
Manna from Heaven:
Improvements in Rogue AP
Attacks
Defcon 22 2014
Ian de Villiers & Dominic White
22
DEFCON
sensepost

Disclaimer & Updates

These are an early version of our slides and the tools, our data and the slides will all be updated by the time of our Defcon talk. You can access these updates at:

- Slides http://slideshare.net/sensepost
- Tools http://github.com/sensepost/manna
- Overview http://www.sensepost.com/blog/

whois

Ian de Villiers & Dominic White
Hackers @ SensePost

We
Hack | Build | Train | Scan
Stuff

@iandvl & @singe

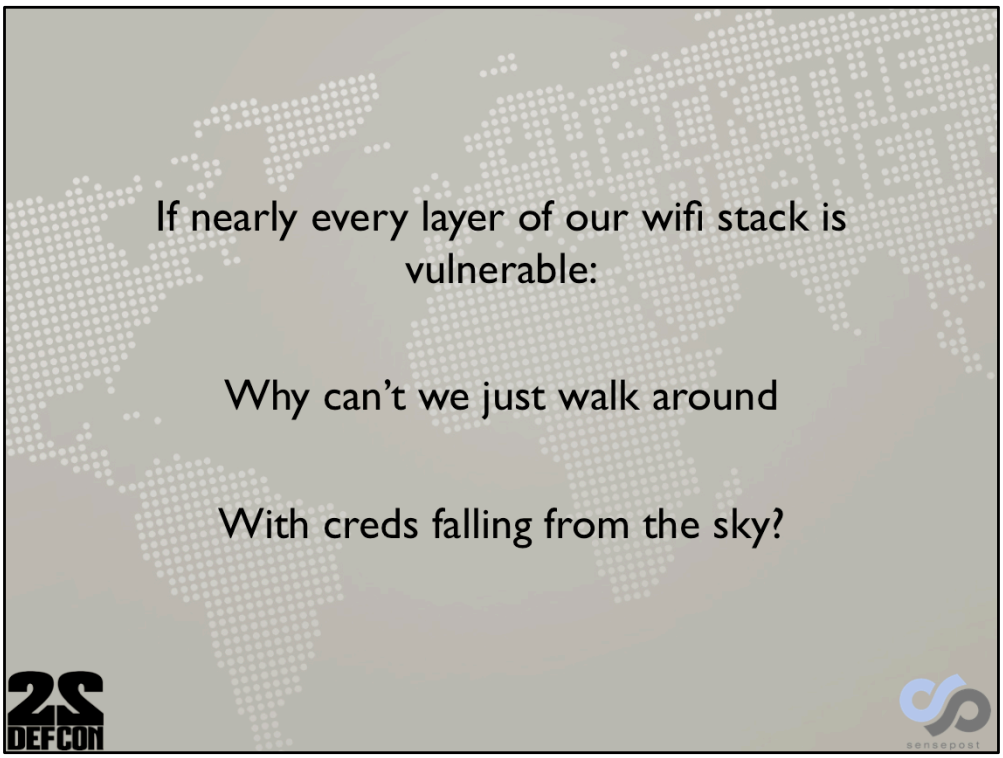
{ian|dominic} @sensepost.com
info/research/jobs @sensepost.com

Why Wi-fi?

- 800 million new devices each year
- Consumer standard for mobile devices
- Widely deployed
  - City-wide projects
- Increase in "cloud" services use & deployment
  - E-mail, Social Networking
- Directly correlates to target (user, home or org)

