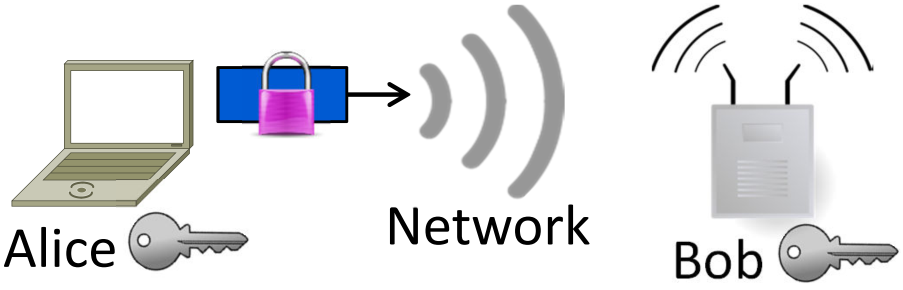
# Introduction to Computer Networks

## Wireless Security (§8.6.4)

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY *of* WASHINGTON

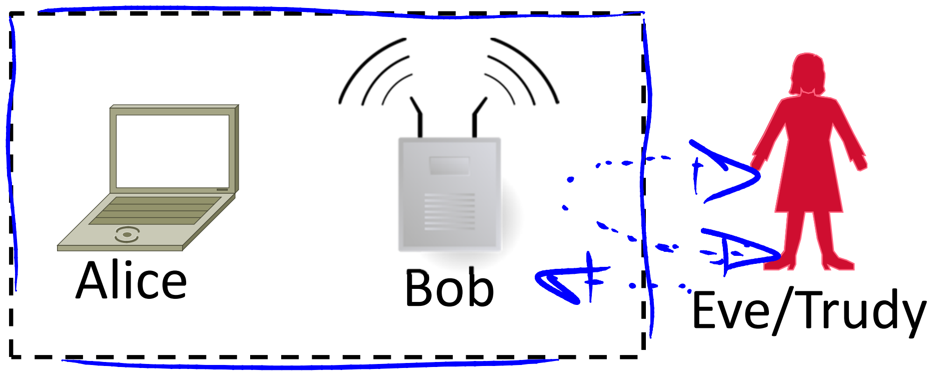
# Topic

- Securing wireless networks
  - Focus on 802.11



# Goal and Threat Model

- Unlike wired, wireless messages are broadcast to all nearby receivers
  - Don’t need physical network access
  - Heightens security problems



# Goal and Threat Model (2)

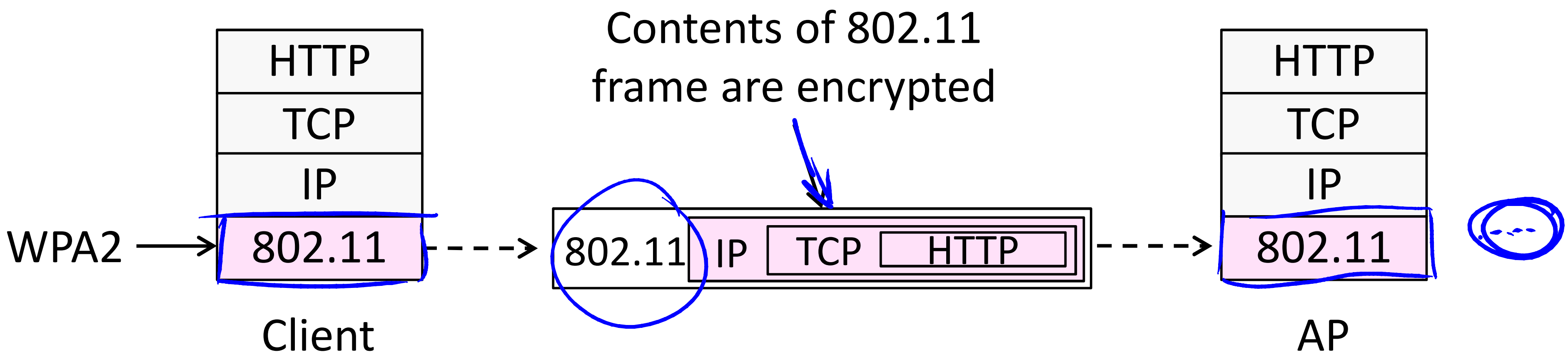
- Two main threats:
  1. Eavesdropping on conversations
  2. Unauthorized access to network
- We'll consider 802.11 setting
  - Assume external attacker can send/receive wireless messages

# 802.11 Security

- Security is based on passwords
  - For access control and confidentiality and integrity/authenticity
- 802.11 standard (1999) used WEP
  - For "Wired Equivalent Privacy"
  - Badly flawed, easily broken
- 802.11i standard in 2004
  - WiFi Protected Access or WPA2
  - This is what you should use

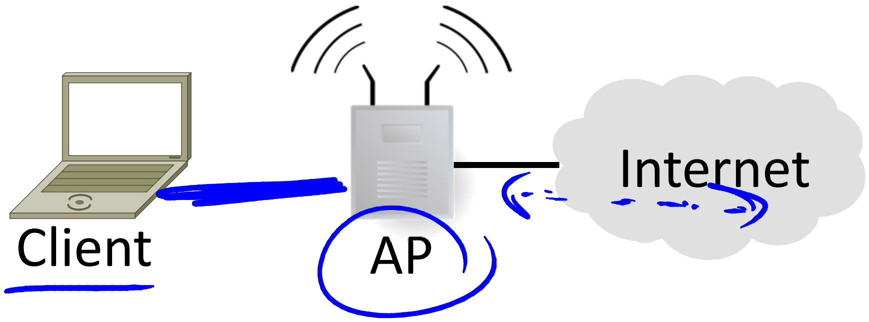
# 802.11 Security

- Security is part of 802.11 protocol
  - Encrypted message between client and AP; removed after AP



