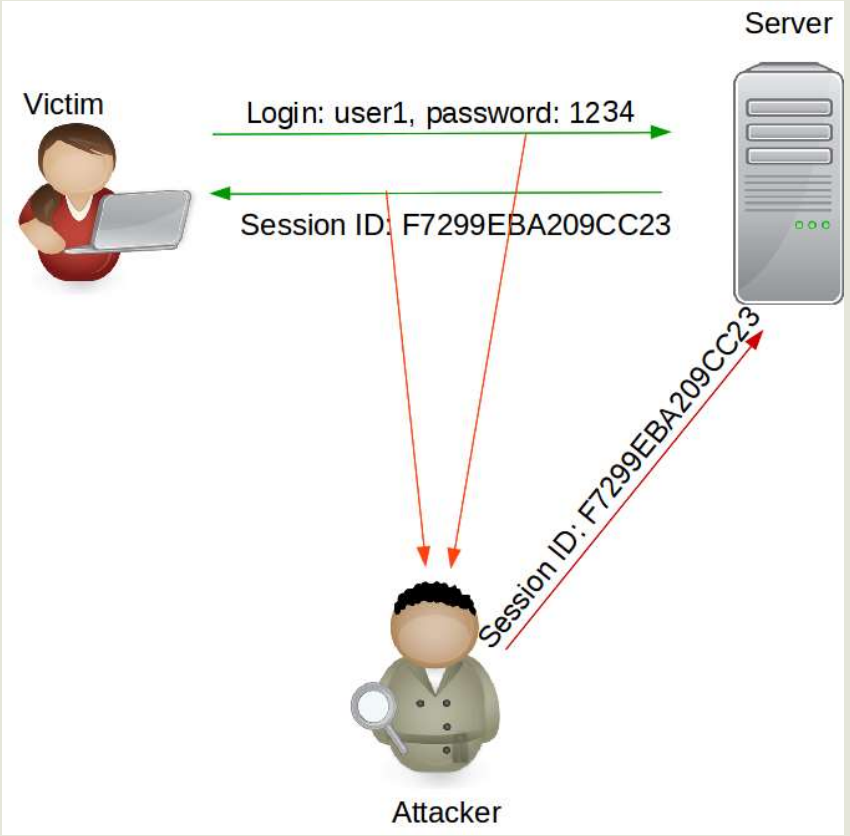
- Browser on every subsequent webpage visit on “example.com” will sent something like this (HTTP header):

```
GET / HTTP/1.1
Host: example.com
Cookie: session=29823bf3-075a-433a-8754-707d05c418ab
```

- **Is Cookie statement same as shown previously?**
- **Previously, it was** `Set-Cookie:`
- **Set-Cookie → sent by server to browser**

2.1 Cookies : session hijacking

- **Are cookies presenting threat to privacy?**
- **Consider:** Data is being communicated via wired or wireless medium and an adversary / hacker can sniff packets. What if an adversary sees this information?
  - In this situation, hacker can impersonate specific user by duplicating cookie value and can get access to private data (Gmail, Facebook, Outlook, etc.)
  - This is called **session hijacking attack**
  - **How to protect against such attack?**



2.1 Cookies : Session hijacking attack

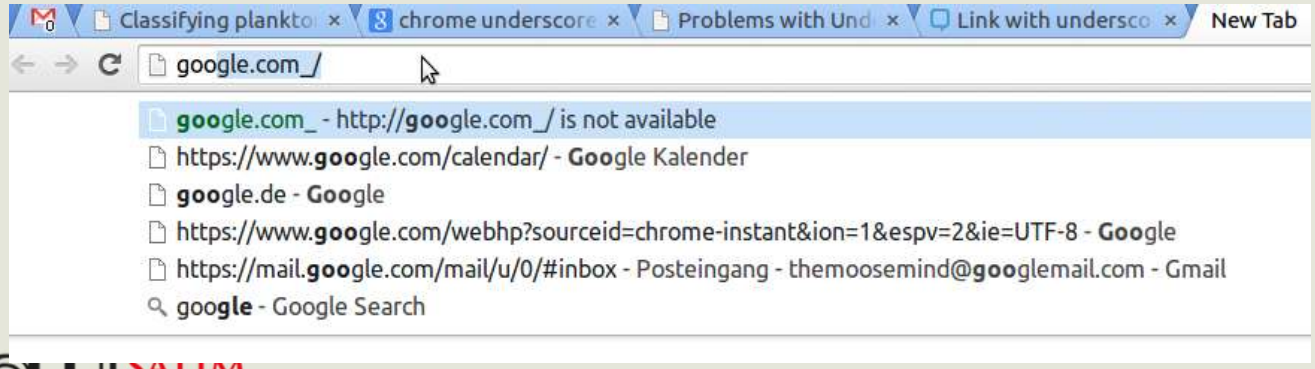
- **How to protect against session hijacking attack?**

1. **Delete cookies** (implications – browsing experience? Delete cookies from physical media?)
2. Usually most websites these days **encrypt** this information.