The State of Wifi Hacks

- We can get devices to connect to Rogue Aps
  - KARMA by Dino Dai Zovi & Shane Macaulay 2004
    - http://www.wirelessdefence.org/Contents/KARMAMain.htm
- We can intercept & crack auth creds to networks
  - coWPAtty by Joshua Wright 2004
    - http://www.aircrack-ng.org/doku.php?id=aircrack-ng&DokuWiki=1d69bf65c0a318129fd5a94a62b344cc
  - Freeradius-wpe by Joshua Wright and Brad Antoniewicz 2008
    - http://www.willhackforsushi.com/?page_id=37
  - Asleap then CloudCracker Josh Wright 2003 then Moxie Marlinspike 2013
- We can intercept creds over the network
  - Firesheep Eric Butler 2010
    - http://codebutler.com/firesheep/
  - Hamster & Ferret Errata Rob 2007
    - http://blog.erratasec.com/2007/08/sidejacking-with-hamster_05.html
  - dsniff Dug Song 2000
    - http://www.monkey.org/~dugsong/dsniff/
- We can downgrade/intercept SSL
  - sslstrip & sslsniff Moxie Marlinspike 2009
    - http://www.thoughtcrime.org/software/sslstrip/


If nearly every layer of our wifi stack is vulnerable:
Why can't we just walk around
With creds falling from the sky?
DEFCON
sensepost

Let's fix that

This talk will cover

- Improvements in rogue AP attacks
- Extensions to support secure networks
- Improvements in MitM
- Integration of existing attacks into a single tool

- Release of MANA toolkit
  - MitM and Authenticated Network Attack toolkit

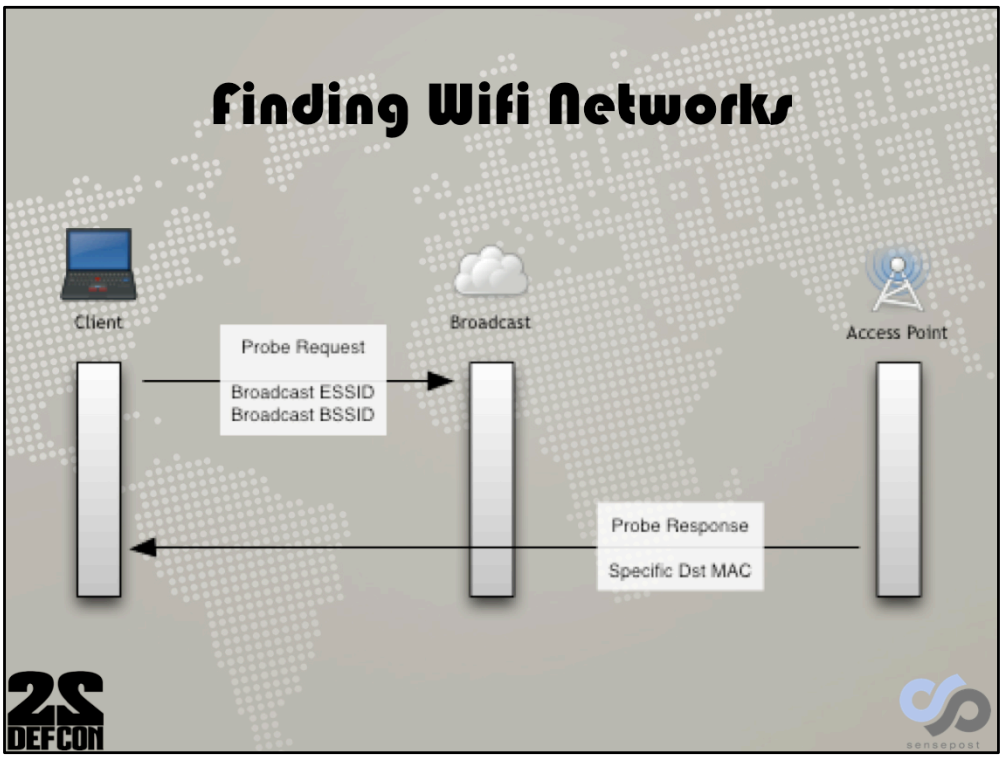
A Wifi Primer

- Wireless Fidelity (brand from Wi-Fi Alliance)
- Extension of wired Ethernet protocol 802.11<x> a/b/g/n/ac
- A plethora of wireless technologies exist (3G, WiMax, WDS, Bluetooth). We're ignoring those.
- Usually used for LAN, limited MAN/WAN/PAN
- Can operate in Infrastructure or Ad-hoc modes
- Uses 2.4Ghz or 5Ghz range (junk bands)

