Wireless Security

By Ananya Chandra and Josh Goldstein

Overview

1. Why Wireless Security?
2. Types of Attacks
    a. MAC Spoofing - Clock Skew Estimation
    b. Denial of Service - SecureArray
3. Current Security Measures
    a. Key Sharing - SafeSlinger
4. What Does the Future Hold?

Why Wireless Security?

- The world will have 30 billion wirelessly connected devices by 2020
- An increasing number of our systems are connected wirelessly
    - Energy Grid
    - Planes
    - Door locks!
- Wireless communications are public in nature

Why Wireless Security?

Wired Security

- Communication travels within a shielded copper cable
- Network is completely contained
- Must physically connect to the network to obtain information
- A single compromised node in the network can compromise the entire network

Wireless Security

- Wireless radio frequency communication travels through open air
- Anyone can capture and record information travelling through a wireless network
- A single compromised node in the network can compromise the entire network

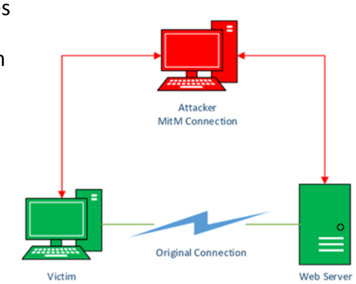
Types of Attacks

- Man in the Middle (MitM)
- MAC Spoofing
- Denial of Service (DoS)

Man in the Middle

Definition: the attacker poses as an access point and forwards packets to/from the user

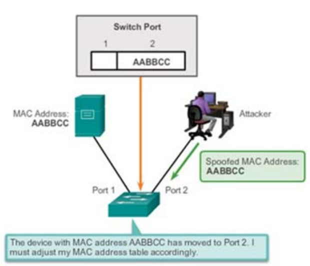
Purpose: allows attackers to intercept and modify information sent in the network



MAC Spoofing

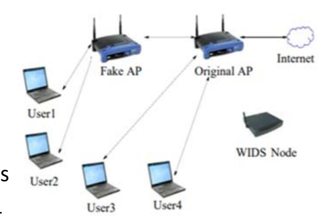
Definition: transmission of packets with the MAC address of a different user

Purpose: allows attackers to transmit packets over a network with the address information of an authorized user



Clock Skew Estimation: Problem Summary

- AP selection algorithms use signal strength as the only criteria
- Attacker can set up fake APs with the same MAC address as the real AP, but with different physical characteristics

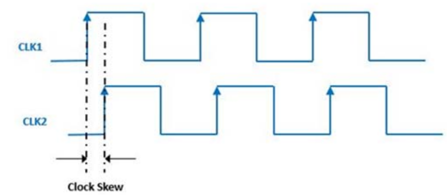


On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews

Suman Jana, University of Utah
Sneha K. Kasera, University of Utah

Clock Skew Estimation: How it Works

- Proposed solution - use clock skew to fingerprint APs
  - Beacons transmit packets from APs regularly
  - User records offsets between TSF timestamps of received packets to estimate clock skew

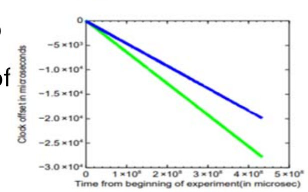


Clock Skew Estimation: How it Works

- Microsecond resolution clock records times received
- Assumes linear offset times
- Uses least square fitting to find line of best fit - slope of line is clock skew estimate

$$o_i = (T_i - T_1) - (t_i - t_1)$$

$$\sum_{i=1}^{n}(o_i - (\delta.x_i + \phi)^2)$$



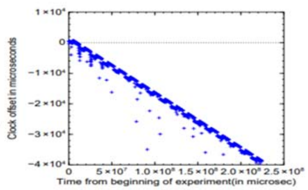
Clock Skew Estimation: How it Works

- Estimates require 50-100 packets to stabilize
- Clock skew is consistent for a particular AP
- Clock skew varies greatly across APs

AP	1st Measurement(LPM)	1st Measurement(LSF)	2nd Measurement(LPM)	2nd Measurement(LSF)
Linksys1	-64.23 ppm	-64.10 ppm	-64.90 ppm	-64.77 ppm
Linksys2	-45.69 ppm	-45.96ppm	-46.94 ppm	-46.71 ppm
Linksys3	-62.05 ppm	-61.84 ppm	-62.77 ppm	-62.64 ppm
Belkin1	-56.37 ppm	-56.57 ppm	-56.71 ppm	-56.85 ppm
Belkin2	-1105.50 ppm	-1105.69 ppm	-1106.29 ppm	-1106.06 ppm
Netgear1	-58.08 ppm	-57.78 ppm	-58.86 ppm	-59.25 ppm
Dlink1	-47.27 ppm	-47.17 ppm	-47.80 ppm	-48.14 ppm
Unknown1	-40.91 ppm	-40.99 ppm	-41.61 ppm	-41.47 ppm

