OWASP

Open Web Application Security Project

Pen-test Lab Initiative ➢ Wireless Security 101

Jon Williams, CISSP

June 15, 2017

Introductions

- OWASP
- About me
- About you: who you are, where you're from, what you're looking to learn

OWASP

Pen-testing initiative

OWASP
Open Web Application
Security Project

Mission

- Create capability within CT chapter that would allow our members to learn and practice ethical hacking skills in a safe environment
- Create forum for practitioners to share techniques and mentor peers in this space

Jon Williams

Jon Williams

- Security Administrator

IGG Software

Banktivity

iggsoftware.com

Jon Williams

- Security Administrator

IGG Software

Banktivity

iggsoftware.com

- Security Researcher

braindead-security.blogspot.com
github.com/braindead-sec

...and you?

Objective

To raise awareness about threats to wi-fi users and techniques for defending against those threats.

Agenda

- Overview: wireless security concepts
- Demonstration: wireless attacks
- Review: risks to remote workers
- Game time: defensive techniques

CONNECT. LEARN. GROW.

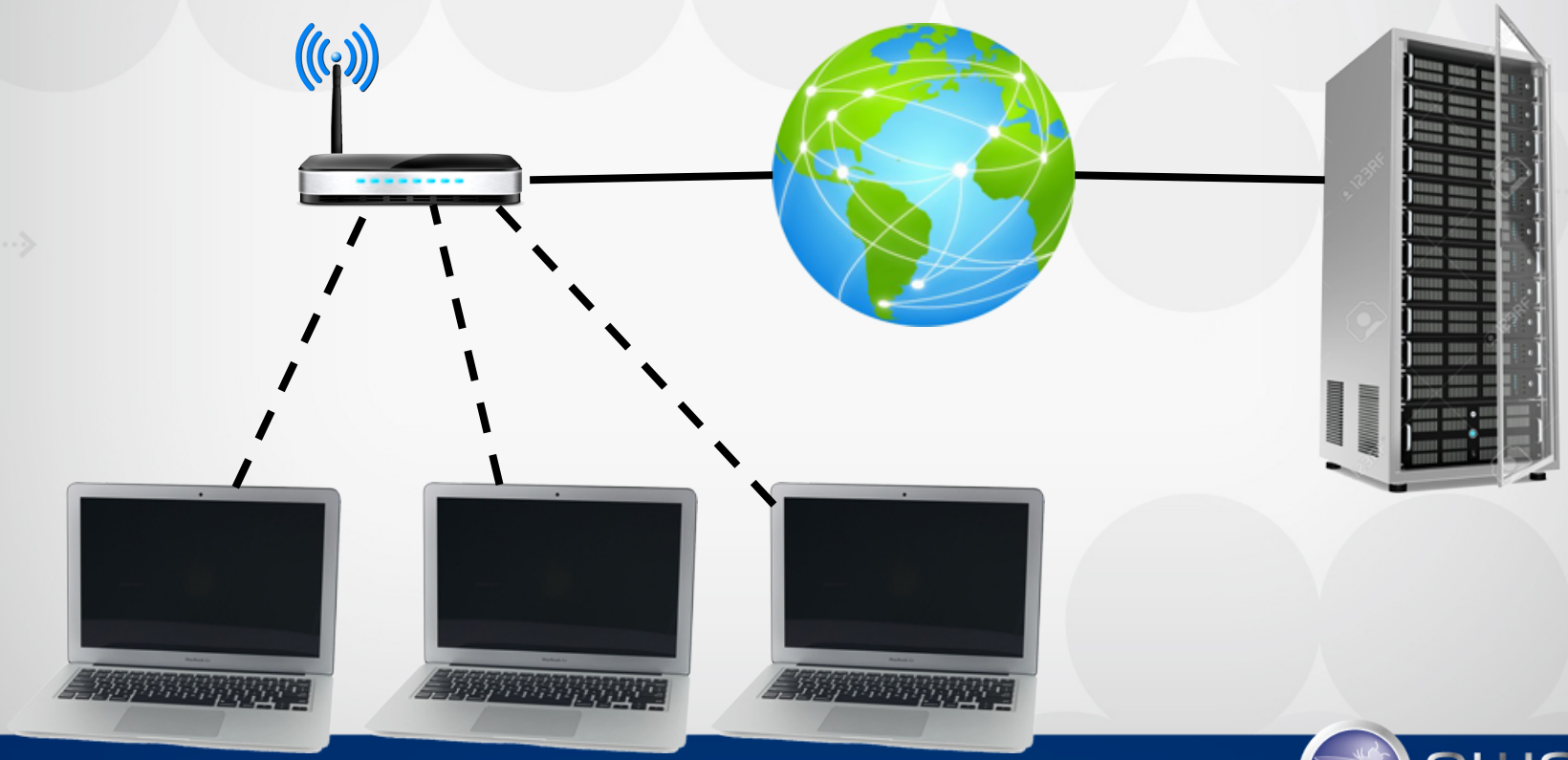
Overview

Wireless security concepts

The Million-Dollar Question

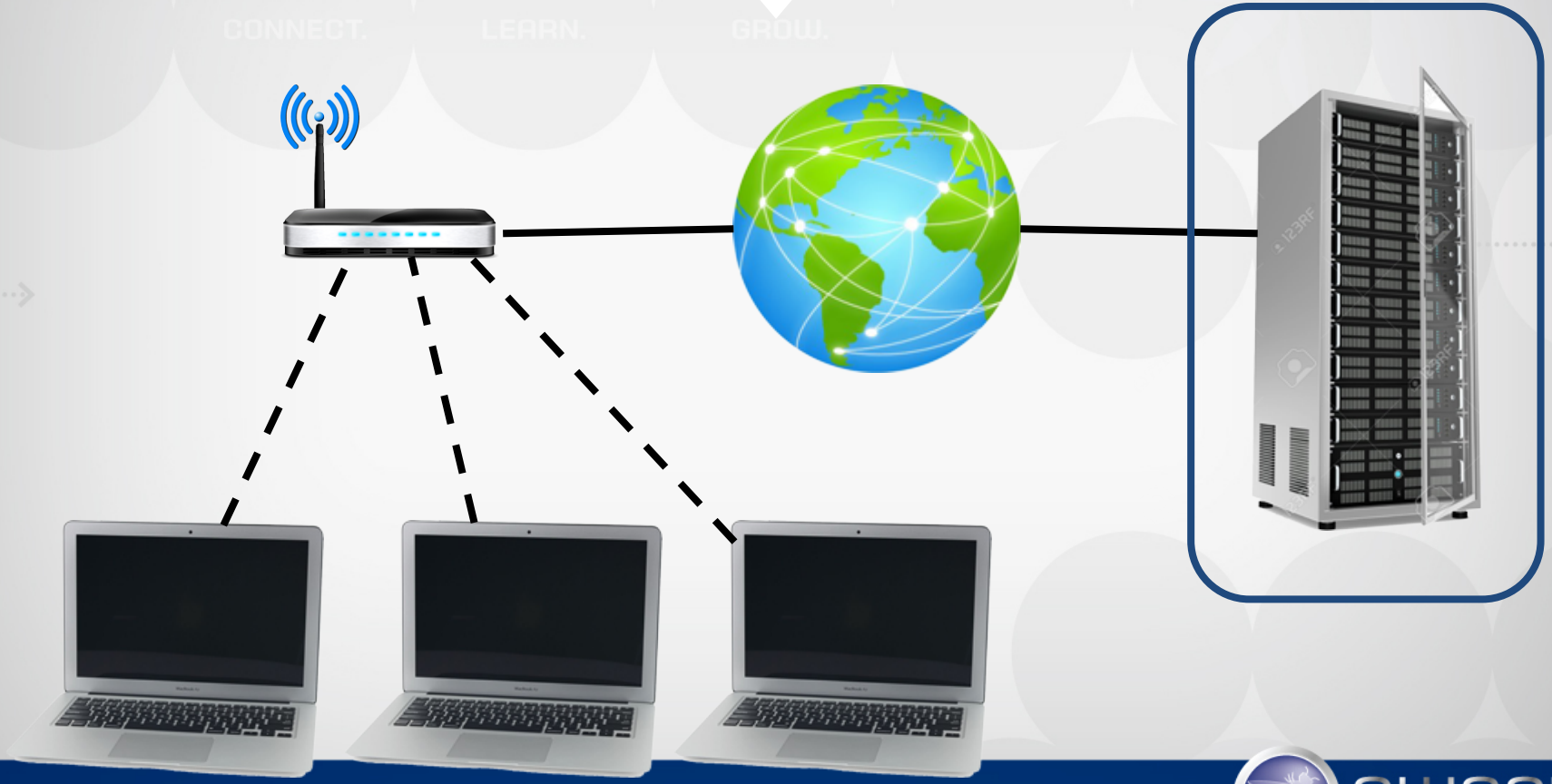
"What is my most valuable asset?"

Wireless Internet Access (simplified)



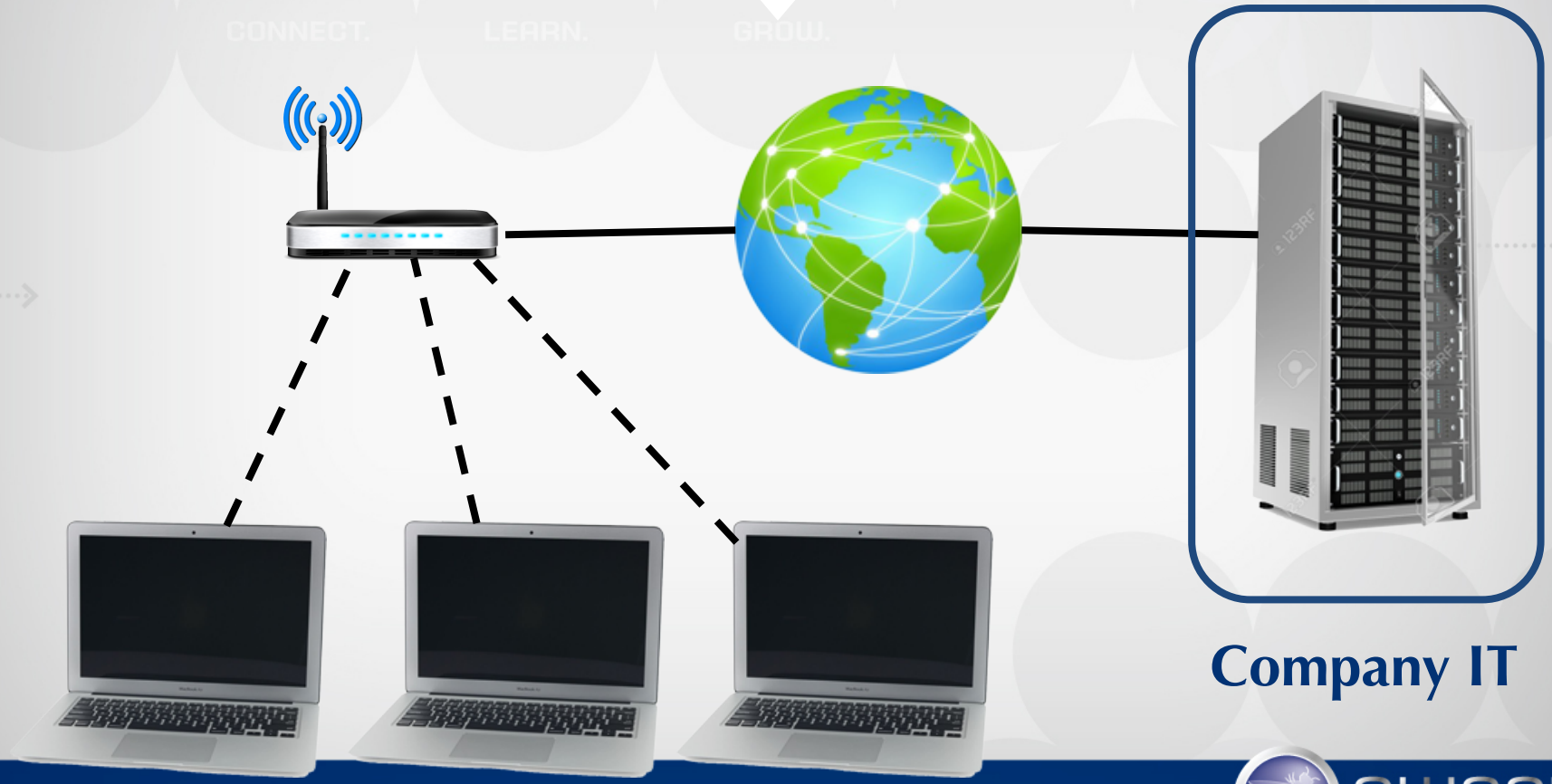
OWASP
Open Web Application Security Project

Wireless Internet Access (simplified)



