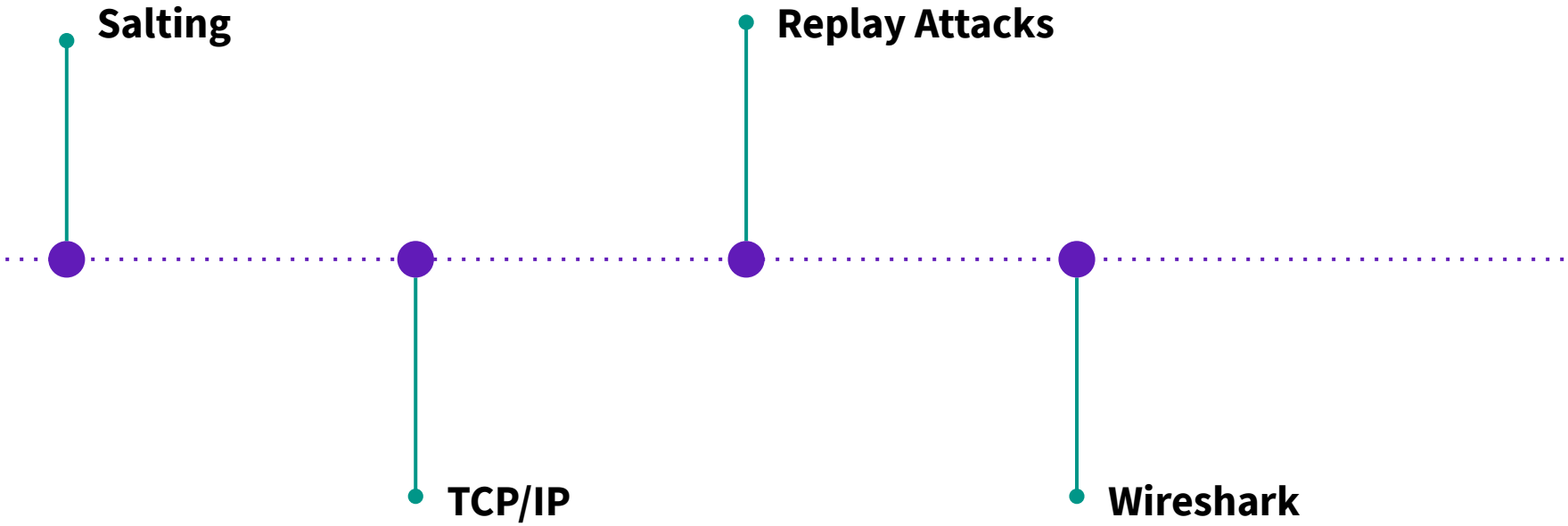
RECITATION - 5

ADITI PRAKASH
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF COLORADO BOULDER

Topics



LinkedIn Data Breach

Year: 2012

What happened? Data Breach

Why? Unauthorized access that resulted in the disclosure of members' passwords

How? LinkedIn stored passwords with an hashing algorithm but with no salt or other advanced security measures in place.

Salting - Password Hashing

- Unique value added to the end of a password to create a different hash
- Protects against brute-force attacks by adding “salt” to the end of the password and hasing it
- Example:
  - hash (“letmein” + “F34564R8”) = 8f3k9j3hdk98jk30lsvn9al30lfb48slhbtwe9uk
  - hash (“letmein” + “Y456f3q9”) = ber5jg0qhekgl8dkjhl52309uwlkmcbkuw385b
- The salt for each password should be different

Add some salt to the password before hashing

Encryption Vs Hashing Vs Salting

- **Encryption:** Two-way function where the information gets encoded and can be decoded later.
- **Hashing:** One-way function where data is mapped to a fixed-length value. Used for authentication(check-sum).
- **Salting:** Additional step during hashing (hashed passwords), that adds an additional value to the end of the password which changes the hash value produced.

TCP/IP

Transmission Control Protocol / Internet Protocol

- Specifies how data is exchanged over the internet.
- TCP: defines how messages are assembled into packets and sent
- IP: defines where to send the packets - address and route

TCP/IP

- Client/server model of communication
  - Client: A user or machine
  - Service : Sending a webpage
  - Server: Another computer in the network
- Stateless protocol
  - Being stateless frees up network paths so they can be used continuously
- The transport layer itself is stateful
  - It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

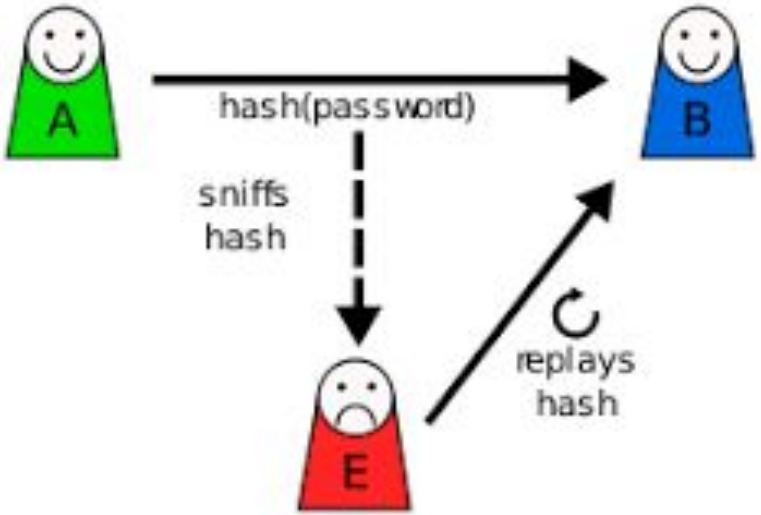
- *Application layer* provides applications with standardized data exchange.
    a. Includes HTTP, FTP, POP3, SMTP and SNMP.
- *Transport layer* maintains end-to-end communications across the network.
    a. Include TCP and UDP
- *Network layer*, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries.
    a. Protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.
- *Physical layer* consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network.
    a. Includes Ethernet for LANs and the Address Resolution Protocol (ARP).

SSL
Secure Sockets Layer

- Encrypted link between web server and browser
- Encrypted with SSL-> browser forms a connection with the webserver, checks SSL certificate, and binds together browser and the server.

Replay Attacks

Why encrypting everything is not enough?



Solution:

1. **Use encryption keys that change over time**
2. **Give the user a different challenge each time**
3. **Using timestamps on all messages**

Wireshark

- Open source Network traffic analyzer tool
- Converts that binary traffic into human-readable format
- This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, etc.
- Applications:
  - Troubleshoot Dropped packets, latency issues, and malicious activity on your network
  - Network administrators use it to *troubleshoot network problems*
  - Network security engineers use it to *examine security problems*
  - QA engineers use it to *verify network applications*
  - Developers use it to *debug protocol implementations*

Resources

- TCP vs UDP
  - https://www.youtube.com/watch?v=Vdc8TCESIg8
  -
- Wireshark Download link
  - Windows & MacOS: https://www.wireshark.org/download.html
  - Linux: http://www.linuxfromscratch.org/blfs/view/svn/basicnet/wireshark.html