

Appraising Wireless Threats



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | LinkedIn: dalemeredith

Wireless is wireless and its digital. When digital first started, I swear I could hear the gap between ones and zeros.

Eddie Van Halen

Types of Attacks

Access Control Attacks



WarDriving

Rogue Access Points

MAC Spoofing

AP Misconfiguration

Ad-Hoc Association

Promiscuous Client

Client-Misconfiguration

Unauthorized Association

Integrity Attacks

Data frame injection

WEP injection

Bit flipping attack

Data Replay

RADIUS Replay

**Wireless network
viruses**

Confidentiality Attacks



Eavesdropping



Traffic analysis



Cracking WEP



Evil twin access point

Confidentiality Attacks



Honeygot APs



Session hijacking



Masquerading



Man-in-the-middle attack



Pause



Rewind



Play again

Availability Attacks



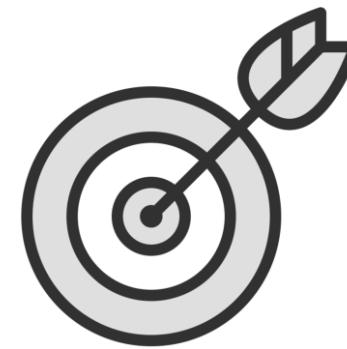
AP Theft



Beacon flooding



Disassociation attack



Denial-of-Service attack



EAP failures



Deauthentication flood

Availability Attacks



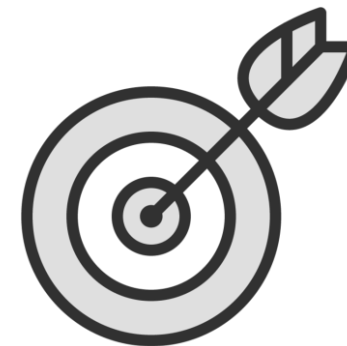
Routing attacks



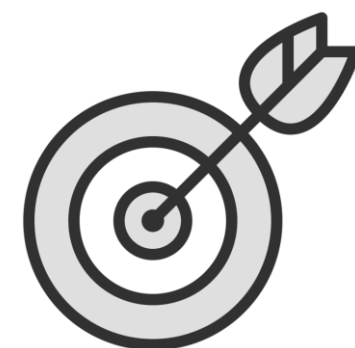
Power saving attack



Authentication flood



TKIP MIC exploit



ARP poisoning

