CHAPTER 2

ORAGNIZATIONAL SECURITY

Organizational Security syllabus

2.1 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non-employees.

2.2 People as Security Tool: Security awareness, and Individual user responsibilities.

2.3 Physical security: Access controls

Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers

2.4 Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.

2.1 PASSWORD SELECTION

- Guidelines on to how-to make a strong password.
- **Steps:**

➢ Take appropriate length password .

➢ Form a "random" sequence of words , letters or ,numbers .

➢ Add numbers to the base-word to make it more secure.

➢ Use punctuation and symbols to "complicate“ it further.

➢ Create complexity with upper and lowercase letters.

➢ Generate similar but altered passwords

2.1 PASSWORD SELECTION

- Change your passwords periodically or whenever it may have become compromised.
- Don't re-use an expired password.
- Try to memorize the password, and avoid writing it down..
- Do not tell anybody your password.

Piggybacking

- Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.
- Piggybacking is sometimes referred to as **"Wi-Fi squatting**
- The usual **purpose** of piggybacking is simply **to gain free network access** rather than any malicious intent, but it can slow down data transfer for legal users of the network

CONTD…

- To protect your network from piggybacking, ensure that encryption is enabled for your router.
- Use Wireless Encryption Protocol (**WEP**), if possible use Wireless Protected Access (**WPA**) or WPA2

2.1 Shoulder Surfing

- A term used to describe a person that looks over another person's shoulder as they enter data into a computer or other device
- Criminals often use used this technique to gain access to your personal accounts or read personal information, such as e-mails

2.1 Dumpster diving

- In IT, dumpster diving refers to using various methods to get information about a technology user
- In general, dumpster diving involves **searching through trash or garbage looking** for something useful. This is often done to uncover useful information that may help an individual get access to a particular network

2.2 PEOPLE AS SECURITY TOOL

- Security awareness , and Individual user responsibilities
- Security awareness:
- Security attention is the knowledge and mindset contributors of an organization possess regarding the protection of the physical, and specifically informational, property of that company
- Being protection conscious method you understand that there may be the ability for some human beings to intentionally or by accident scouse borrow, damage, or misuse the statistics that is stored within a enterprise's computer systems and at some point of its employer.

2.3 PHYSICAL SECURITY: ACCESS CONTROL

- ❑ Originally, access control usually refereed to restricting physical access to a facility, building or room to authorized persons. This used to be enforced mainly through a physical security guard.
- ❑ Then, with the advent of electronic devices, access control has evolved into the use of physical card access systems of a wide variety including biometric activated devices

2.3 PHYSICAL SECURITY: ACCESS CONTROL

- ❑ Originally, access control usually refereed to restricting physical access to a facility, building or room to authorized persons. This used to be enforced mainly through a physical security guard.
- ❑ Then, with the advent of electronic devices, access control has evolved into the use of physical card access systems of a wide variety including biometric activated devices
- ❑ Physical safety is in the main concerned with restricting physical access via unauthorized humans (normally interpreted as intruders)

Biometric

- ❑ Each person has a set of unique characteristics that can be used for authentication
- ❑ Today’s Biometric systems examine retina patterns, fingerprints, handprints, voice patterns, keystroke patterns etc for authentication

Retina pattern Biometric system

- Retina scanners use the blood vessels inside the back of the eye for authentication. The blood vessel pattern inside the returned of the attention is unique to the man or woman. This method could be very intrusive and isn't widely accepted because it breaches someone's medical privateness. For example, possible discovery of disorder in the eye or other clinical situations may additionally alert the corporation and can purpose employment issues.)

Fingerprint pattern Biometric system

- Fingerprint scanners are the least intrusive out of the institution because they simplest measure the fingerprint. They degree the whorl, loop, and arch styles of the finger, that are unique to anybody. Fingerprint scanners also are the perfect to enforce and are value effective. Fingerprint scanners do now not expose any medical statistics; consequently, they may be broadly used within the enterprise with regard to get entry to manage.

Voice pattern Biometric system

- Voice authentication is a biometric approach of speaker reputation based on measuring the distinctions in individual voices to uniquely discover customers. Instead of a password, which might be forgotten or not robust enough to make sure security, voice authentication allows human beings to use their voices themselves as passwords