OWASP
Open Web Application Security Project

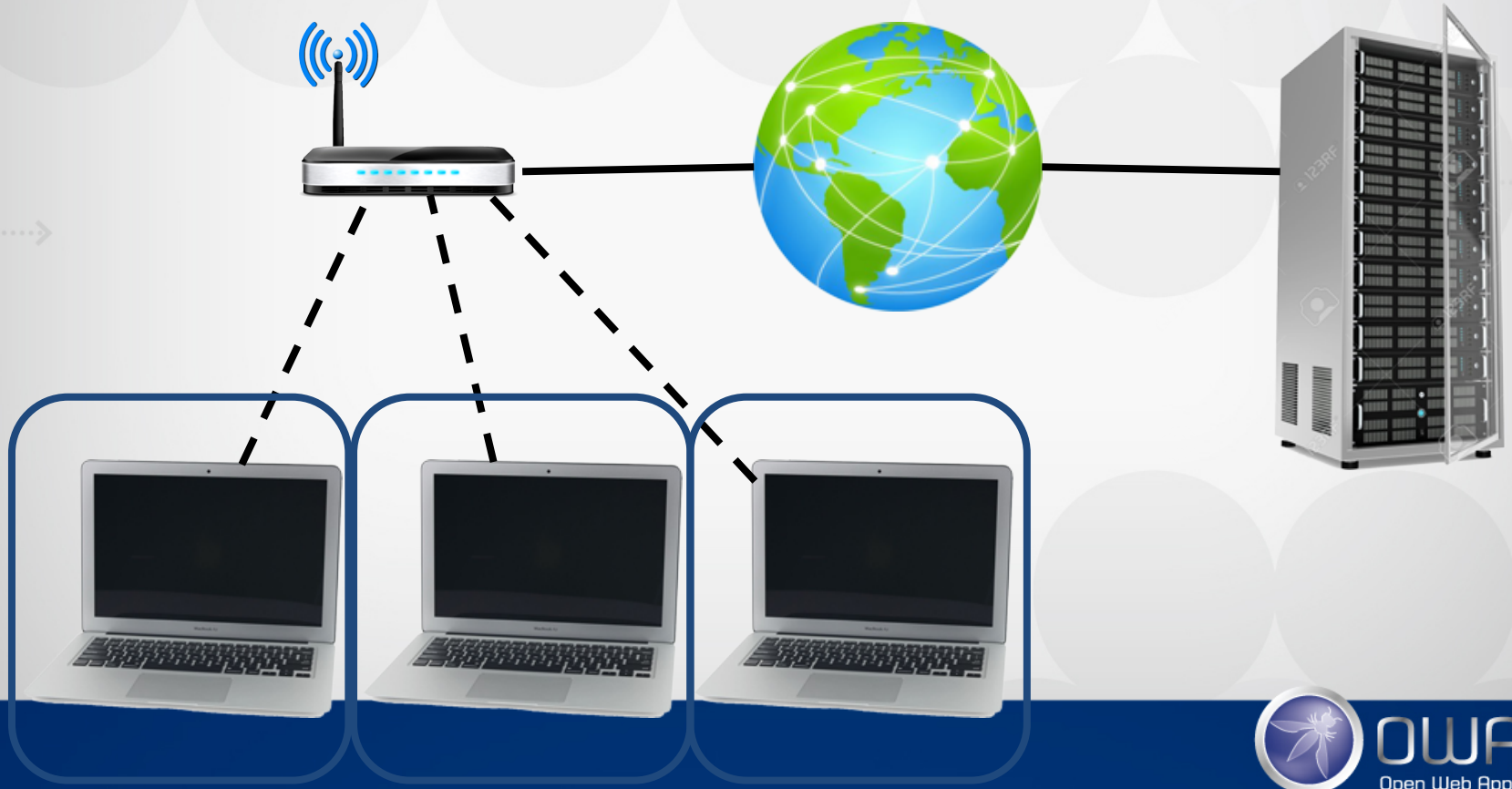
Wireless Internet Access (simplified)



Company IT

OWASP
Open Web Application Security Project

Wireless Internet Access (simplified)

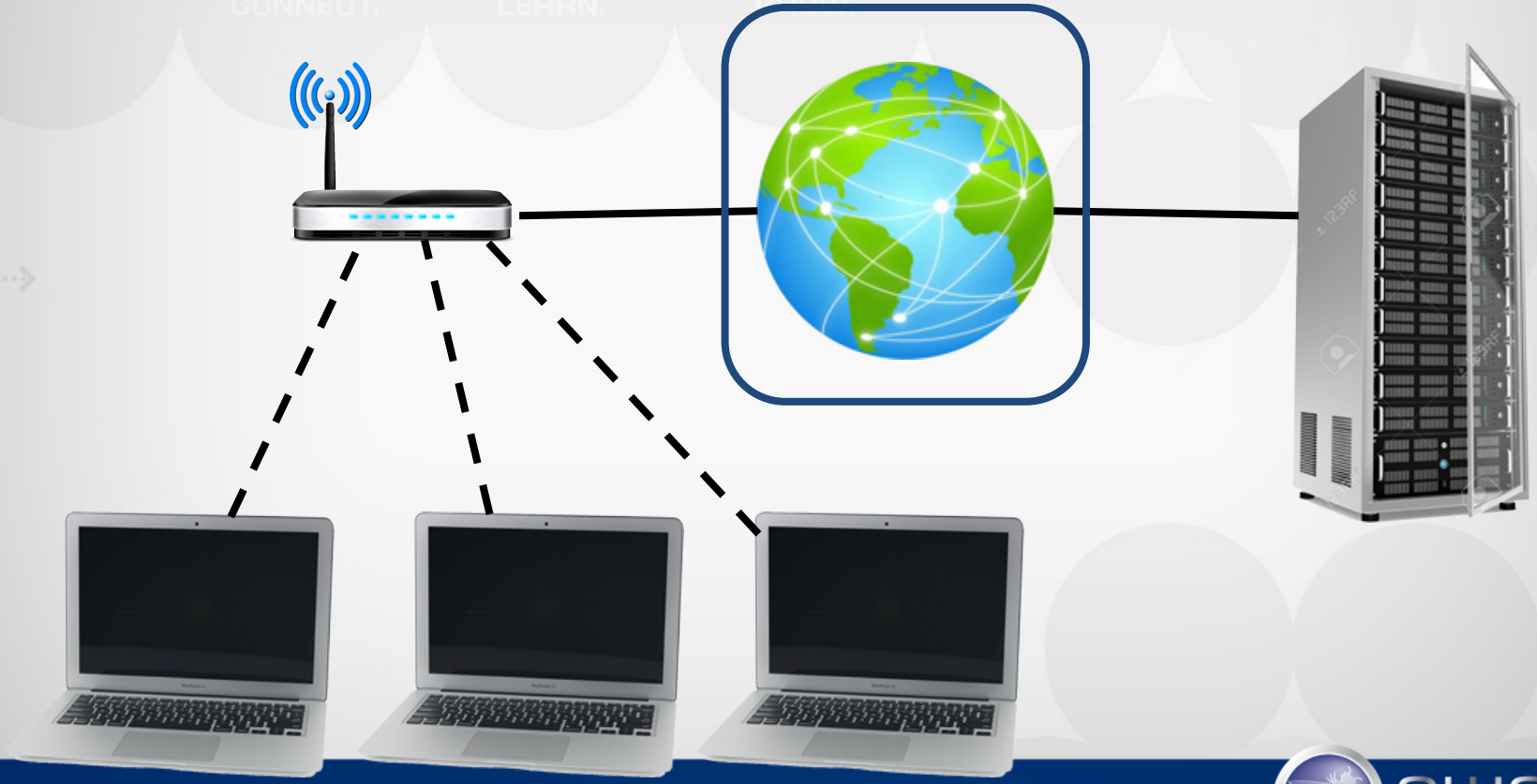


OWASP
Open Web Application Security Project

Wireless Internet Access (simplified)