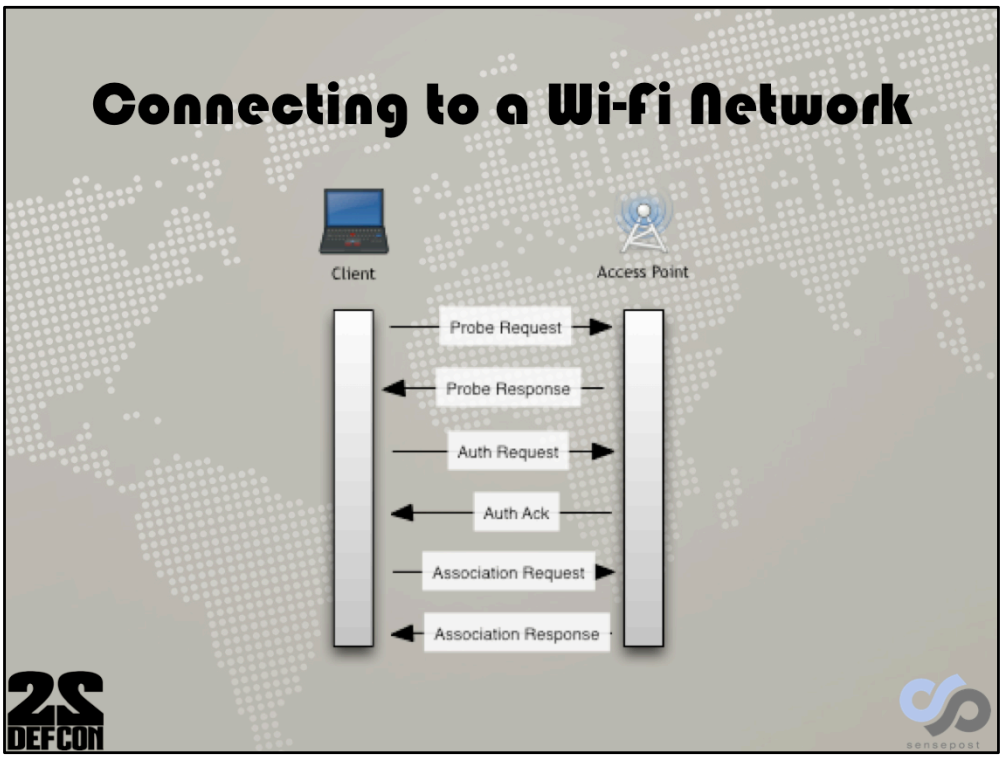
A Wifi Primer

- 3 types of packets
  - Management – Probes/Beacons
  - Control – RTS/CTS
  - Data – The goods

- We're mostly interested in Management frames at this point



This is how networks show up in your network list when searching for wifi networks on your device.



When you join a network, this interaction happens.

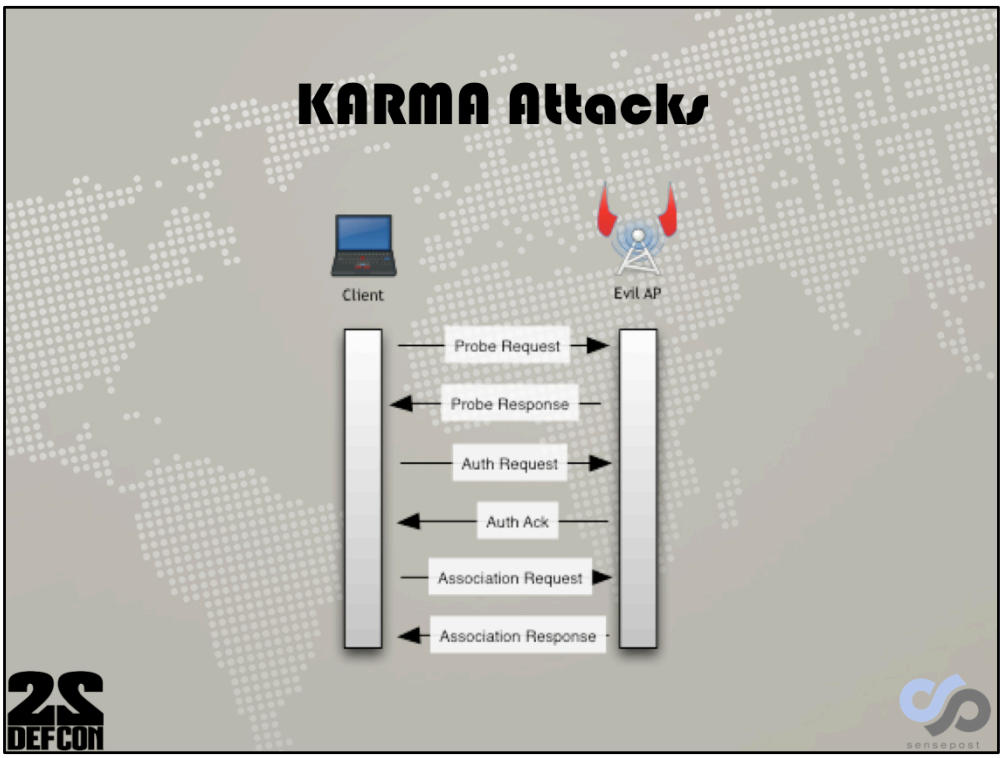
Connecting to a Wi-fi Network

- Client sends probe
- Station responds to probe
- Client sends authentication request
  - A formality, nobody uses shared key networks, all open
  - SSID sent in the clear, even if hidden
- AP acknowledges authentication
- Client sends association request
  - Contains capabilities e.g. rates
- AP sends association response

Management Packets

Unauthenticated in Open Network


KARMA ATTACKS
DEFCON
sensepost



KARMA attacks do exactly the same thing as a normal association, it's just an evil AP instead of the actual AP doing it.

KARMA Attacks

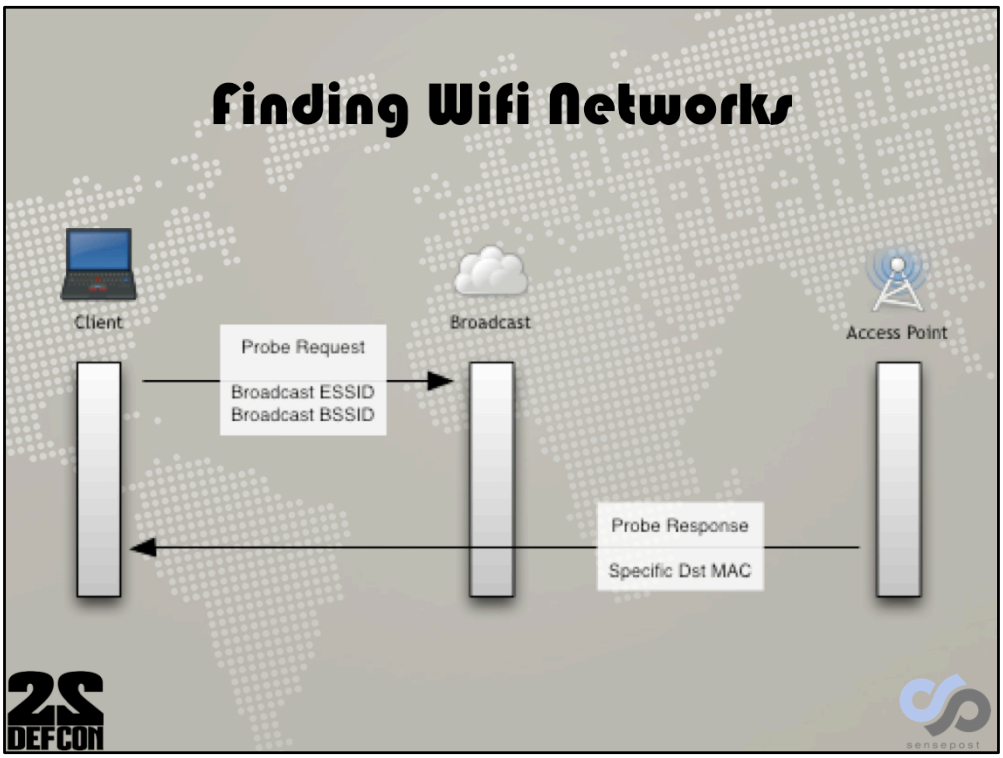
- Device will probe for remembered nets (preferred network list [PNL]), even when not near them
- We just respond as the normal network would
  - Hey "home network" you there?
  - Uh, sure, I'm "home network"
- First presented in 2004 by Dino dai Zovi & Shane Macaulay
- Modern implementations:
  - airbase-ng by Thomas d'Otreppe
    - Software only, no master mode needed
  - hostapd-1.0-karma by Robin Wood (digininja)
    - Used on the Hak5 pineapple

