# İTÜ
# Computer Security

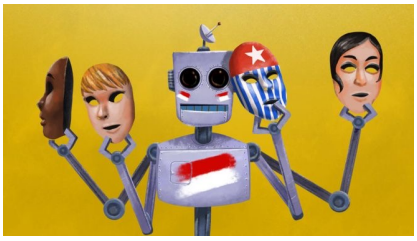
## User Authentication

Dr. Şerif Bahtiyar

1

## Before Starting

Papua unrest: Social media bots 'skewing the narrative'



Indonesia's Papua province has become the focus of a well-funded social media campaign using bots to promote a pro-government agenda

https://www.bbc.com/news/world-asia-49883667



2

## Before Starting

Could a hacker hijack your connected car?

In 2015, 15% of car recalls in the US were related to software errors, up from 5% four years before.

Hackers showed two years ago that they could remotely take control of a Chrysler Jeep.

http://www.bbc.com/news/business-41367214



3

## Before Starting

İstanbul Üniversitesi'nde not skandalı!

İstanbul Üniversitesi Hukuk Fakültesi'nde 8 öğrencinin notlarını sisteme izinsiz girip, yükselten iki personel hakkında dava açıldı

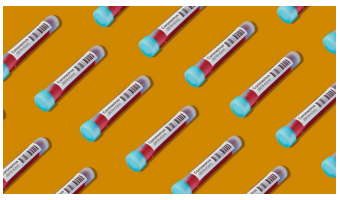
http://www.hurriyet.com.tr/istanbul-universitesinde-not-skandali-ihbar-mektubuyla-ortaya-cikti-40606472



4

## Before Starting

Coronavirus: North Korea and Russia hackers 'targeting vaccine'



State-backed hackers from North Korea and Russia have been targeting organisations working on a coronavirus vaccine, Microsoft has said.

https://www.bbc.com/news/technology-54936886



5

## Before Starting

US announces 'strongest global action yet' on AI safety


The White House has announced what it is calling "the most significant actions ever taken by any government to advance the field of AI safety".

https://www.bbc.com/news/technology-67261284



6

# Outline

- Basics of Authentication
- Password-Based Authentication
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- CAPTCHA
- Some Attacks on Authentication Systems



7

## Basics of Authentication

Authentication is the binding of an identity to a principal.

- Message authentication is a procedure that allows communicating parties to verify that received or stored messages are authentic.
- User authentication is the process of verifying an identity claimed by or for a system entity. (RFC2828)



8

## Basics of Authentication

User authentication is the fundamental building block and the primary line of defense.

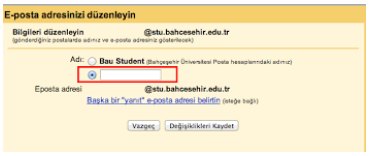
Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic from a particular client until that client has correctly supplied a valid username and password. (Cisco)



9

## Basics of Authentication

Electronic User Authentication is the process of establishing confidence in user identities that are presented electronically to an information system. *(NIST SP 800-63-2: Electronic Authentication Guideline)*




Digital Authentication or **E-Authentication** may be used synonymously when referring to the authentication process that confirms or certifies a person's identity and works.



10

## Basics of Authentication

User authentication is the basis for many types of access control and user accountability.

Steps of an authentication process:

- Identification: specify identifier

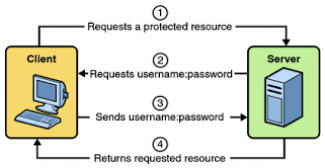

- Verification: bind the entity and the identifier



11

## Basics of Authentication

- Subscriber or Claimant: The party to be authenticated.
- Verifier: The party verifying the identity of a subscriber.



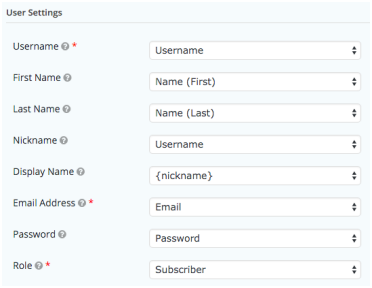

- Credential: A data structure that authoritatively binds identity and additional attributes to a token possessed by a subscriber that can be verified by the verifier in an authentication transaction.
- Token: can be an encryption key or an encrypted password that identifies the subscriber.



12

## Basics of Authentication

The initial requirement of user authentication is registration.






13

## Basics of Authentication

Risk Assessment

Risk assessment is related to

- Assurance level: describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity.
- Potential impact: defines the level of impact where there is a breach of security FIPS 199. (here failure of authentication)
- Areas of risk: the mapping between the potential impact and the appropriate level of assurance that is satisfactory to deal with the potential impact.