"Encryption is the method by which information is converted into secret code that hides the information's true meaning"

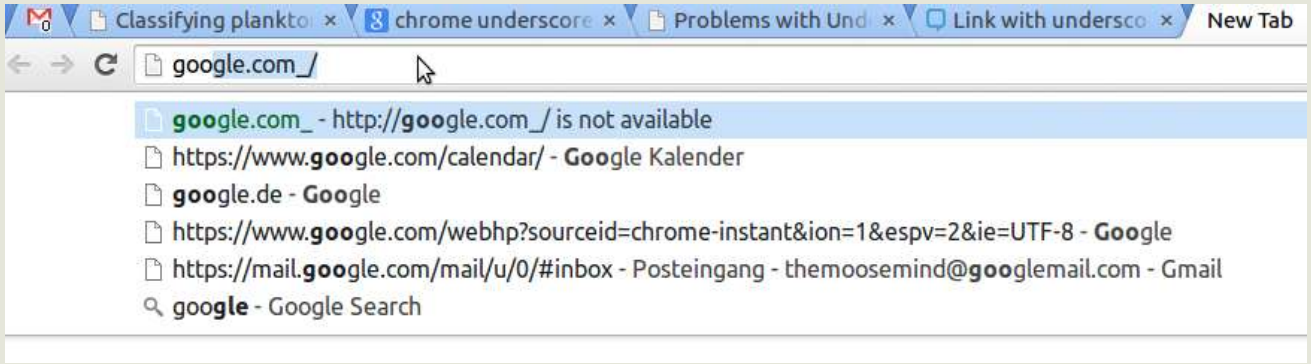
2.2 Browsing history

- Another threat to privacy while browsing internet is stored **browsing history**
- Browsers are powerful, they do keep track of online activities. They are beneficial as:
  - User doesn't need to keep typing same address
  - Type first few letters to search website that has the useful content (don't need to search again)
  - Search browsing history to find webpage that has required information



2.2 Browsing history

- Another threat to privacy while browsing internet is stored **browsing history**
- Apart from benefits, they present privacy threat as well, as:
  - Some individual, if get a chance, can see online activities
  - Visible search history with date and time information

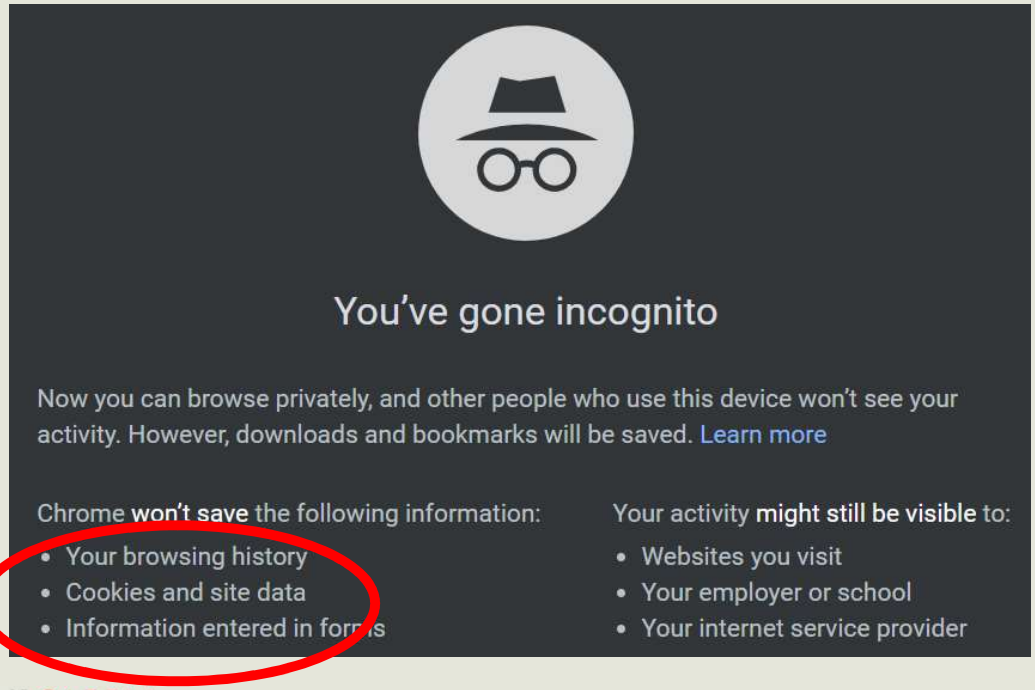


2.2 Clearing browsing history

- Usually with **clearing browsing history, cookies are also deleted**.
- **Upside:**
  - Some individual, if get a chance, can't see online activities of other user.
  - Search history deleted.
  - Adversary can't get hold of session of authenticated user.
- **Downside:**
  - User need to login again to any website that was ever logged in (annoying browsing experience).
  - Need to type complete webpage addresses (annoying browsing experience).
  - Can't search information within browsed pages.

2.3 Private browsing

- Any alternative for not deleting cookies?
- Most of the web browser have private mode or incognito mode



2.3 Private browsing

- Incognito mode automatically deletes history and cookies without effecting what previously has been stored in browser i.e. cookies, browsing history etc.

- This mode is also used by tech people when they need to see current webpage as it ensures not to take information from browsing history (forgets history) and displays information from current process.