Limitations of Clock Skew Estimation

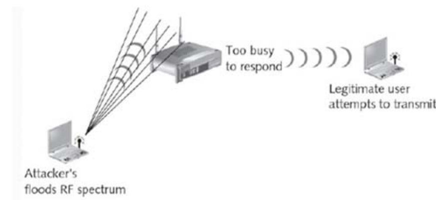
- Assumes constant data rate and clock skew for the receiving device
- Assumes that the fake AP cannot forge timestamps to align with the real AP's clock skew



Denial of Service

Definition: the flooding of a network with packets, preventing authorized users from transmitting

Purpose: allows attackers to observe handshake codes on network restart, could relay packets from jammed users



SecureArray: Problem Summary

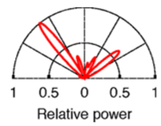
- WPA allows for injection attacks - attacker injects a frame into the network, leading to Denial of Service
- Security protocols can be compromised when shared secrets can be exposed
- Users need a procedure to uniquely identify other network participants

SecureArray: Improving Wifi Security with Fine-grained Physical Layer

Jie Xiong, Singapore Management University

Kyle Jamieson, University College London

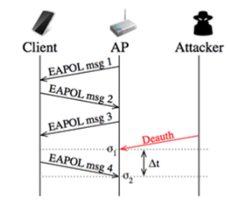
SecureArray: How it Works



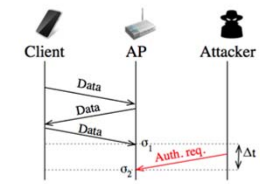
- SecureArray leverages modern access points that exploit MIMO through the use of multiple antennas and spatial division multiplexing
- An Angle of Arrival signature is established between a client and an Access Point to profile direction of signal received
  - AoA signature is detailed due to multipath effects

SecureArray: Mitigating Attacks

Deauthentication Deadlock



Authentication Deadlock

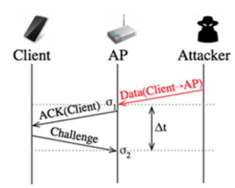


- Attacker leverages WPA weaknesses
- AP engages in AoA signature comparisons of local maximas when attack is suspected

SecureArray: Mitigating Attacks

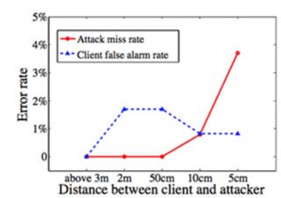
Authenticated Mac Address Spoofing

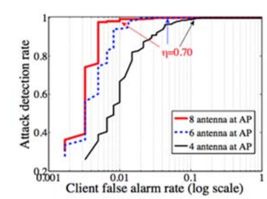
- Attacker manages to be authenticated with AP, and can sniff Mac Address of another authenticated client and spoof it
- Uses **DataCheck** protocol to mitigate authenticated spoofing
  - Client detects unexpected ACK frame and challenges AP



SecureArray: Results

- 100% attack detection rate of WiFi spoofing attack and 0.6% false alarm rate in noisy office environment





Limitations of SecureArray

- Increased latency of the protocol with added overhead of the Angle of Arrival signatures
- Attacker can replicate Angle of Arrival signature by being in close proximity to the client (~ 5cm)

Current Security Measures

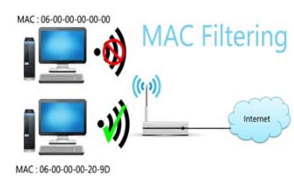
- SSID Hiding
- MAC Address Filtering
- Key Exchange Protocols: WPA

SSID Hiding

- Service Set Identifier (SSID) - 32 character sequence that uniquely identifies a WLAN
- APs broadcast their SSIDs by default
- SSID Hiding - SSID broadcasting is disabled, mandating clients to know SSID
- **Cons**: **Does not prevent malicious attackers from sniffing packets containing SSIDs**

MAC Address Filtering

- Defines a list of devices that are allowed on your WiFi network
- **Cons: Can easily be breached by MAC address spoofing**



Key Exchange Protocols: WPA

Wi-Fi Protected Access

- Four-way handshake with the Access Point to exchange shared key
- Uses Temporal Key Integrity Protocol
  - Uses **Dynamic Key Generation** - separate 128 bit key is generated for each packet transmission
  - **Message Integrity Code** - inserted to validate the message
- Uses the **Advanced Encryption Scheme** - advanced symmetric key generation algorithm

Key Exchange Protocols: WPA Weaknesses

- Injection Attacks - malicious code can be inserted into WPA protocol stack
- WPA lacks a **forward secrecy system**
  - Compromised keys can decrypt all subsequent packets
  - Key generation process is pseudorandom - brute-force testing

SafeSlinger: Easy-to-Use and Secure Public-Key Exchange

Michael Farb, CyLab / CMU
Yue-Hsun Lin, CyLab / CMU
Tiffany Hyun-Jin Kim, CyLab / CMU
Jonathan McCune, Google Inc.
Adrian Perrig ETH Zürich, CyLab / CMU

SafeSlinger: How it Works

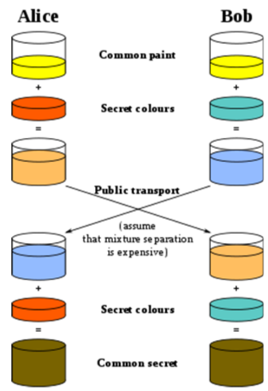
- iOS and Android application
- Enables secure communications between pairs or groups of users

(a) Secure Introduction feature panel for selecting recipients.

(b) Dialog displays chain of SafeSlinger exchanges from recipient to invitee.

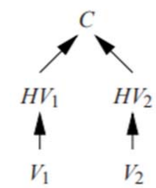
Diffie-Hellman Key Exchange

- Prime numbers p and g known
- Alice - makes private key a
- Alice - sends ($X = g^a$ mod p) to Bob
- Bob - makes private key b
- Bob - sends ($Y = g^b$ mod p) to Alice
- Alice - computes Y^a mod p
- Bob - computes X^b mod p
- Alice and Bob now have a shared secret key



SafeSlinger: How it Works

- Step 1: Multi-Commitment Generation
  - Each user creates a Diffie-Hellman private key
  - Key is encrypted and sent to the server



SafeSlinger: How it Works

- Step 2: Authenticity Verification
  - Server assigns IDs to each user
  - Users receive IDs and commitments from all other users
  - Each user must sort the decommitments by ID to generate 24-bit hash value
  - Hash value is inputted into the PGP word list to generate the correct 3-word phrase

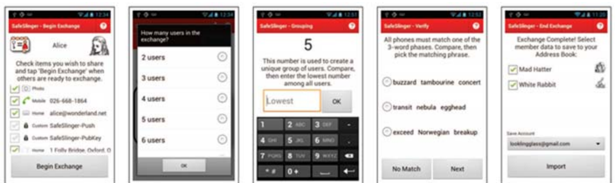
Hex	Even Word	Odd Word
00	aardvark	adroitness
01	absurd	adviser
02	accrue	aftermath
03	acme	aggregate
04	adrift	alkali

SafeSlinger: How it Works

- Step 3: Secret Sharing Round
  - Once all users have sent in the correct phrase, users can send their contact information encrypted with the shared group key
  - Users decrypt contact information and store it on their phones for future use

SafeSlinger: How it Works

- Includes an API to import specific user public keys from contacts on phone



(a) Data Selection (b) Counting (c) User Grouping (d) Word Phrase Comparison (e) Contact Data Import

Limitations of SafeSlinger

- Scalability - Key management between many groups of connections is logistically difficult
- Difficult to verify effectiveness - paper asked users how secure they felt using the application

	Easy to use min:1 max:5	Annoyance min:1 max:5	Security of app. min:1 max:5	Likely to use min:1 max:5
Bump	3.3 ± 1.4	**3.8 ± 1.1**	2.3 ± 1.1	2.4 ± 1.1
SafeSlinger	**4.2 ± 1.1**	2.1 ± 1.0	**$4.3 \pm .7$**	**3.6 ± 1.1**
T-test	$t(23) = 2.6,\ p = .015$	$t(23) = 6.1,\ p < .0001$	$t(23) = -7.6,\ p < 0.0001$	$t(23) = 5.1,\ p = .139$

What Does the Future Hold?

- The number of connected devices and communication paths will increase rapidly in the coming decades
- How do we secure networks against future attacks?
  - Restrict access
  - Isolate the network
  - End-to-end encryption

QUESTIONS?

References

http://www.netsec.ethz.ch/publications/papers/farb_safeslinger_mobicom2013.pdf

http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3704&context=sis_research

http://www.cs.columbia.edu/~suman/docs/mobicom08-skew.pdf

https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

https://www.scmagazine.com/understanding-common-wireless-lan-attacks/article/549838/

http://slideplayer.com/slide/7382216/

https://www.researchgate.net/figure/A-typical-Man-in-the-Middle-layout_fig3_307946535

https://www.slideshare.net/itsec/ch04-network-vulnerabilities-and-attacks

http://www.ciscopress.com/articles/article.asp?p=2351131

https://betanews.com/2016/08/30/password-is-dead/

https://searchsecurity.techtarget.com/WLAN-security-Best-practices-for-wireless-network-security