# Home Network

- AP is set up with network password
- Each client also knows password
- Client proves it knows password »
  - AP grants network access if successful

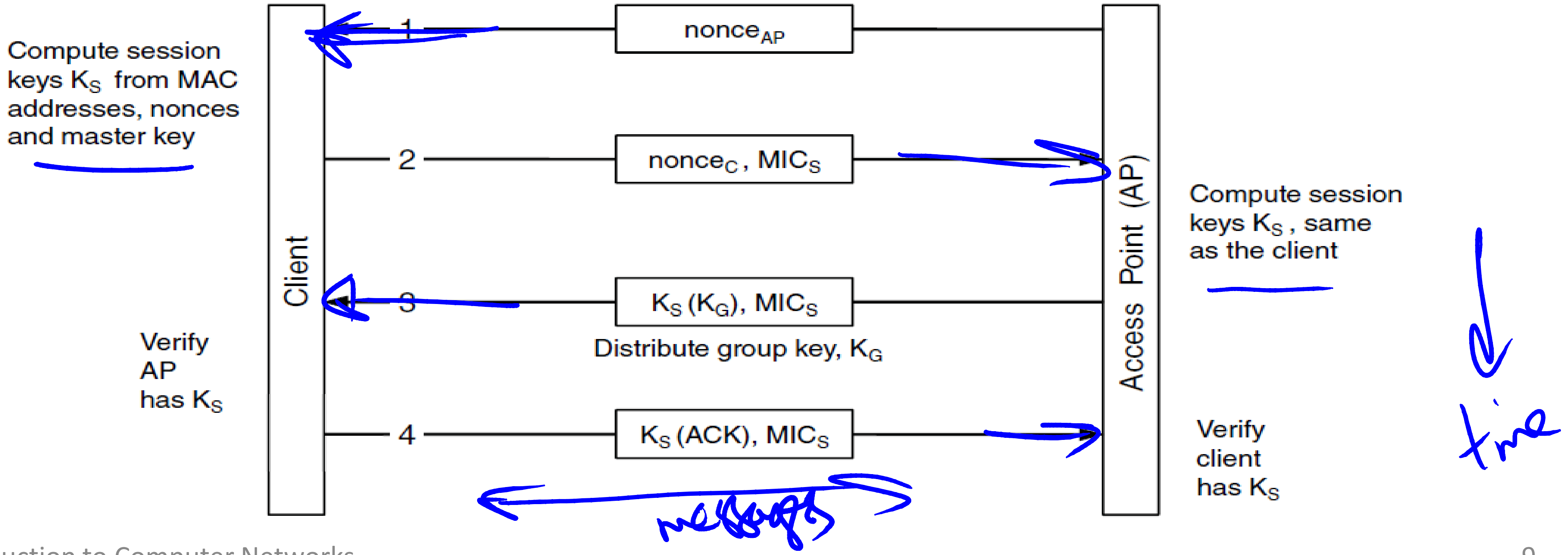


# Home Network (2)

- For access, client authenticates to AP »
  - Both compute a shared session key based on the password
  - If client knows the session key it has proved that is has the password
- For usage, client/AP encrypt messages
  - For confidentiality, integrity/authenticity
  - No access without the session key
  - Also group key for AP to reach all clients

# Home Network (3)

- Master key is from password; nonces for freshness
  - $K_S$ lets client talk to AP; $K_G$ lets AP talk to all clients



Client

Access Point (AP)

Compute session keys $K_S$ from MAC addresses, nonces and master key

1 nonce$_{AP}$

2 nonce$_C$, MIC$_S$

Compute session keys $K_S$, same as the client

3 $K_S$ ($K_G$), MIC$_S$

Distribute group key, $K_G$

Verify AP has $K_S$

4 $K_S$ (ACK), MIC$_S$

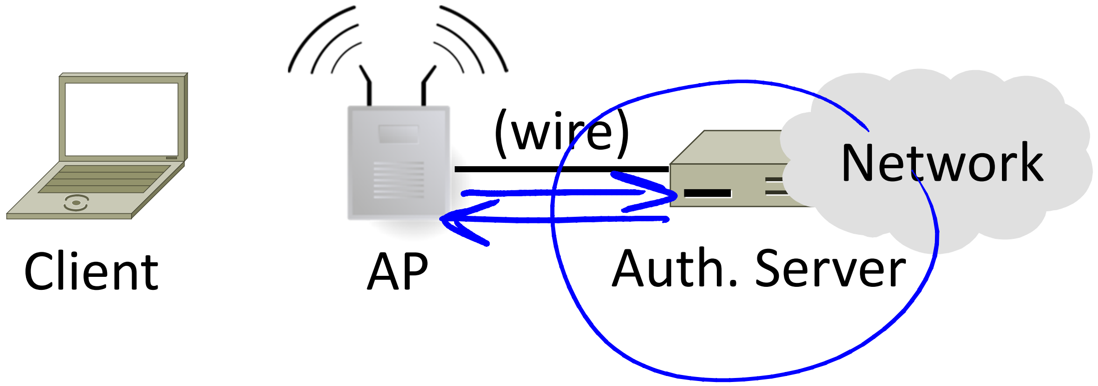
Verify client has $K_S$

messages

time

# Enterprise Network

- Network has authentication server
- Each client has own credentials
- AP lets client talk to auth. server
  - Grants network access if successful



# END

UNIVERSITY of WASHINGTON