FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

6. WiFi Hacking

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

Security through Obscurity

WiFi Di-association/De-authentication

Security Through Obscurity

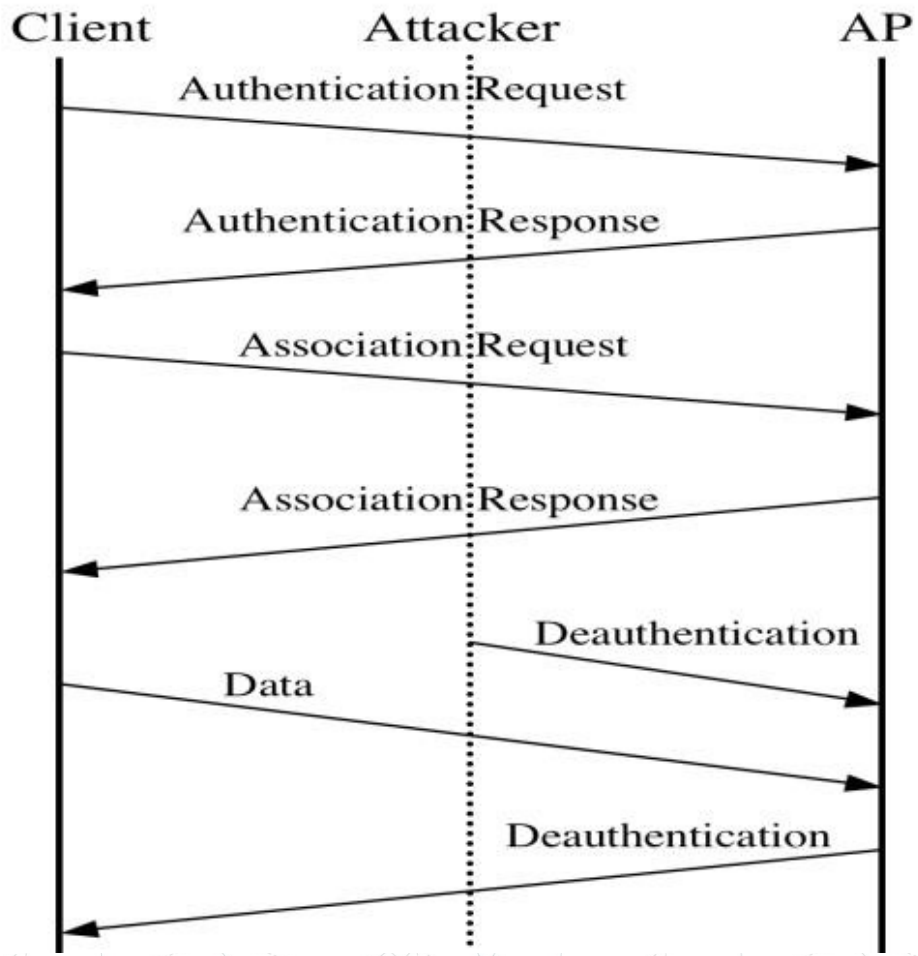
- Wireless network can operate in hidden or non-broadcasting mode
  - They don't include their SSID (network name) in beacon packets, and don't respond to broadcast probe requests
- SSID is not (cannot be) a secret since it is included in many packets coming from legitimate clients (not just beacon packets)
  - You need to know SSID associated with which AP

Security Through Obscurity

- Passive sniffers can easily take advantage of this behavior
  - If you sniff the network, you will get the SSID whenever someone joins the network
  - You may even force user's hand
    - How?

