Course Instructor:
Anwar Haque

Lecture #10
Dept. of Computer Sc, Western University
Network Security

- Importance of Security in networks
- What is network security?
- Principles of cryptography
- Message *authentication*
- E-mail Security
- Securing TCP Connections: SSL
- Network layer security: IPsec for VPN
- Wireless Networks Security
- Firewalls
- IDS / IPS
What is network security?

- **confidentiality**: only sender, intended receiver should “understand” message contents
  - sender encrypts message
  - receiver decrypts message
- **authentication**: sender, receiver want to confirm identity of each other
- **message integrity**: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- **access and availability**: services must be accessible and available to users

What is Wireless Access Networks?

Wireless Clients

WAP 1

WAP 2

Wired Networks
Wireless Access Networks

❖ Basic components of Wireless Access
  ▪ Wireless Clients
  ▪ Distribution Stations (DS)
  ▪ Wireless Access Points (WAP)

❖ Why Wireless (compare to wired access networks)
  ▪ Client convenience
  ▪ Mobility
  ▪ Simplified network management/maintenance
  ▪ ISP economic benefits
  ▪ Better network reliability as fewer network access points

Info Source: Dr. Daniel Soper @
https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgpqWAF01wh7GNICyQLfxi&index=9&t=0s
Wireless Access Networks

- **Wireless Access Points (WAP)**
  - Connected to a wired network
  - Radio communication between the clients
    - Must have transmitted and receiver
  - Operates on IEEE 802.11x standards (1999 to present)
    - IEEE 802.11b: 11Mbps, 150 feet, 2.4GHz
    - IEEE 802.11a: 54Mbps, 5GHz
    - IEEE 802.11n: 300Mbps, 2.4GHz and 5GHz
    - IEEE 802.11ac: 1300Mbps on 5GHz | 450Mbps on 2.4GHz

- SSID (broadcast or hidden)
Wireless Access Networks

- Wireless Clients
  - Radio communication between the client and WAP
    - Client must have transmitted and receiver
  - Network Interface Card (or similar interface integrated into the client hardware systems)
    - Media Access Control (MAC) address which is theoretically unique
  - Operates on IEEE 802.11 standards

Info Source: Dr. Daniel Soper @ https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNIcCyQL.fxi&index=9&t=0s
Wireless Access Networks

- IEEE 802.11 Frame Format*

*IEEE 802.11 MAC frame format. Image from William Stallings "Data and Computer Communications".
Wireless Access Networks Security

❖ How does it different than Wired Access
  ▪ No Physical Access
  ▪ Unknown network footprint

❖ Security Risks
  ▪ SSID Broadcasting
    • Open vs closed
  ▪ SSID cloaking
  ▪ MAC Spoofing
  ▪ With an SSID and a spoofed MAC address, an existing wireless connection can be hijacked

Info Source: Dr. Daniel Soper @
https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAtO1wh7GNIcylfQxi&index=9&t=0s
Wired Eqv Privacy (WEP)

- A wireless access protocol in 1999
  - Goal is to provide similar data privacy in wireless domain as it is for wired network

- Security Loopholes
  - Shared static key
  - Short key
  - Weak encryption
  - Integrity check algorithm is public
  - No Authentication
  - WEP can be decrypted in a few mins with special software

Info Source: Dr. Daniel Soper @
https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNICyQLfxi&index=9&t=0s
Wifi Protected Access (WPA and WPA2)

❖ WPA / WPA2 replaces WEP

❖ Security Loopholes Addressed by WPA
  ▪ Shared static key: WPA uses a dynamic encryption key
  ▪ Short key: WPA uses long key
  ▪ Weak encryption: WPA uses strong encryption
  ▪ Integrity check algorithm is public: WPA uses improved integrity protection
  ▪ Uses real authentication

Info Source: Dr. Daniel Soper @ https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNlCyQLfxi&index=9&t=0s
Wifi Protected Access (WPA and WPA2)

- WPA:
- TKIP (Temporal Key Integrity Protocol)
  - Rotation of keys
  - WPA was built on TKIP
    - Each packet gets a new unique encryption key
    - Adds sequence counter to avoid replay attack
    - 64-bit message Integrity Check

- WPA2 started from 2004
  - Advanced Encryption Standard (AES) with CCMP (Counter mode with Cypher block chaining Method authentication Protocol)

Info source: https://www.youtube.com/watch?v=8hTGoSiRcyQ
(WPA and WPA2) Security Issues

❖ WPA2
❖ CCMP:
  ▪ Replaced TKIP when WPA2 is introduced
  ▪ Introduces AES and uses 128 bit key
  ▪ Requires additional computing resources
  ▪ Introduces wired network like public-private key encryption, authentication, certification etc.

Info source: https://www.youtube.com/watch?v=8hTGoSiRcyQ
**WPA and WPA2 Man-in-the-Middle-Attack**

- The intruder waits in a WAP zone for a legitimate client / user to initiate an association with the WAP, and then extracts MAC of both WAP and the legitimate user.

- The intruder then changes its MAC to match the WAP’s MAC and sends a dis-associate request to the legitimate user.

- The legitimate user terminates the association (WAP is not aware of this), and meanwhile the intruder changes its MAC to match the legitimate user’s MAC and continued legitimate user’s authenticated session with WAP.

*Info Source: Dr. Daniel Soper @ https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNlCyQLfxi&index=9&t=0s*
WPA and WPA2 Authentication Attack

- The intruder acquires the SSID of a legitimate, established WAP.
- The intruder then establishes his WAP using the same SSID as the legitimate established WAP. This allows the intruder to masquerade as the legitimate WAP.
- A legitimate user attempts to authenticate the malicious WAP by sending its authentic credentials.
- The malicious WAP can then uses the legitimate user’s credentials to access the network via the legitimate WAP.

Info Source: Dr. Daniel Soper @ https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNIcylfL.fxi&index=9&t=0s
WPA and WPA2 Password Attack

- WPA and WPA2 allows for password-based authentication
- Password attack is effective if the password is short or not difficult to guess
- In such cases, password-cracking approaches such as brute-force attack or dictionary attacks are used

Info Source: Dr. Daniel Soper @
https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgPqWAfO1wh7GNIcYQL.fxi&index=9&t=0s
Securing Wireless Networks

❖ Use WPA2 NOT WEP
❖ Network Authentication: Long/complex/hard to guess password
❖ Decision between Open vs Closed SSID broadcasting
❖ Specify allowable MAC addresses

Info Source: Dr. Daniel Soper @
https://www.youtube.com/watch?v=6pYZ2N9y2fQ&list=PL1LIXLIF50uWgLwPqWAfO1wh7GNIcYQL.fxi&index=9&t=0s
Network Security

❖ Importance of Security in networks
❖ What is network security?
❖ Principles of cryptography
❖ Message authentication
❖ E-mail Security
❖ Securing TCP Connections: SSL
❖ Network layer security: IPsec for VPN
❖ Wireless Networks Security
❖ Firewalls
❖ IDS / IPS