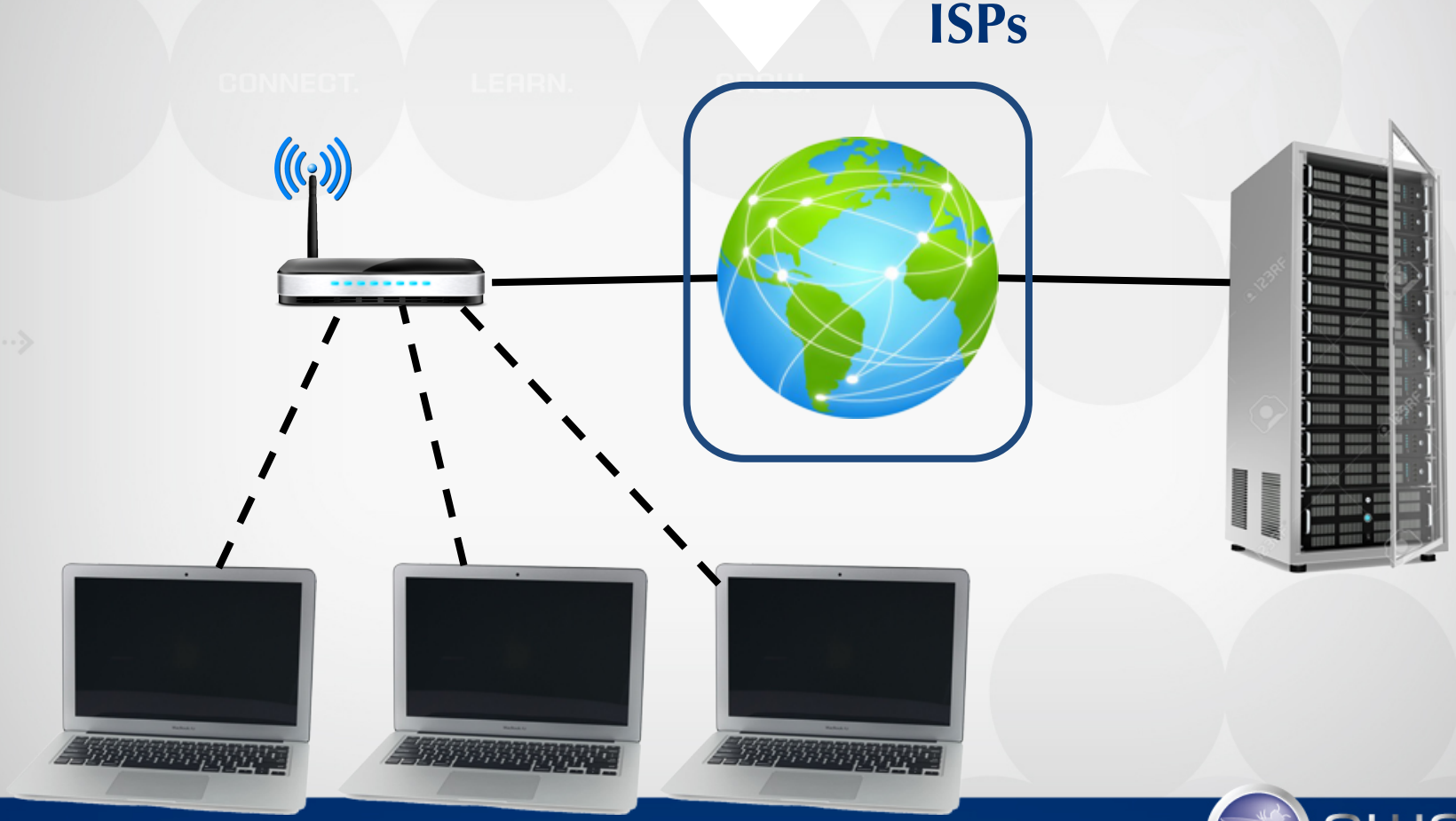
You (and your IT)

Wireless Internet Access (simplified)

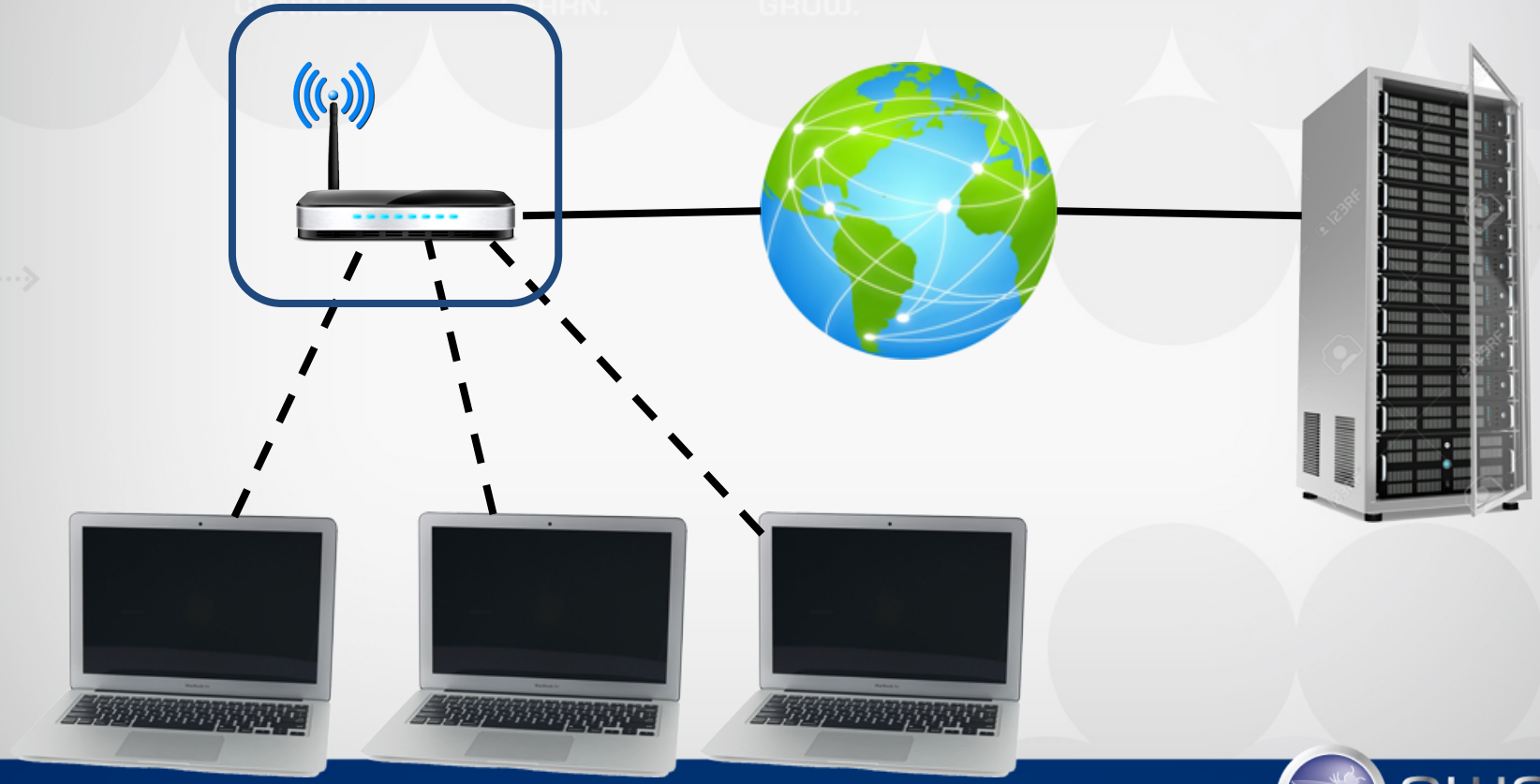


OWASP
Open Web Application Security Project

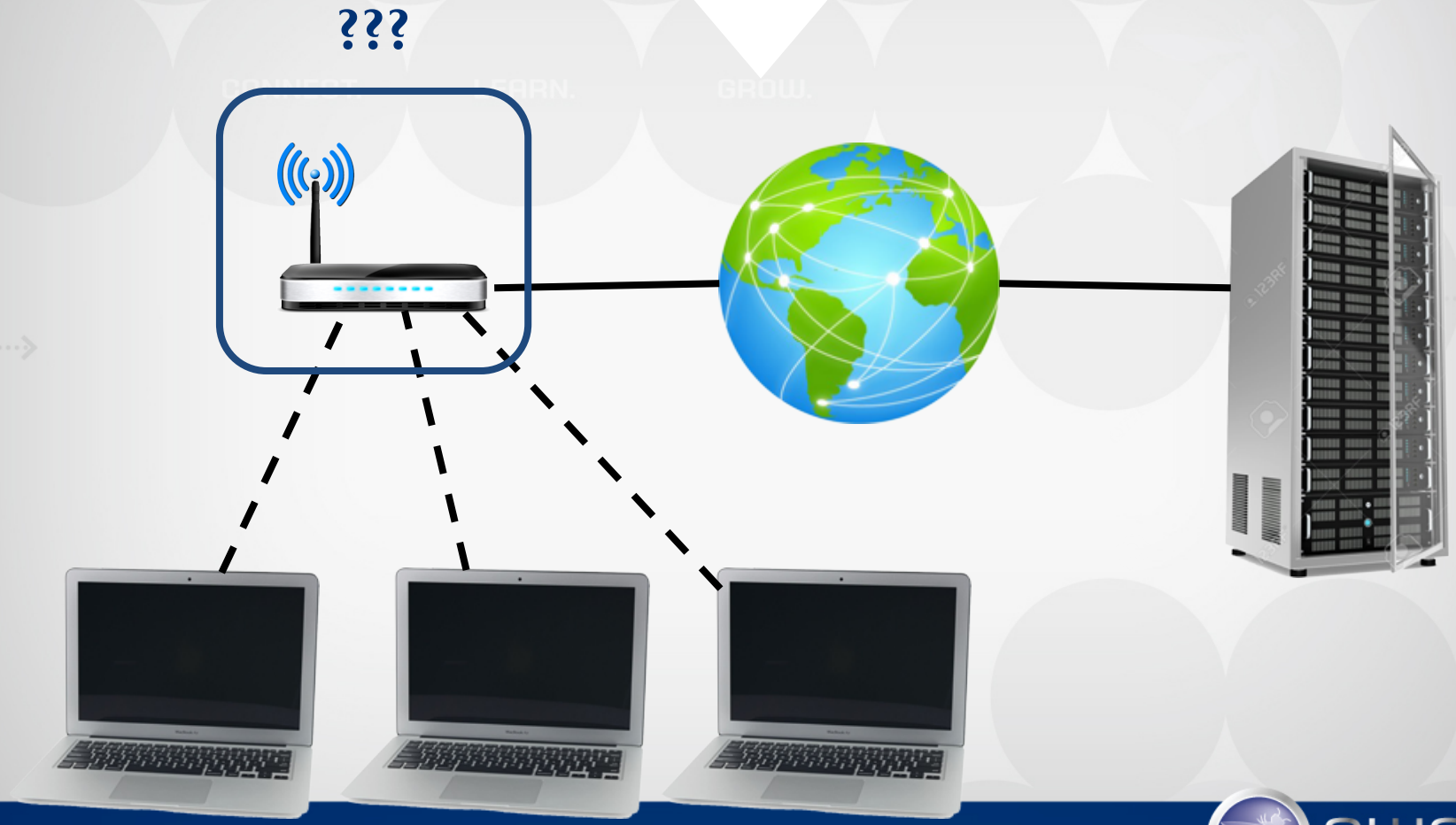
Wireless Internet Access (simplified)



Wireless Internet Access (simplified)

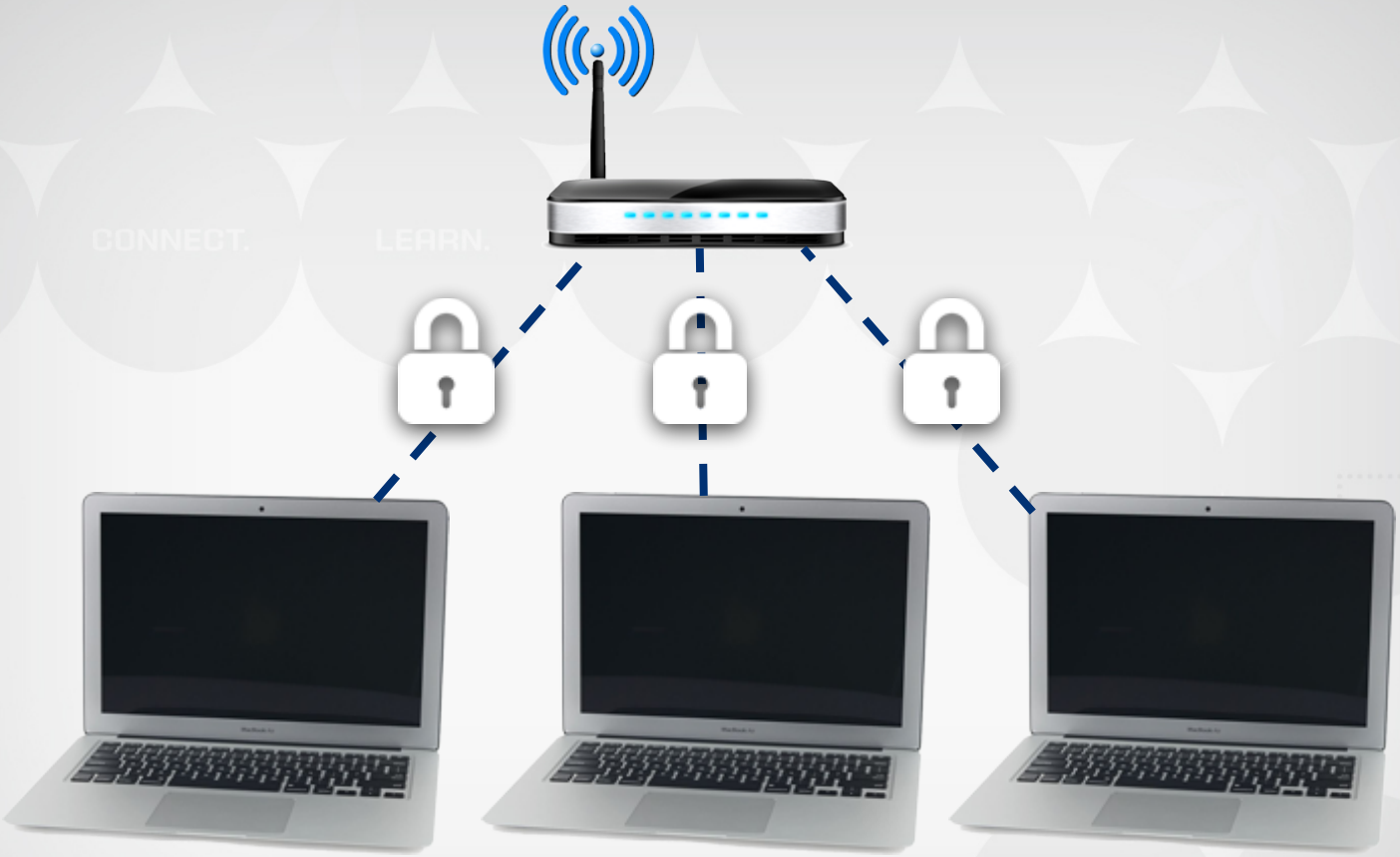


Wireless Internet Access (simplified)



Local Network - No Encryption

Local Network - With Encryption



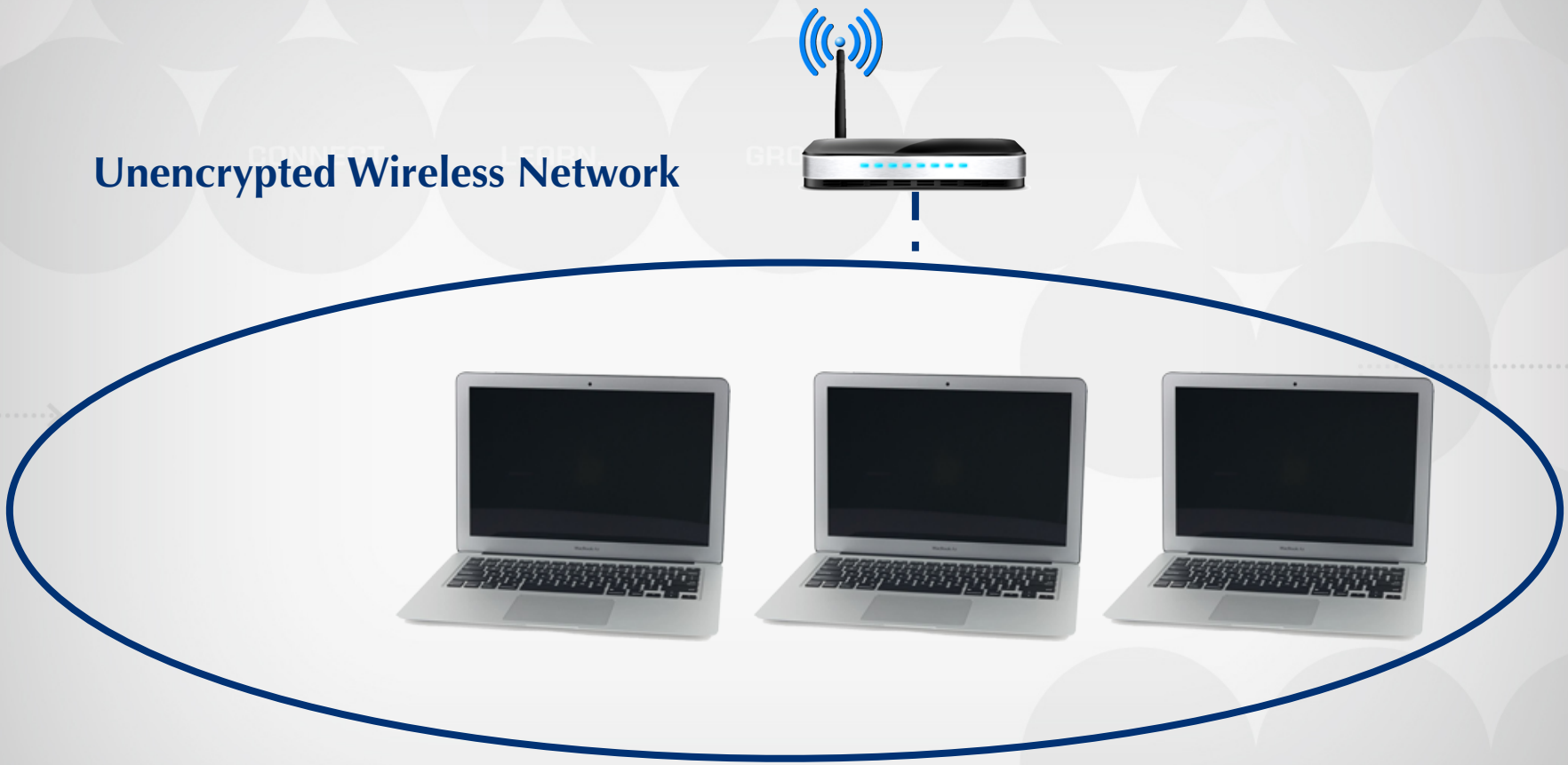
CONNECT. LEARN. GROW.

Wireless Attacks

Threats facing remote workers

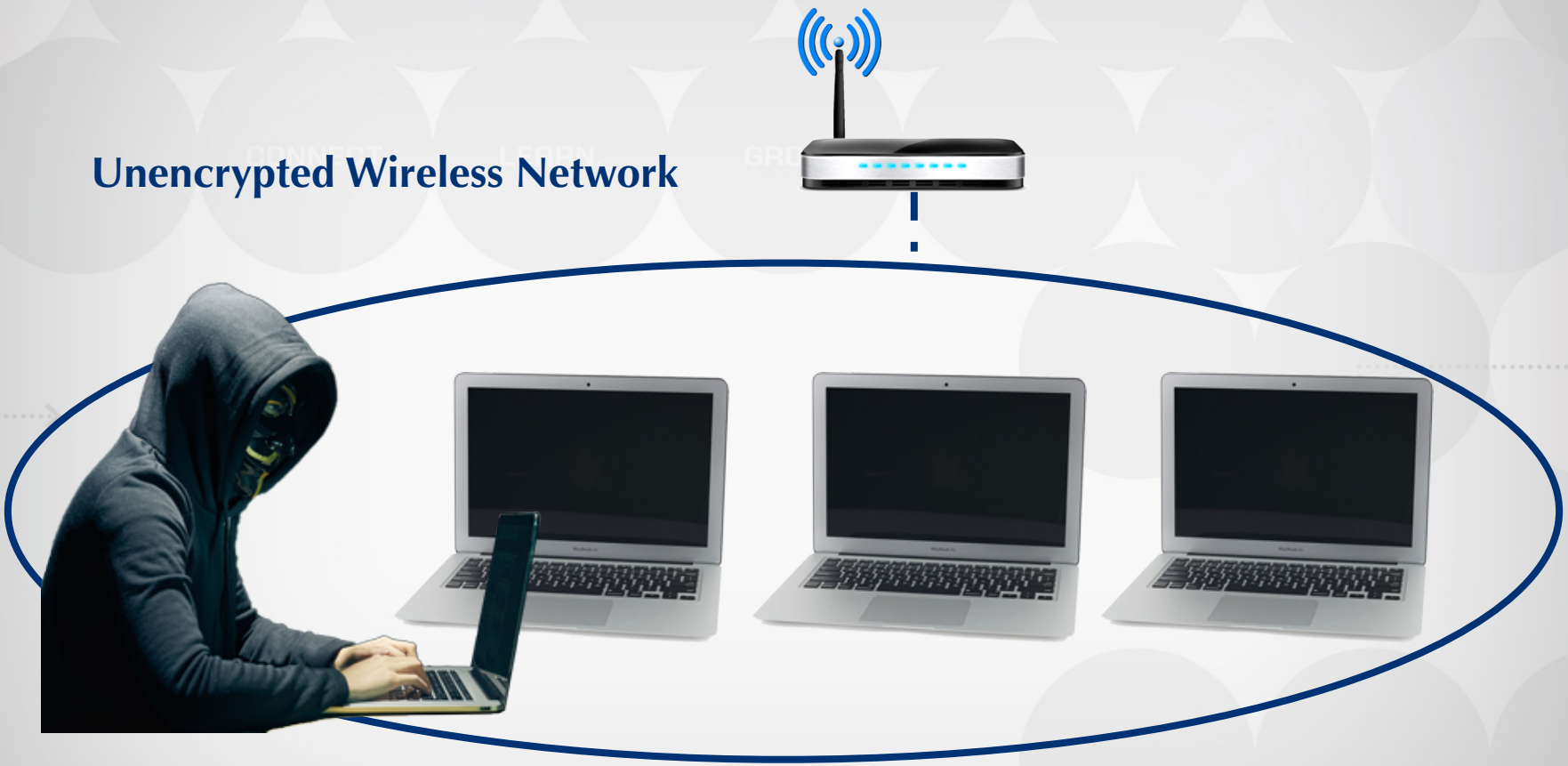
Radio Monitoring

Unencrypted Wireless Network

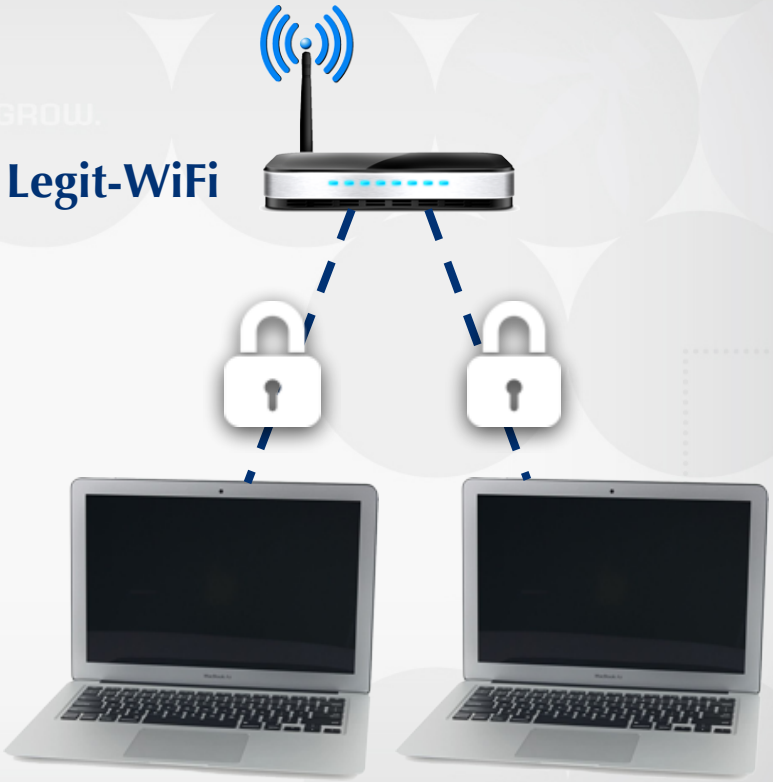


Radio Monitoring

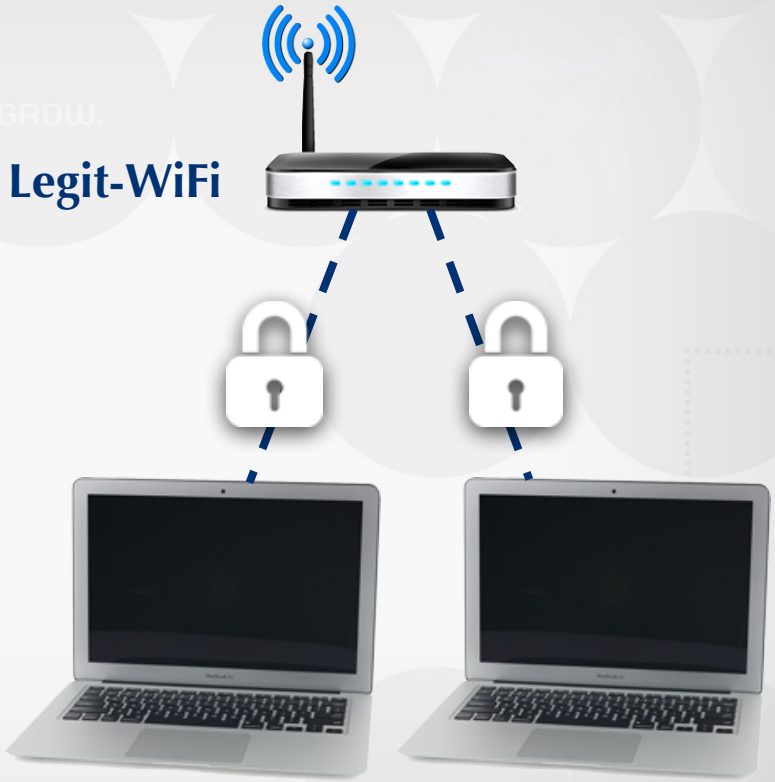
Unencrypted Wireless Network



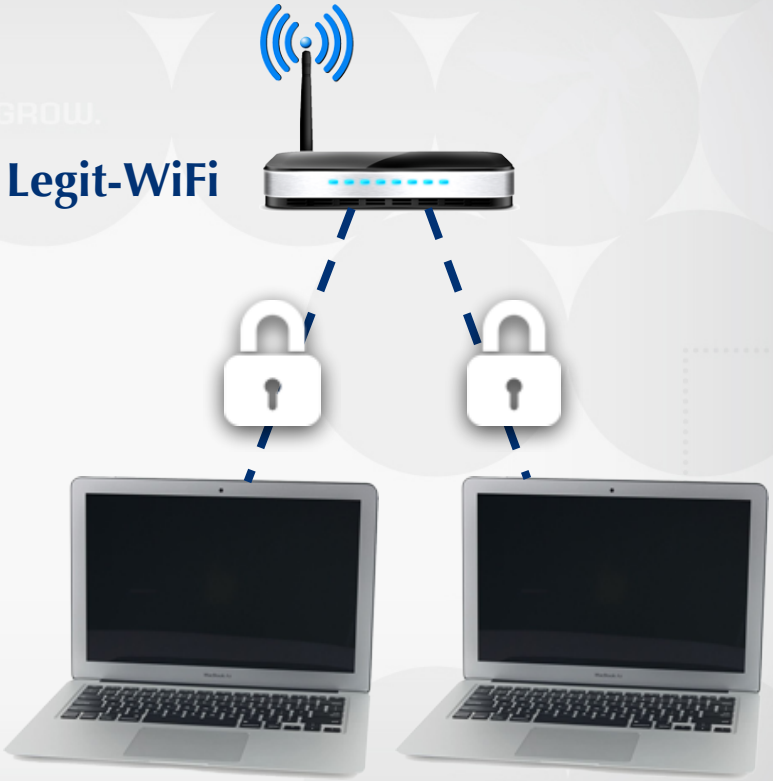
Rogue Access Point



Rogue Access Point

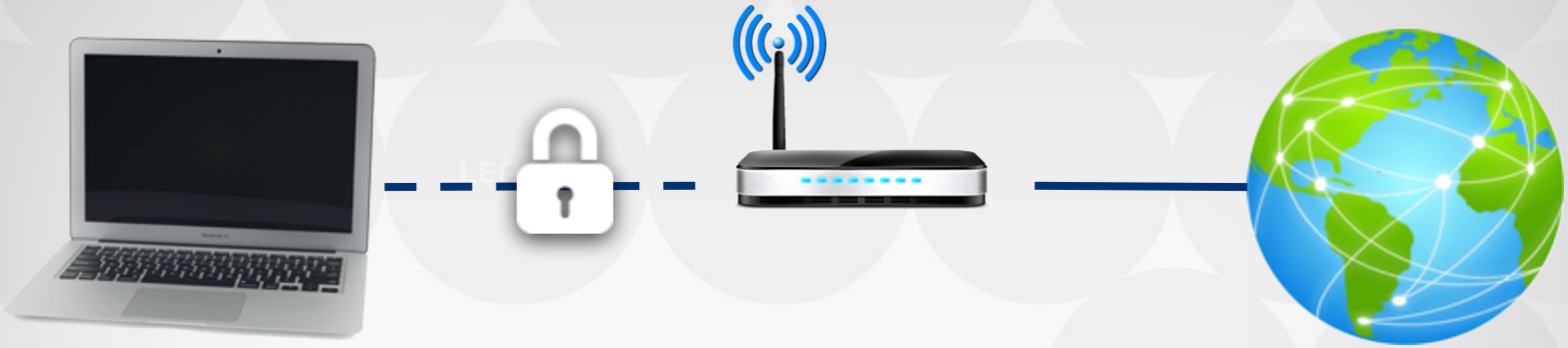


Rogue Access Point

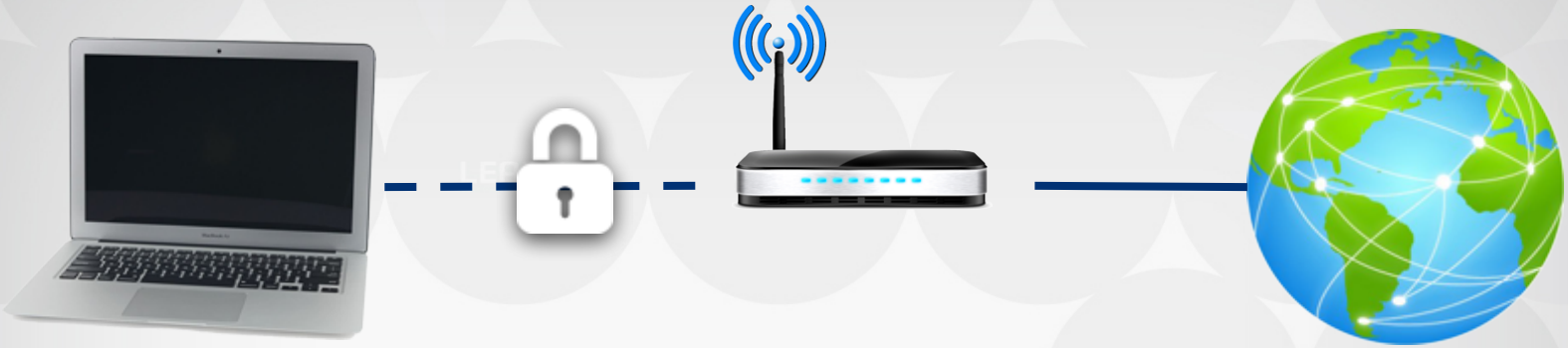


Rogue Access Point

Man-in-the-Middle



Man-in-the-Middle



Man-in-the-Middle

- Monitor
- Intercept
- Inject

Session Hijacking

1. Log in to website, get cookie
2. Browse site using cookie for authentication
3. Log out, remove cookie

Session Hijacking

1. Log in to website, get cookie
2. Browse site using cookie for authentication
3. Log out, remove cookie

2.5. Steal cookie, plant in browser, pretend to be authenticated user without logging in

Credential Theft

- Rogue access point
- Captive portal
- Fake login form

Credential Theft

- Rogue access point
- Captive portal
- Fake login form

- Looks legit
- Login fails
- Pwnd

Risk Review

- Unencrypted wifi
- Rogue access point
- Passive connections
- Evil twin ➤ man-in-the-middle
- Unencrypted login forms
- Password reuse
- Insecure cookies ➤ session hijacking

CONNECT. LEARN. GROW.

Game Time!

Mitigating risks

Any questions?

Thank you!

Stay safe out there.