Keystroke Biometric System

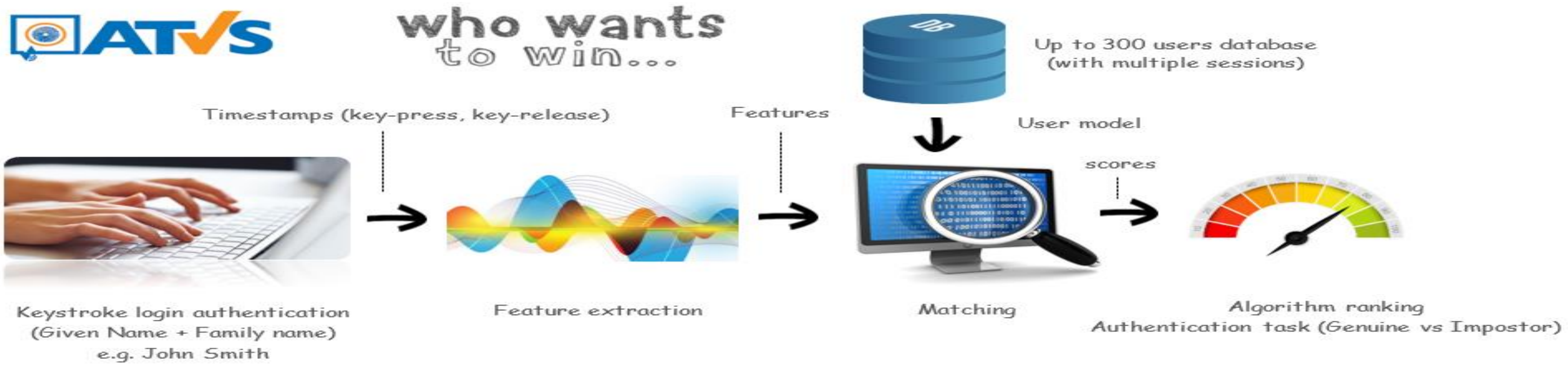
❑ Keystroke recognition has been described by way of both industry and academics because the method of measuring and assessing a typing rhythm on virtual devices, along with on: laptop keyboards, mobile phones, and touch display panels.

- The 3 most widely used features for keystroke dynamics are:
- Hold time – time between press and release of a key.
- Keydown-Keydown time – time between the pressing of consecutive keys.
- Keyup-Keydown time – time between the release of one key and the press of next key.

CONTD…

- A noted typing measurement, keystroke recognition, often called “keystroke dynamics”, refers to the detailed timing information that describes exactly when each key was pressed on a digital device and when it was released as a person types. Though biometrics tend to rely on physical traits like fingerprint and face or behavioural characteristics, many consider keystroke dynamics a biometric.[3]

CONTD ……



ATVS

who wants to win...

Up to 300 users database (with multiple sessions)

Timestamps (key-press, key-release)

Features

User model

scores

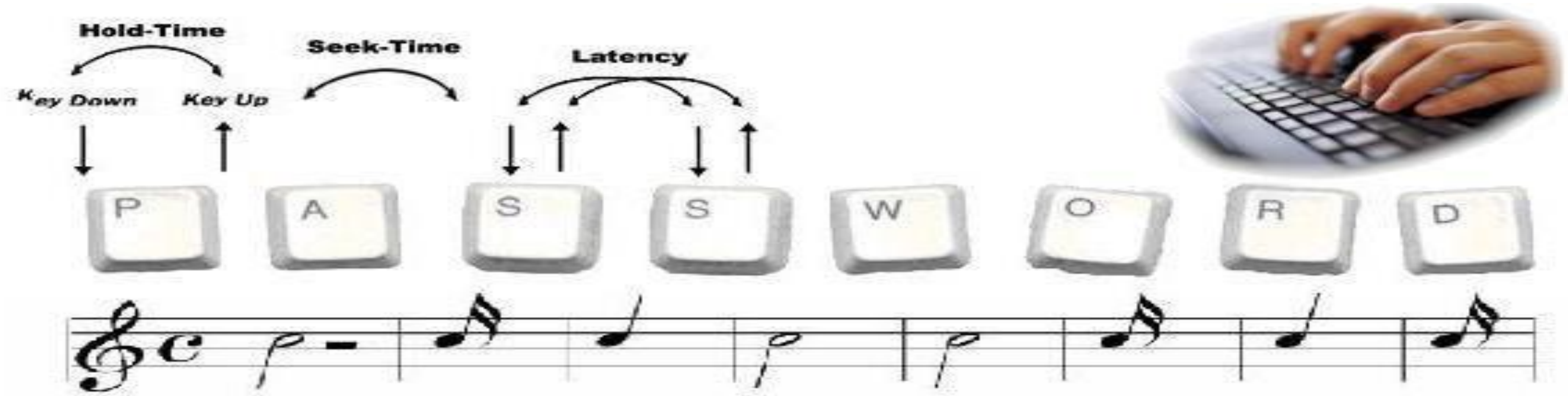
Keystroke login authentication (Given Name + Family name) e.g. John Smith

Feature extraction

Matching

Algorithm ranking

Authentication task (Genuine vs Impostor)



COMPONENTS OF A GOOD PASSWORD

- Common suggestions to make the password more tough to guess or gain are as follows:

❑ It must be at least 8 characters long.

❑ It should include uppercase and lowercase letters, numbers, unique characters or punctuation marks.

❑ It must no longer contain dictionary phrases.

COMPONENTS OF A GOOD PASSWORD

❑ It need to now not comprise the user's private statistics consisting of their name, family member's name, birth date, pet name, phone number or any other detail that can easily be identified It should not be similar to the person's login name.

❑ It ought to no longer be the default passwords as supplied by using the device dealer such as password, guest, admin and so on.

LINKS :

1. https://www.youtube.com/watch?v=30Jy4JBDanI
2. https://www.youtube.com/watch?v=Xs8IAvk1khY
3. https://www.umsl.edu/technology/security/passwords.html