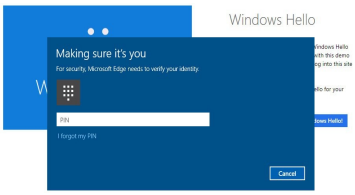


14

## Basics of Authentication

Four (five) factors of user authentication based on individual:

1- Knows: password, PIN







15

## Basics of Authentication

Four (five) factors of user authentication based on individual:

2-Possesses (token): electronic keycards, smart cards, physical keys



16

## Basics of Authentication

Four (five) factors of user authentication based on individual:

3-Is (static biometrics): fingerprint, retina, face

4-Does (dynamic biometrics): voice pattern, handwriting characteristic

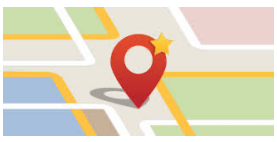


17

## Basics of Authentication

Four (five) factors of user authentication based on individual:

5-Location



Each of these methods has problems.



18

## Password Based Authentication

- Widely used user authentication method
  - User provides name and password
  - System compares name and password
- Authenticate identifier (ID) of user logging
  - User is authorized to access system
  - Determines user's privileges






19

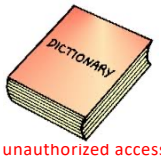
## Password Based Authentication

Vulnerabilities of passwords and countermeasures

Password cracking software: Aircrack, Hydra, … (Do not use for MALICIOUS purpose!)

Offline dictionary attack

A guessing attack which uses precompiled list of options. It does not try every option, only tries complete options which are likely to work.




Countermeasure: Prevent unauthorized access to the password file, IDS measures



20

## Password Based Authentication

Vulnerabilities of passwords and countermeasures

Specific account attack

The attacker targets a specific account and submits password guesses until the correct password is discovered.


Countermeasure: Apply account lockout mechanism



21

## Password Based Authentication

Vulnerabilities of passwords and countermeasures

- Popular password attack – policies, scanning IP address and cookies
- Password guessing against single user – training and enforcement of policies

**TOP 20 MOST COMMON PASSWORDS**
*(as a percentage of all passwords)*

| | | | | | |
|---|---|---|---|---|---|
| 1. | 123456 | 4.1% | 11. | login | 0.2% |
| 2. | password | 1.3% | 12. | welcome | 0.2% |
| 3. | 12345 | 0.8% | 13. | loveme | 0.2% |
| 4. | 1234 | 0.6% | 14. | hottie | 0.2% |
| 5. | football | 0.3% | 15. | abc123 | 0.2% |
| 6. | qwerty | 0.3% | 16. | 121212 | 0.2% |
| 7. | 1234567890 | 0.3% | 17. | 123654789 | 0.2% |
| 8. | 1234567 | 0.3% | 18. | flower | 0.2% |
| 9. | princess | 0.3% | 19. | passw0rd | 0.2% |
| 10. | solo | 0.2% | 20. | dragon | 0.1% |



22

## Password Based Authentication

Vulnerabilities of passwords and countermeasures

- Workstation hijacking - IDS
- Exploiting user mistakes – training, IDS, combined with other means
- Exploiting multiple password use – policy
- Electronic monitoring – encrypted links




23

## Password Based Authentication

Vulnerabilities of passwords and countermeasures (for Web)

Top 10 2013-A2-Broken Authentication and Session Management

Attack Example (OWASP)

Airline reservations application supports URL rewriting, putting session IDs in the URL:

An authenticated user of the site wants to let his friends know about the sale. He e-mails the above link without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.

https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication



24

## Password Based Authentication

Vulnerabilities of passwords and countermeasures (for Web)

Top 10 2013-A2-Broken Authentication and Session Management

Countermeasure

- A single set of strong authentication and session management controls

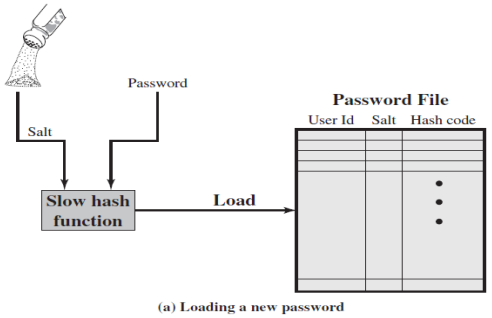

- Strong efforts should also be made to avoid XSS flaws which can be used to steal session IDs



25

## Password Based Authentication

Hash based authentication: Loading a new password




(a) Loading a new password



26

## Password Based Authentication

Salt and Its Benefits

Salt: A fixed-length value.