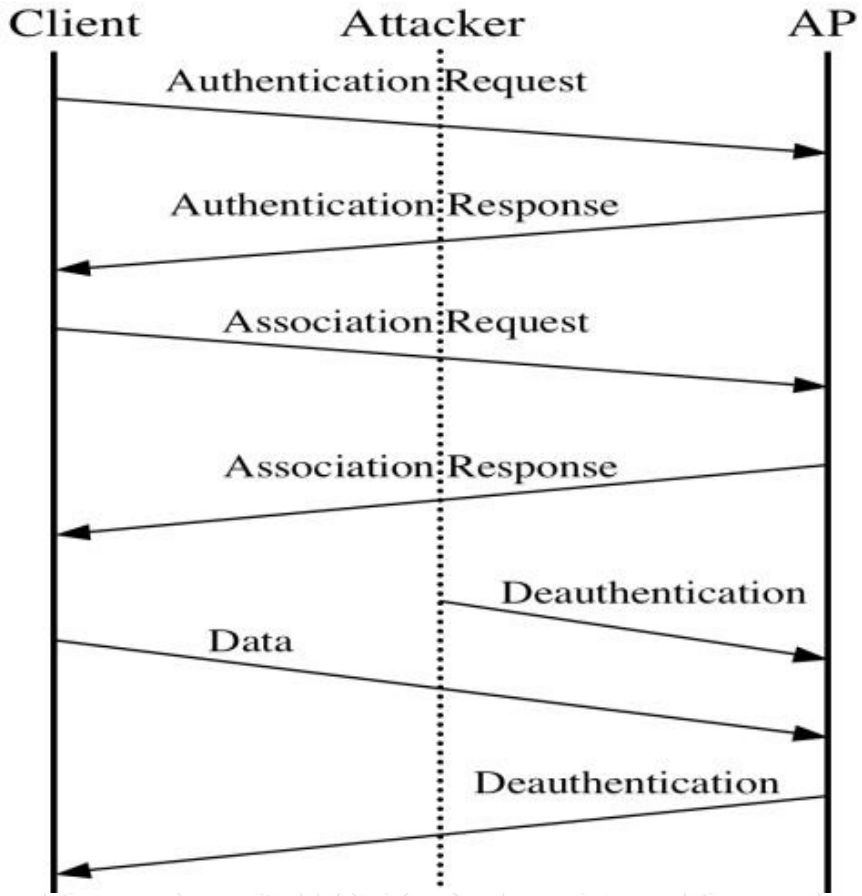
De-authenticating user

- Management frames in 802.11 are not authenticated
  - Send a packet to user that looks like coming from AP
  - The user can't tell the difference
  - Wireless driver will reconnect immediately
  - Reassociation request with the SSID in it will be sent



The De-authentication Frame

- A type of packet defined in the IEEE 802.11 WiFi standard
  - It has been part of the standard since the beginning and still plays an important role
- It's used to terminate a WiFi connection
  - It can be sent by either the AP or the station to let the other side know that the connection is closed