Authentication Attacks

PSK Cracking

LEAP Cracking

VPN Cracking

**Password
assumption**

App login theft

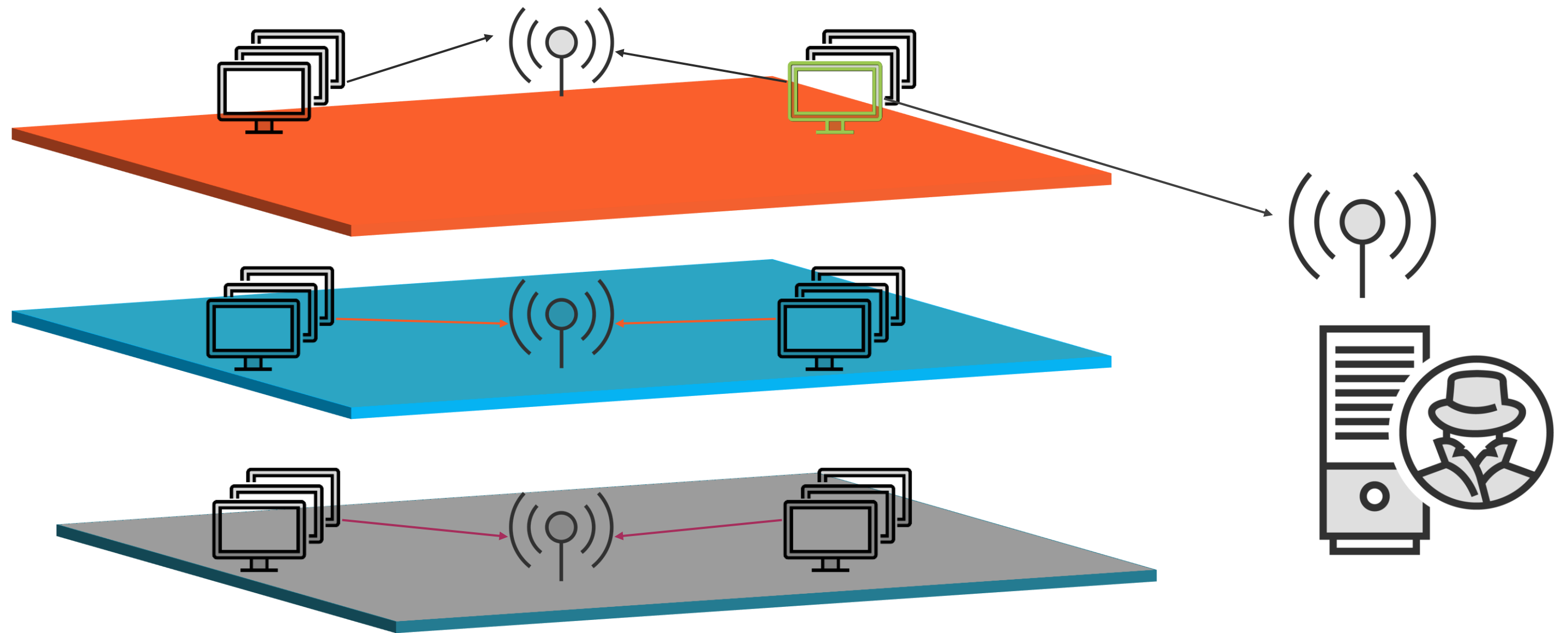
Demo



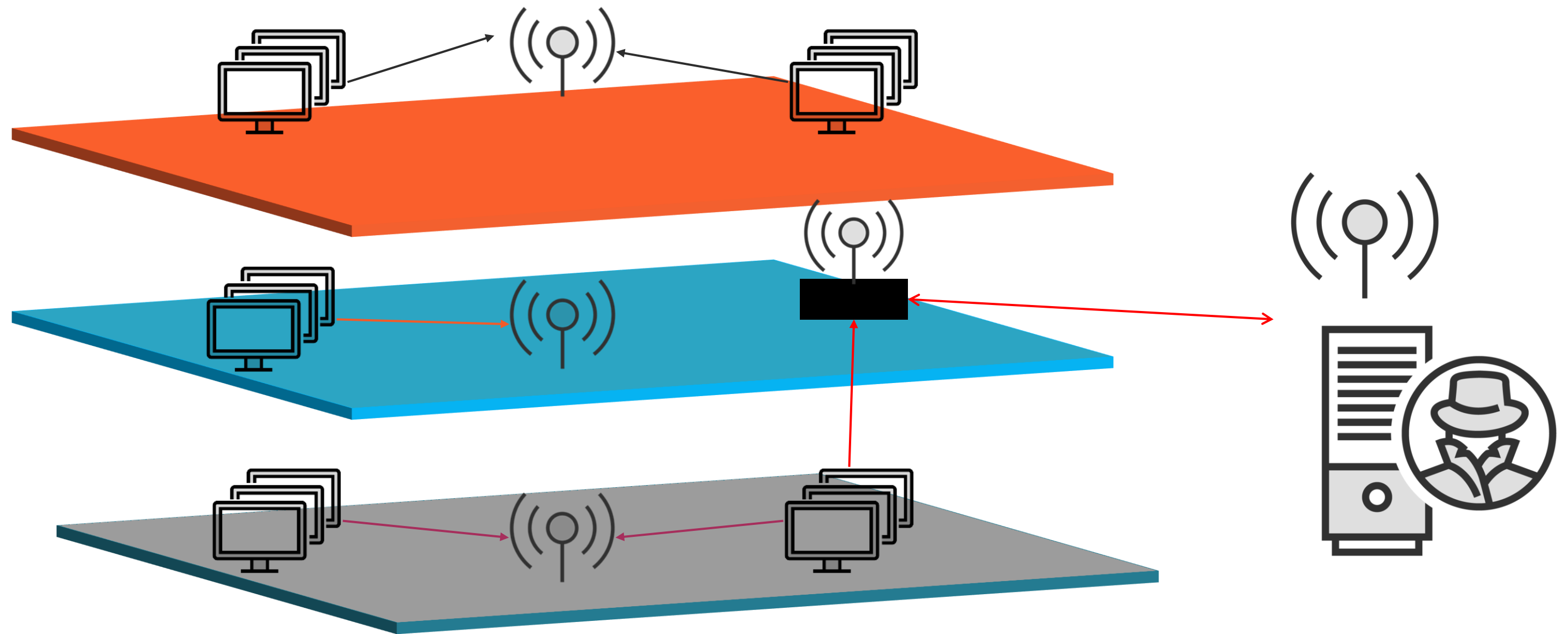
Let's do a little WarDriving

Access Point Attacks

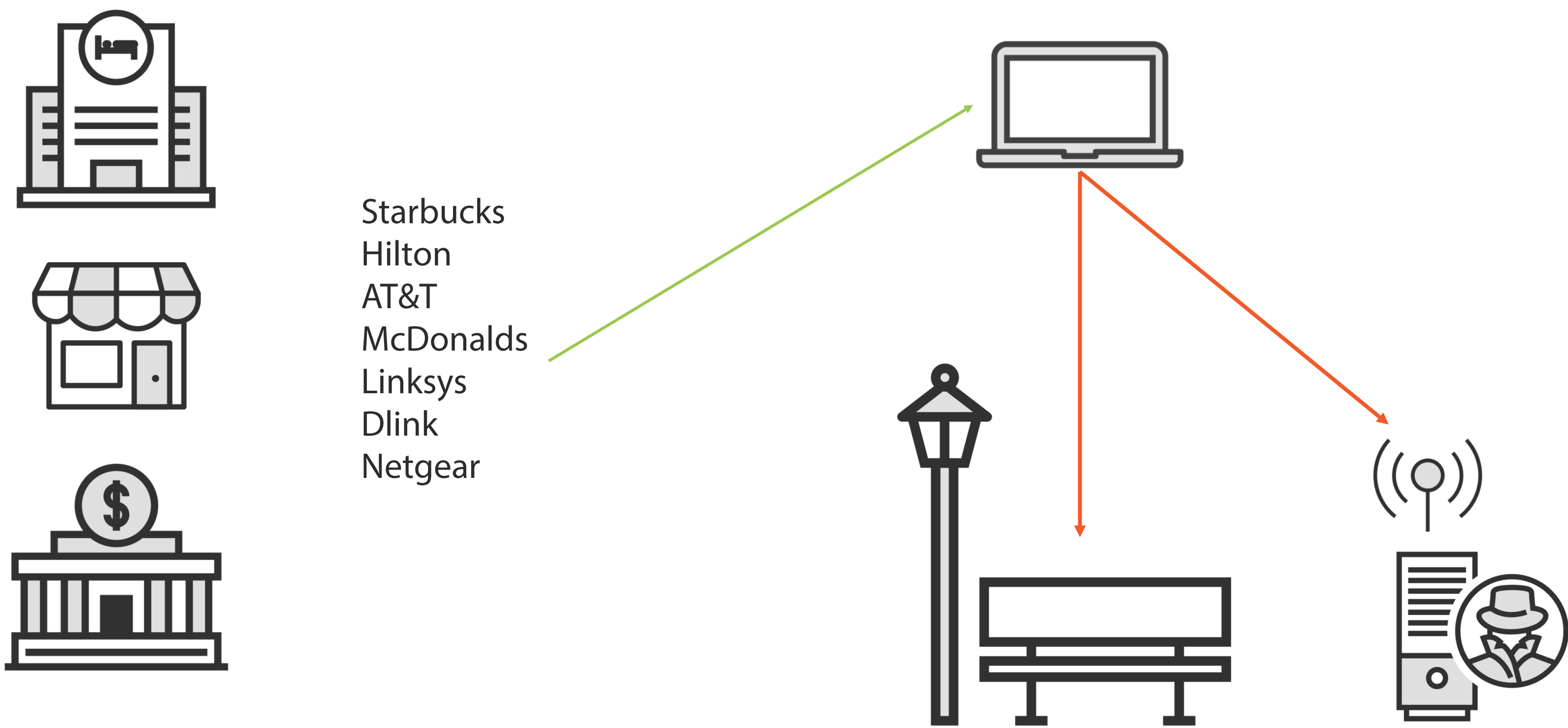
Let's Go Rogue



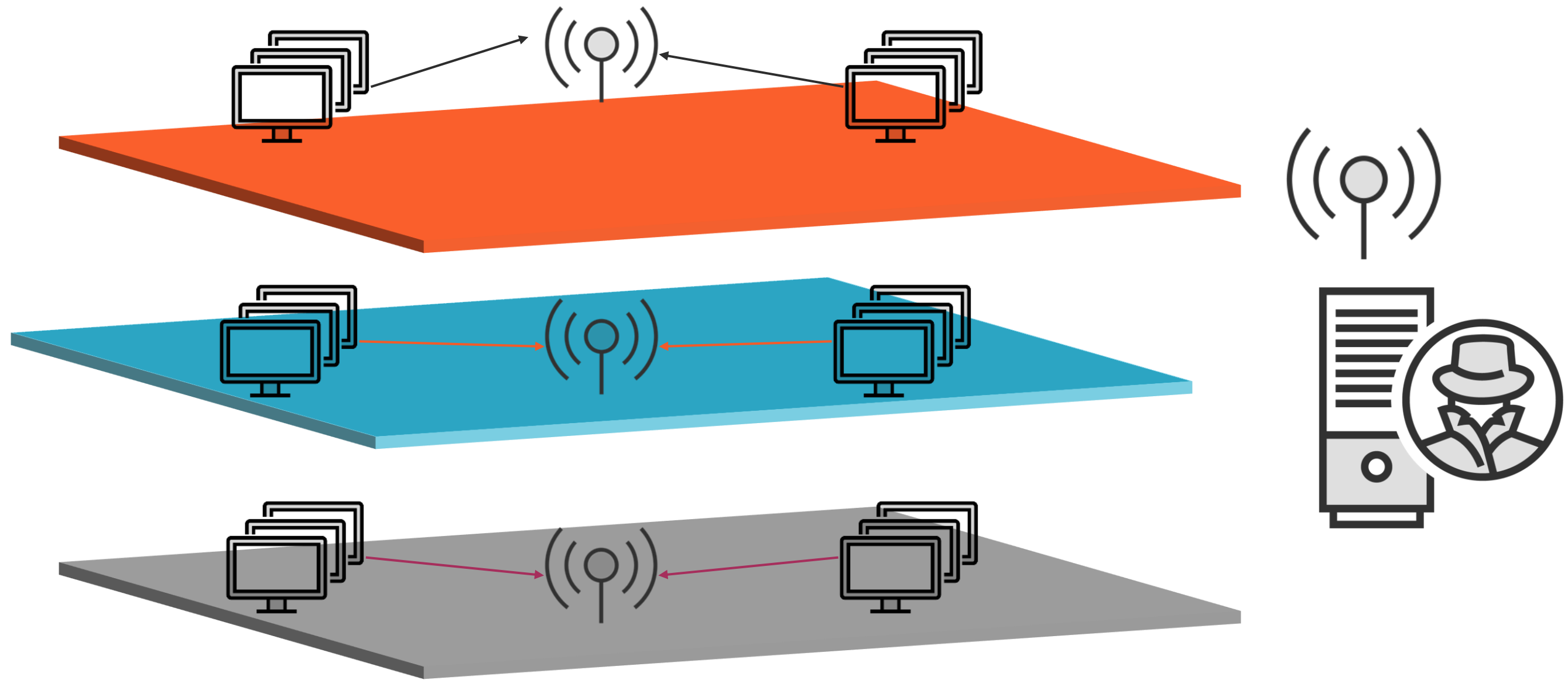
Unauthorized Association



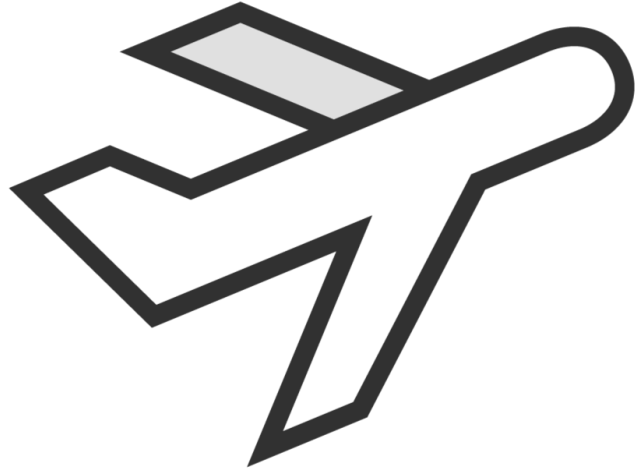
Honeypot AP Attacks



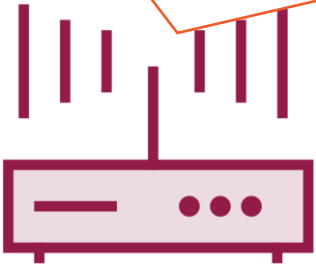
AP MAC Spoofing



AP MAC Spoofing



Allow
AA:BB:CC:DD:EE:FF



AA:BB:CC:DD:EE:FF

AA:BB:CC:DD:EE:FF



Demo



Looking at known networks

Client Attacks

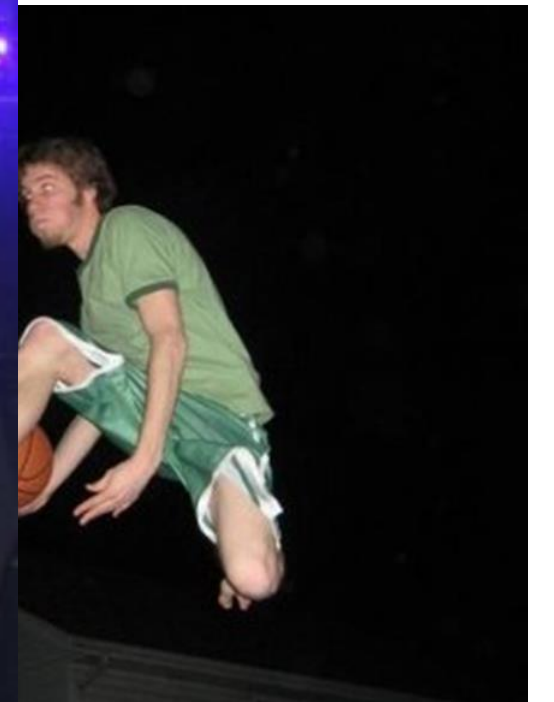
DoS Attacks

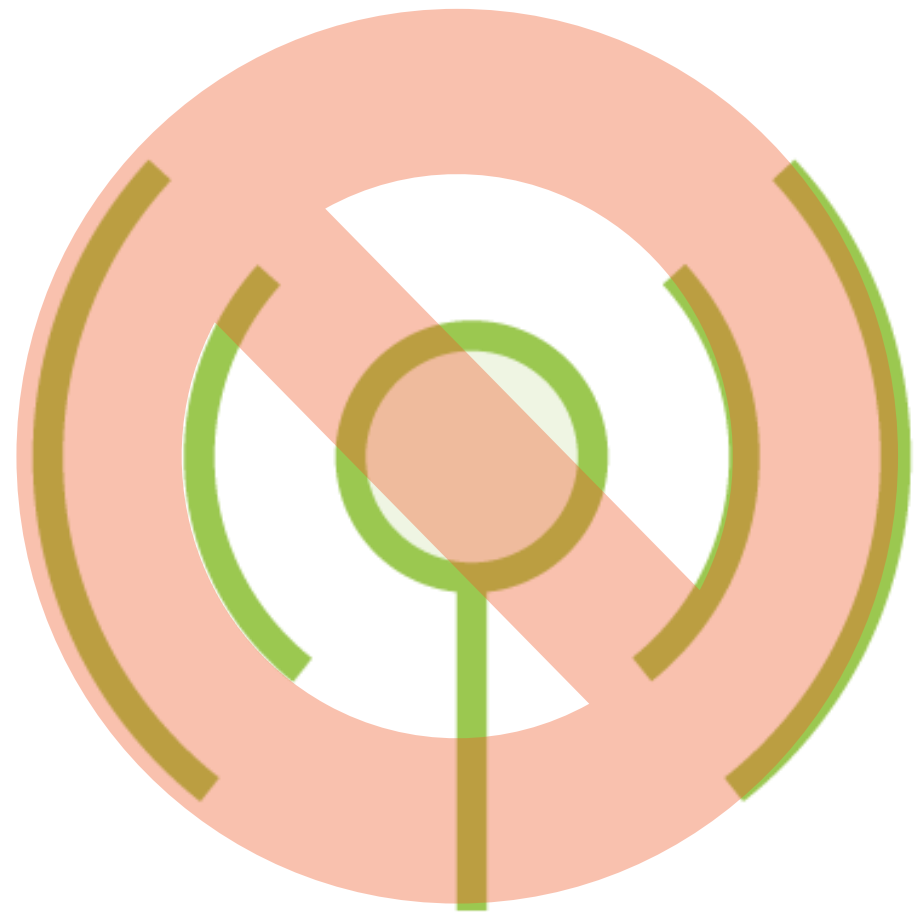


Ad-hoc Attacks



Jamming





Up Next:

Illustrating the Wireless Attack
Methodology