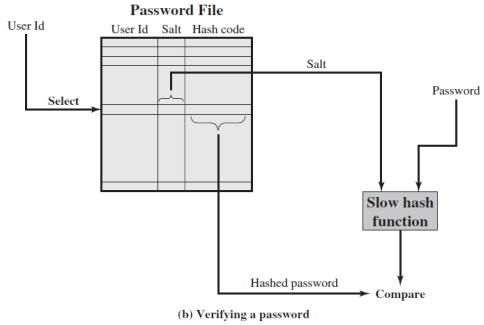
- Prevent duplicate password in the password file
- Increase the difficulty of offline dictionary attack
- Nearly impossible to find out the same password in many systems for a specific user



27

## Password Based Authentication

Hash based authentication: Verifying a password




(b) Verifying a password



28

## Password Based Authentication

Password cracking

- Dictionary attacks : try each word then obvious variants in large dictionary against hash in password file
- Rainbow table attacks
  - Pre-compute tables of hash values
  - a table of hash values, hash chains
  - e.g. 1.4GB table cracks 99.9% of alphanumeric Windows passwords in 13.8 secs
  - not feasible if larger salt values used

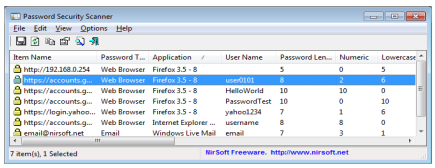


29

## Password Based Authentication

Password selection strategies

- User education
- Computer generated passwords
- Reactive password checking: system periodically runs its password cracker to find guessable passwords.




- Proactive password checking: a user is allowed to select password if it complies with system requirements at the time of selection.

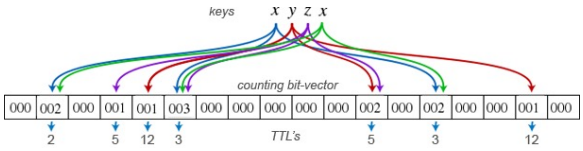


30

## Password Based Authentication

Approaches to proactive password checking

- Rule enforcement
- Password checker
- Bloom filter






31

## Token Based Authentication

Objects that a user possesses for the purpose of user authentication are called tokens.

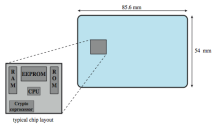



32

## Token Based Authentication

Some cards used as tokens

- Electronic Identity Cards
- Memory
  - Memory cards can store but not process data.
  - Store only a simple security code.
- Smart Card
  - Electronic memory and processor inside
  - Authentication protocol
    - Static
    - Dynamic password generator
    - Challenge-response

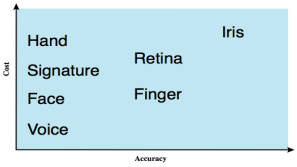




33

## Biometric Based Authentication

- Authenticates an individual based on one of its physical characteristic.
- Based on pattern recognition
- Technically complex and expensive

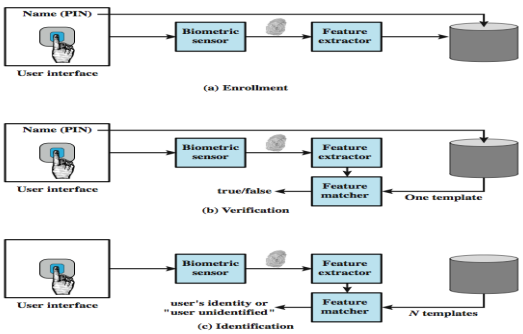





34

## Biometric Based Authentication

Operations



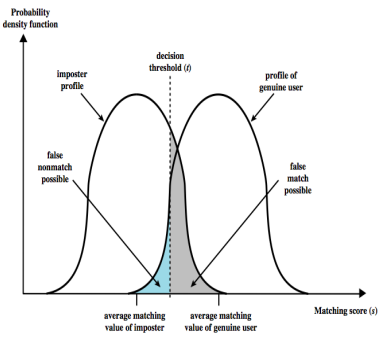



35

## Biometric Based Authentication

Accuracy

- never get identical templates
- problems of false match / false non-match






36

## Remote User Authentication

- Authentication over a network or communication link.
- Problems: complex, eavesdropping, replay

- Challenge-response protocol

1. User sends identity
2. Host responds with a random number
3. User computes f(r, h(P)) and sends back
4. Host compares values from user with own computed value, if mach user authenticated

| Client | Transmission | Host |
|---|---|---|
| $U$, user | $U \rightarrow$ | |
| | $\leftarrow \{r, h(), f()\}$ | random number h(), f(), functions |
| $P'$ password $r'$, return of $r$ | $f(r', h(P')) \rightarrow$ | |
| | $\leftarrow$ yes/no | if $f(r', h(P')) = f(r, h(P(U)))$ then yes else no |

(a) Protocol for a password



37

## CAPTCHA

A CAPTCHA (a backronym for "**C**ompletely **A**utomated **P**ublic Turing test to tell **C**omputers and **H**umans **A**part") is a type of challenge-response test used in computing to determine whether or not the user is human.


A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text, but current computer programs cannot:



38

## Some Attacks on User Authentication

- Client attacks
  - Password guessing, exhaustive search for tokens,..
  - Limited attempts, large entropy,…
- Host attacks
  - Plaintext theft, passcode theft, template theft,..
  - Hashing, large entropy, protection of password database, OTP,..
- Eavesdropping
  - Shoulder surfing, theft, Copying (spoofing) biometric,..
  - Multifactor authentication, tamper resistant token, ..
- Replay, Trojan Horse, Denial-of-service, …



39

## Summary

- Introduction to authentication
- Password, Token, Biometrics
- Remote user authentication
- Security issues



40