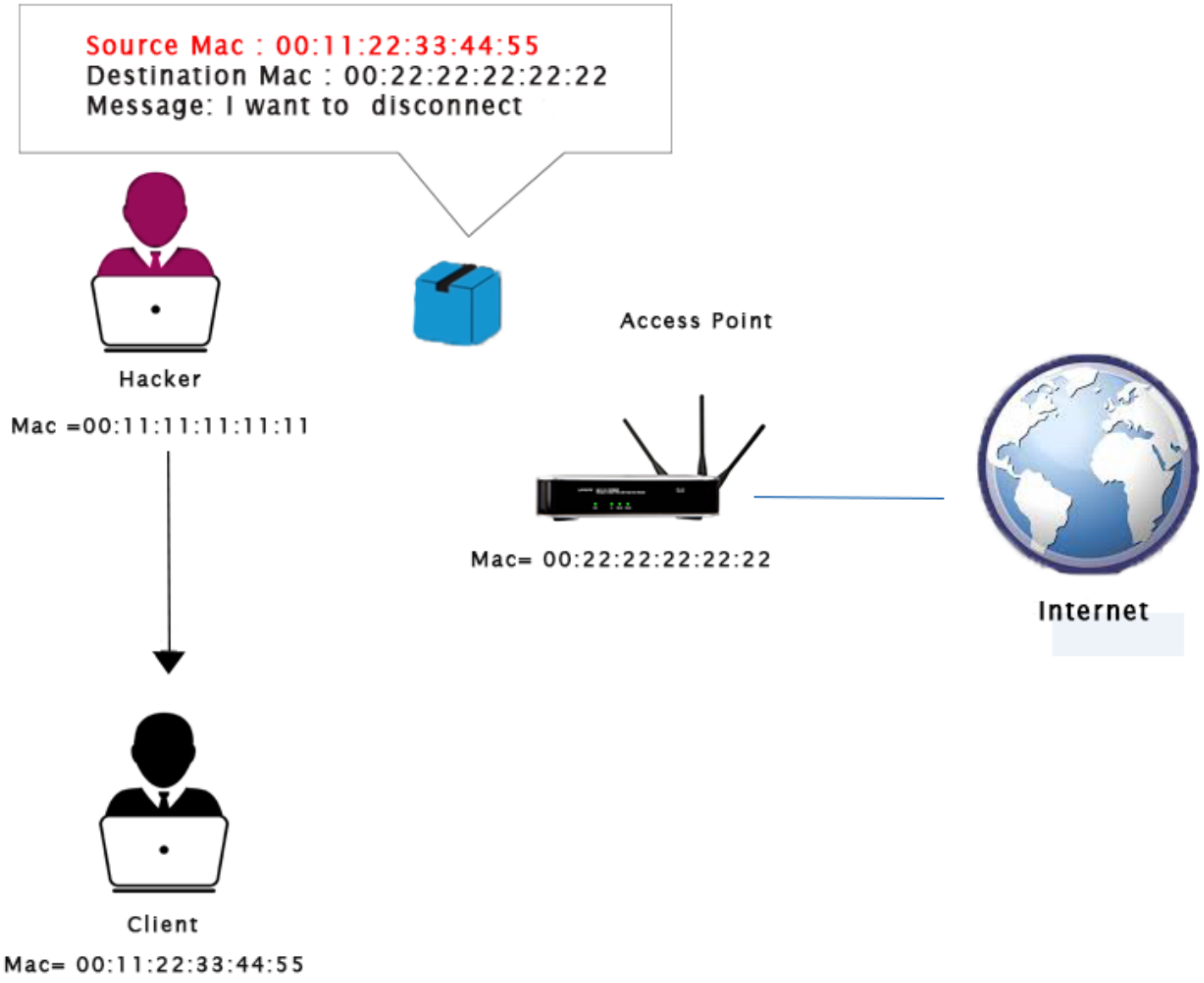


The Deauthentication Frame

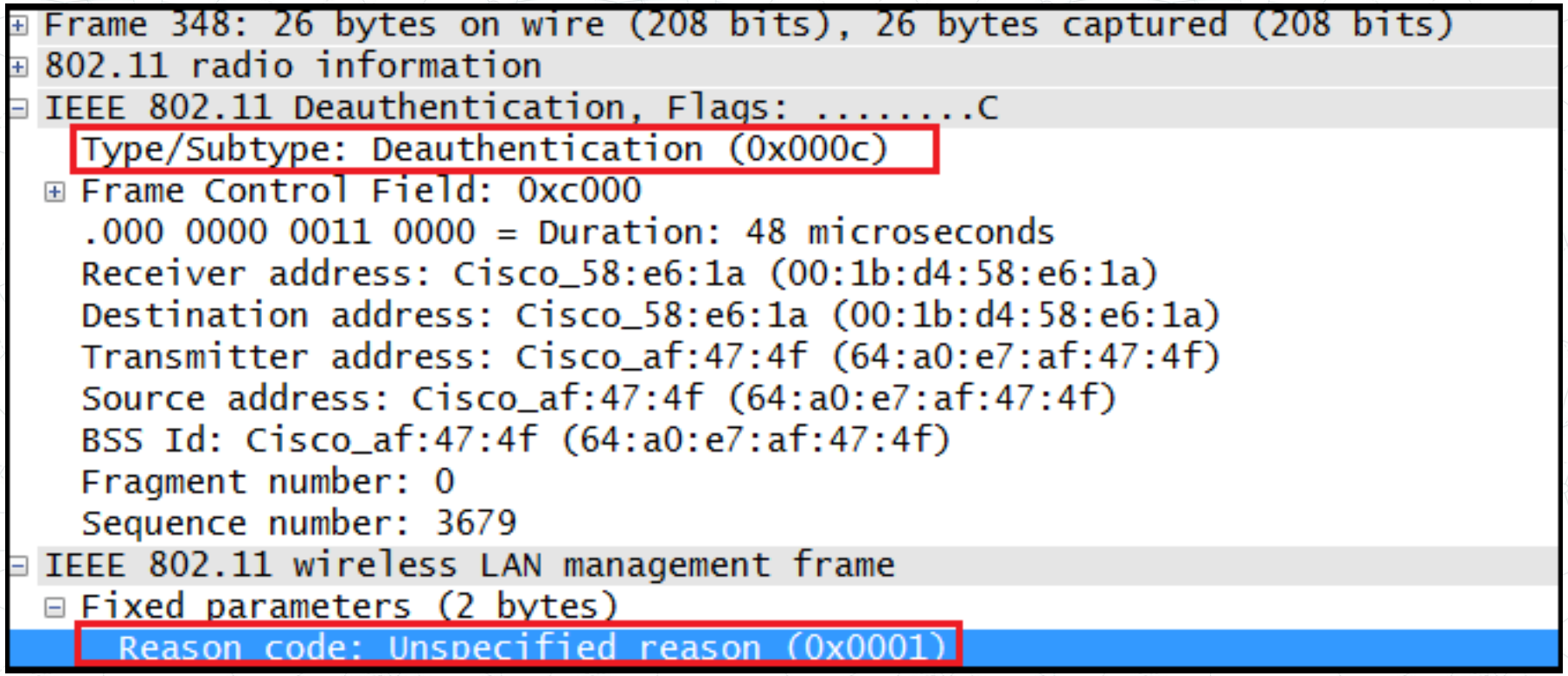
- The station might send a deauthentication frame to the access point because it's switching to another WiFi network
  - Or the access point might send a deauthentication frame to the station because the router has to restart
  - Deauthentication works both ways, and there are plenty of reasons why they are sent - you can find a complete list of reasons below

The Deauthentication Frame

- But one crucial attribute of the deauthentication frame is that it's not a request; it's a notification, and it can not be refused



The Deauthentication Frame Example



Di-association vs. De-authentication

- In the case of a regular home router, you both authenticate and associate to the same AP
  - And if you disconnect, you both deauthenticate and disassociate to the same AP
- But in a larger network made out of multiple APs, you might disassociate from one AP and associate to a new one while staying authenticated to the same network

How can De-auth be Exploited?

- Deauthentication frames are very simple in their structure
  - You basically only need a sender or receiver MAC address
  - And you can obtain such by simply scanning for WiFi devices nearby
- Thus, it's very easy to spoof a deauth packet
  - And keep in mind that if the target receives it, it has to drop its connection

How can De-auth be Exploited?

- The target can reconnect immediately and it can do that quite fast, maybe without the user noticing that the connection was ever dropped
- But if these deauth packets are sent continuously, it results in a denial of service attack, and network access is blocked for the entirety of the attack
- Luckily this was addressed, and we now have protected management frames!
  - This feature allows packets like deauthentication frames to be safe against spoofing

Protected Management Frames

- PMF provide protection for unicast and multicast management action frames
  - Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging
- PMF is required for all new certified devices
  - However, may not be implemented in all devices out there

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger