Wireless Security

William Mitchell & Greg Cortazzo

Background

Common Challenges

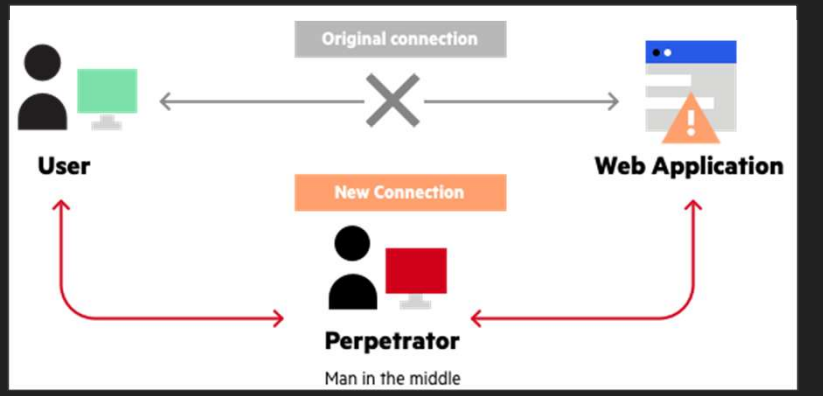
- Authenticating Clients
- Authenticating APs
- Maintaining ease of use
- Low-latency solutions

Image Source: https://www.iconfinder.com/icons/4399436/protection_security_wifi_icon

Potential Wireless Network Exploits

- Capturing private traffic
- Man-in-the-middle attacks
- Denial of service
- Network injection

MITM Attack



Picture Source:
http://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Common Security Designs

- End-to-end Encryption
- Network Passwords and Authentication Certificates
- Wireless Intrusion Prevention System (WIPS)

Image Source: https://www.acrylicwifi.com/blog/es-segura-red-wifi-wpa-wpa2/

Detecting Unauthorized APs

- Fake Access Points can infiltrate and harm a network
- Cryptographic techniques (like digital certificates) can often prevent these attacks
- AP fingerprinting can be used to accurately ID APs

Detecting Unauthorized APs - Existing Problems

- Fake APs can launch variety of attacks
- Traditional digital certificates techniques (802.11i RSNA)
  - Management of cert. across domains can be difficult
  - AP selection algorithm - (Strongest signal strength)
  - MAC spoofing
  - Taking down true AP with DOS attack
- Setting up a fake AP is relatively easy

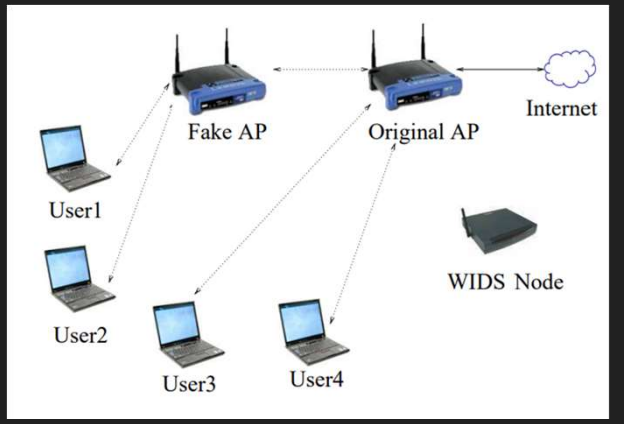


Photo Credit: https://www.cs.columbia.edu/~suman/docs/mobicom08-skew.pdf

Detecting Unauthorized APs - Approach

- Fingerprinting APs
- Clock skew
  - Product of the variation between hardware clocks.
  - Unique to the silicon in the AP
- Clock skew detection
  - Capture AP periodic beacons (Use Timer Sensitive Function: TSF Field)
  - Track clock skew using (Linear Programming Method or Least Squares Fitting)
- WLAN intrusion detection system (WIDS/WIPS node)

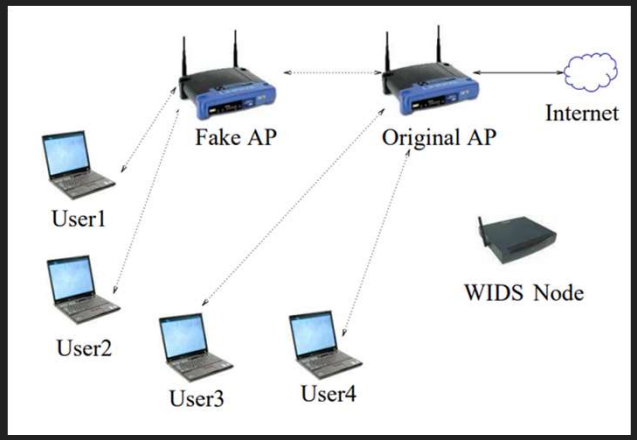


Photo Credit: https://www.cs.columbia.edu/~suman/docs/mobicom08-skew.pdf

Detecting Unauthorized APs - Challenges/Risks

- Requires pre-authorized APs
- Temperature can affect clock skew
- Virtual Access Points share same skew
- Spoofing the Clock Skew attack
  - If True AP is active: Fake beacons arrive offset from true beacons (detectable)
  - If True AP is not active: Not possible with current drivers (potential problem)

Detecting Unauthorized APs - Benefits+Results

- Low overhead
  - Capturing beacons
  - Requires a WIPS node
- Fast detection
  - In the realm of seconds
- Highly accurate
  - Data shows clock skew derivation is consistent
  - Clock skew itself its relatively consistent
- Difficult to fake clock skew

Geofencing Security - Key Idea

- Real-world physical boundaries to secure Wi-Fi
- Use of overlapping AP regions for well-defined regions
- As small as 5’x5’ regions

Green: Actual wifi coverage
Magenta: Desired coverage

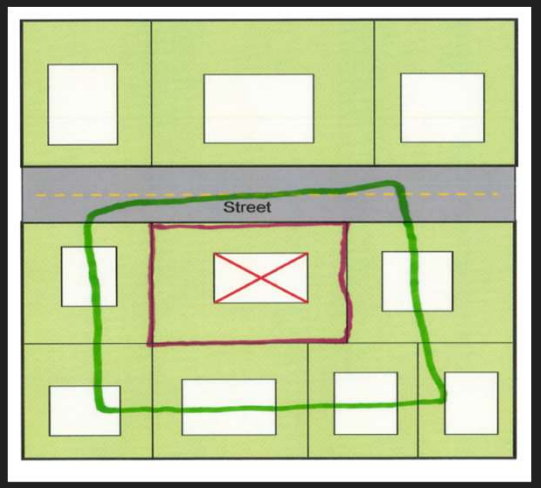


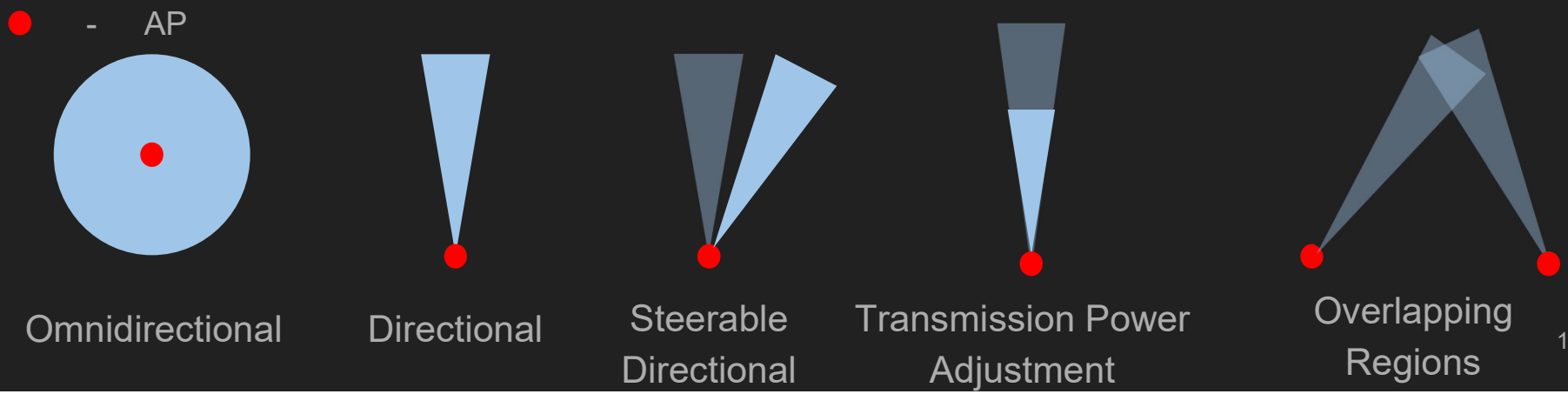
Photo Credit: Sheth A., Seshan S., Wetherall D. (2009) Geo-fencing: Confining Wi-Fi Coverage to Physical Boundaries. In: Tokuda H., Beigl M., Friday A., Brush A.J.B., Tobe Y. (eds) Pervasive Computing. Pervasive 2009. Lecture Notes in Computer Science, vol 5538. Springer, Berlin, Heidelberg

Geofencing Security - Existing Problems

- Signals overly-accessible
- Encryption is not enough
  - Side channel attacks
- Unnecessary interference
- Unmanaged networks
  - Persistent clients on network (Coffee shop example)
  - Security Updates
- Ease of access

Geofencing Security Approach

- Steerable Directional Antennas
- Adjusting transmission power
- Overlapping Regions
  - Code packets between APs
- Minimum Overlap Heuristic and Dense Fingerprinting approaches



Geofencing Security - Sample Results

- Dense fingerprinting is best
- Directional outperformed omni
- Smaller target regions (desk sized)

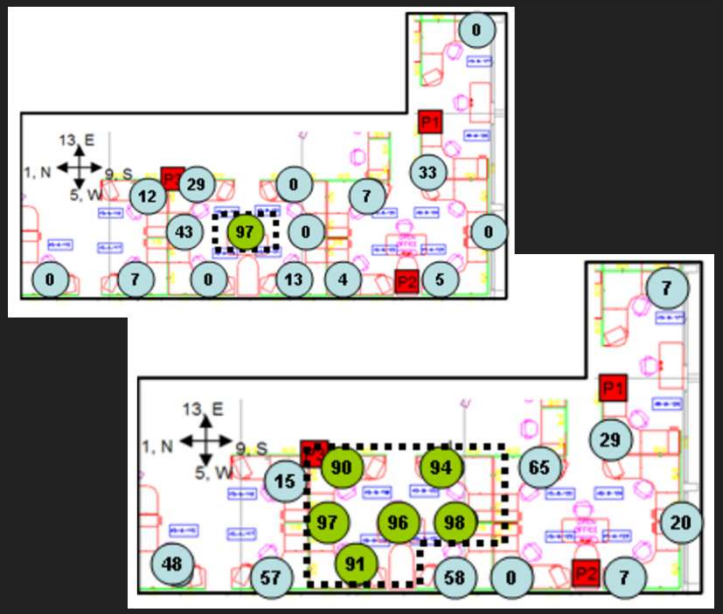


Photo Credit: Sheth A., Seshan S., Wetherall D. (2009) Geo-fencing: Confining Wi-Fi Coverage to Physical Boundaries. In: Tokuda H., Beigl M., Friday A., Brush A.J.B., Tobe Y. (eds) Pervasive Computing. Pervasive 2009. Lecture Notes in Computer Science, vol 5538. Springer, Berlin, Heidelberg

Geofencing Security - Concerns/Challenges

- Configuring effective setup
  - Additional costs: extra APs, stricter hardware requirements, physical boundaries enforcement
  - Setup requires higher skill
  - Updating/managing the geofence just as difficult as initial setup
- Attacks
  - Failure of physical boundary
  - High-gain directional antenna attack
- Quality of service
- Not all data necessarily protected by physical boundaries
- Changes in environment (physical and interference)

Geofencing Security - Benefits

- Physical boundaries already in place
- Additional security / low security applications
- Usefulness of hardware upgrades

Future:

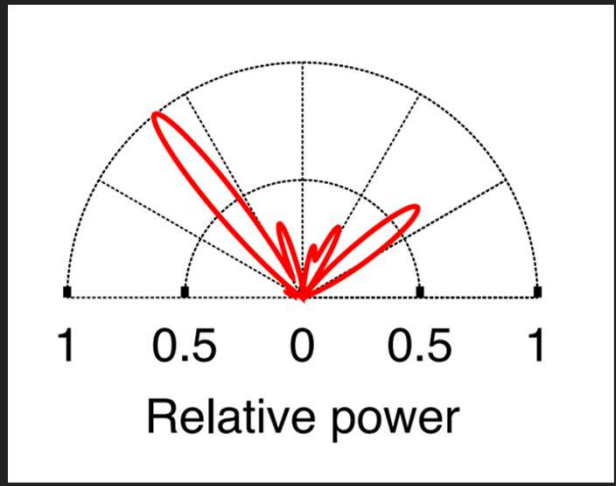
- IoT
- Smart homes
- Easy additional security measure

SecureArray

SecureArray - Key Ideas

SecureArray analyzes the power of a packet with respect to the angle of arrival (the “AoA spectrum”) to determine authenticity

In theory, each host has a uniquely identifiable fingerprint determined by antenna setup and signal propagation



SecureArray - Existing Problems

Security protocols are slow to be adopted and quicker to be broken

Since attackers can generate arbitrary data streams, spoofing is effective against many security protocols

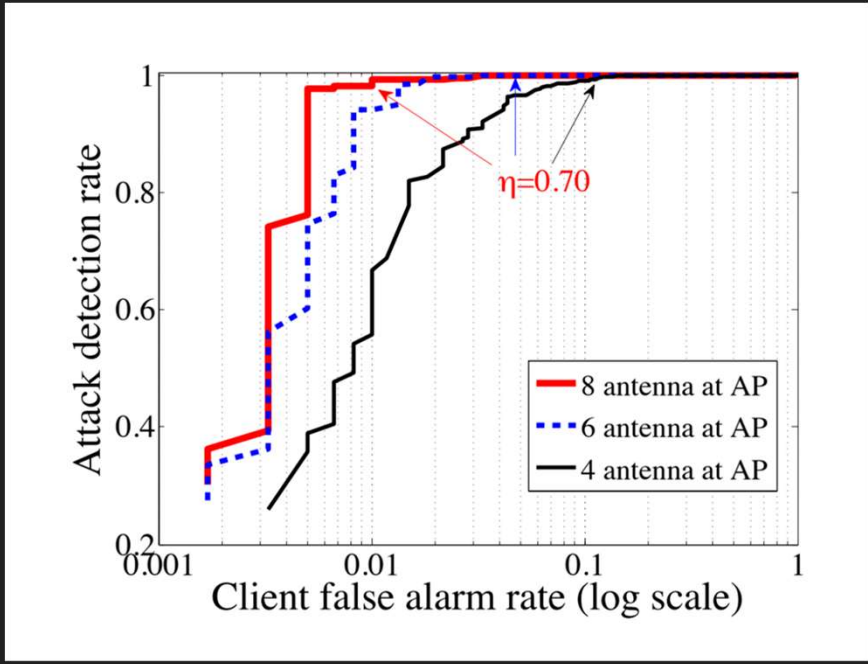
Some location-based security protocols can be spoofed with specialized antenna setups

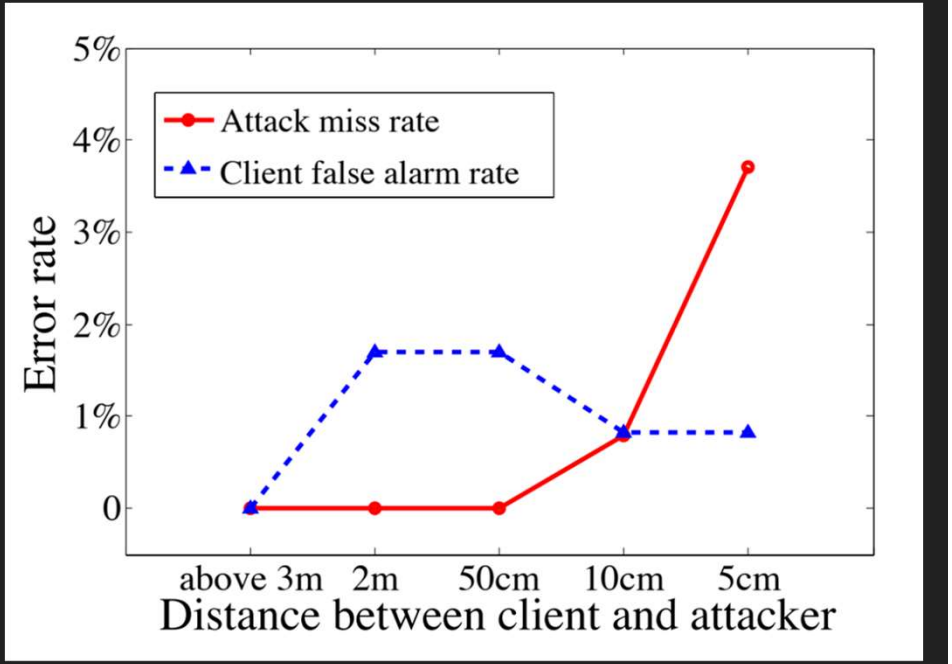
SecureArray - Sample Results

Attacker was placed in a busy office area and attempted spoofing attacks

Against both stationary and mobile hosts, detection rate was 100% (1500 comparisons) and false positives appeared for 0.6% of traffic

SecureArray - Sample Results





SecureArray - Takeaways

SecureArray provides an extra layer of authentication that’s very difficult to spoof

Attacker would need to read fingerprints from the location of the AP and then also spoof them from the location of the user

SecureArray - Challenges/Risks

Latency during the experiment was about 20ms; expected to be “orders of magnitude” faster in a final FPGA design

Hardware dependent: older APs with fewer antenna are less effective for this protocol

Fingerprint must be established using about 10 data points before it can be checked against incoming traffic

SecureArray - Opportunity

Relatively unexplored security idea in industry

Could represent a difficult-to-attack extra layer of authentication

Mitigates spoofing attacks greatly

Further Research / Sources

Geo-fencing: Confining Wi-Fi coverage to physical boundaries, International Conference on Pervasive Computing, 2005, Springer.

SecureArray: Improving WiFi Security with Fine-Grained Physical-Layer Information, ACM Mobicom 2013

On fast and accurate detection of unauthorized wireless access points using clock skews. ACM MobiCom, 2008

Questions?