Why this works?

- Networks/ESSIDs can have multiple APs (e.g. corporate nets)
  - BSSID doesn't have to match
  - Devices need to switch APs as they move
- Anti-spoofing done at higher level
  - WEP & WPA/2 PSK
    - AP & STA prove they know the key to each other)
  - EAPs
    - other proof, like TLS validation
- Devices probe directly for networks on their PNL
  - We built snoopy off of this single flaw

It doesn't work well

- iOS devices significantly reduced the amount they probe since iOS 7
- Android devices only connected when you explicitly joined the network
  - Didn't show up in the available network list in modern android
- Same for Linux (shared wpa_supplicant code)
- Windows devices varied greatly across versions
- Only Macs (OSX) seemed to auto-connect to any of these networks!



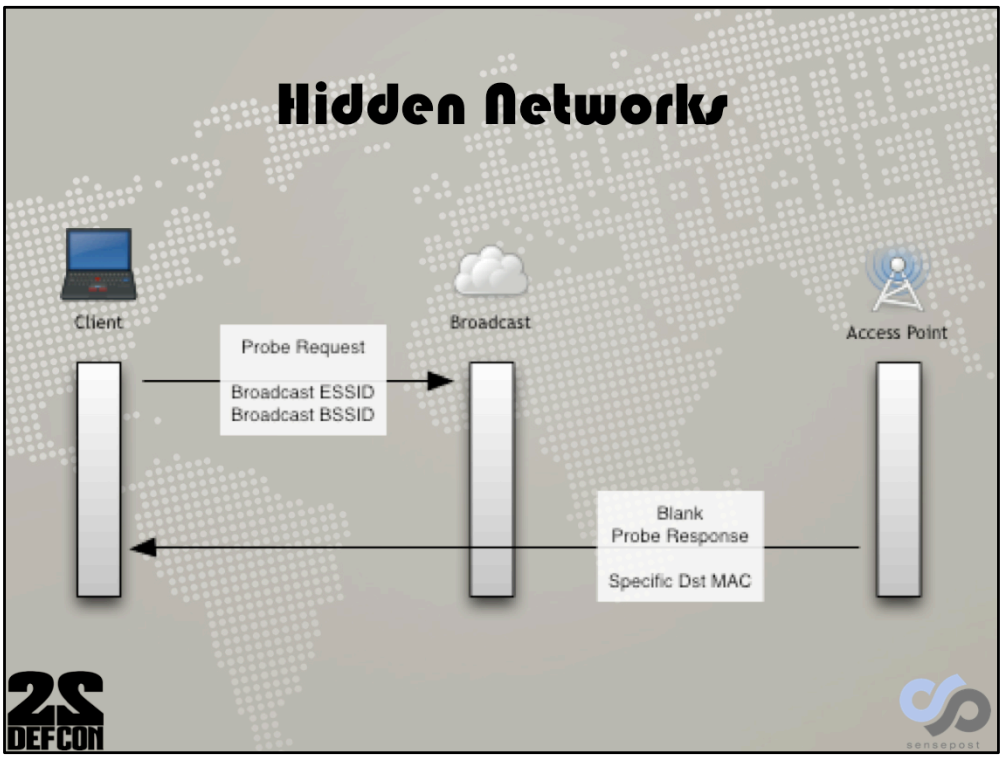
This is why KARMA attacks weren't working well, we weren't responding to the broadcast probes.

Improving KARMA

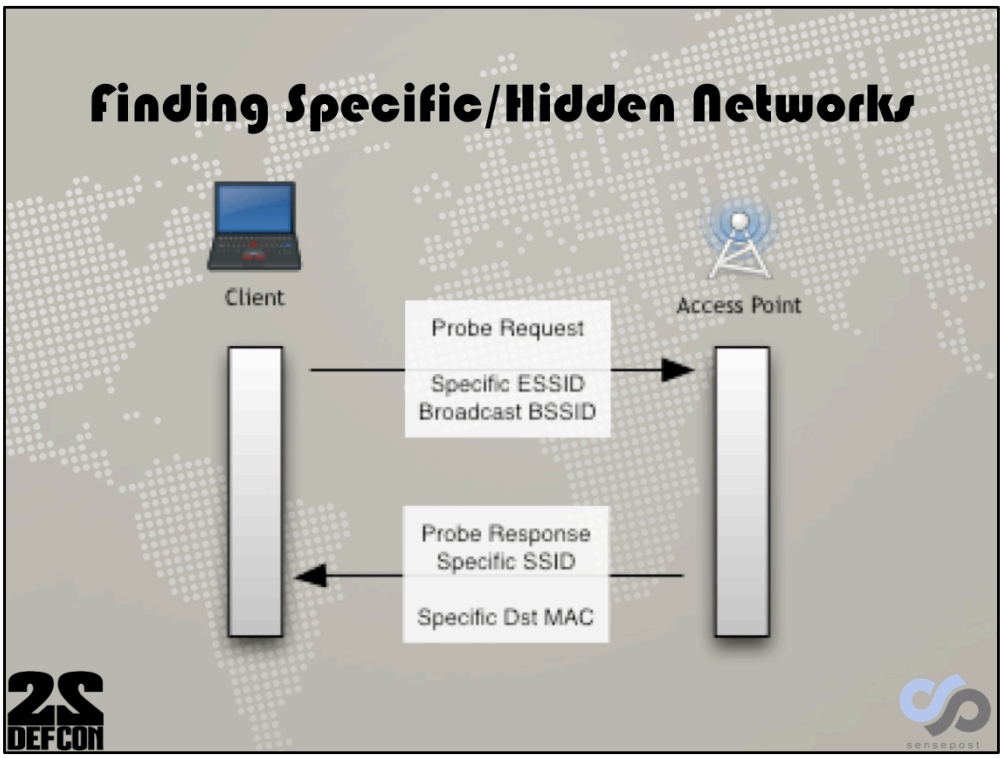
- Turns out our AP needs to respond to the broadcast probe as well as the directed probe
- It also turns out we can send multiple probe responses for different networks (ESSID) from the same BSSID
- Process
  - Watch for directed probes
  - Build per-MAC view of PNL
  - Respond to a broadcast probe with directed responses for each network in PNL
- This increases our karma attack significantly!
- Implemented in our hostapd mod included in MANA

Still Problems

- Snoopy screwed us (yay)
- iOS devices barely probe
- iOS has promised to introduce MAC randomisation on probe (not seen yet)
- Android had changes committed in July 2014 to reduce probes (fix low-power offload probing)
- wpa_supplicant got the patches, so Linux too



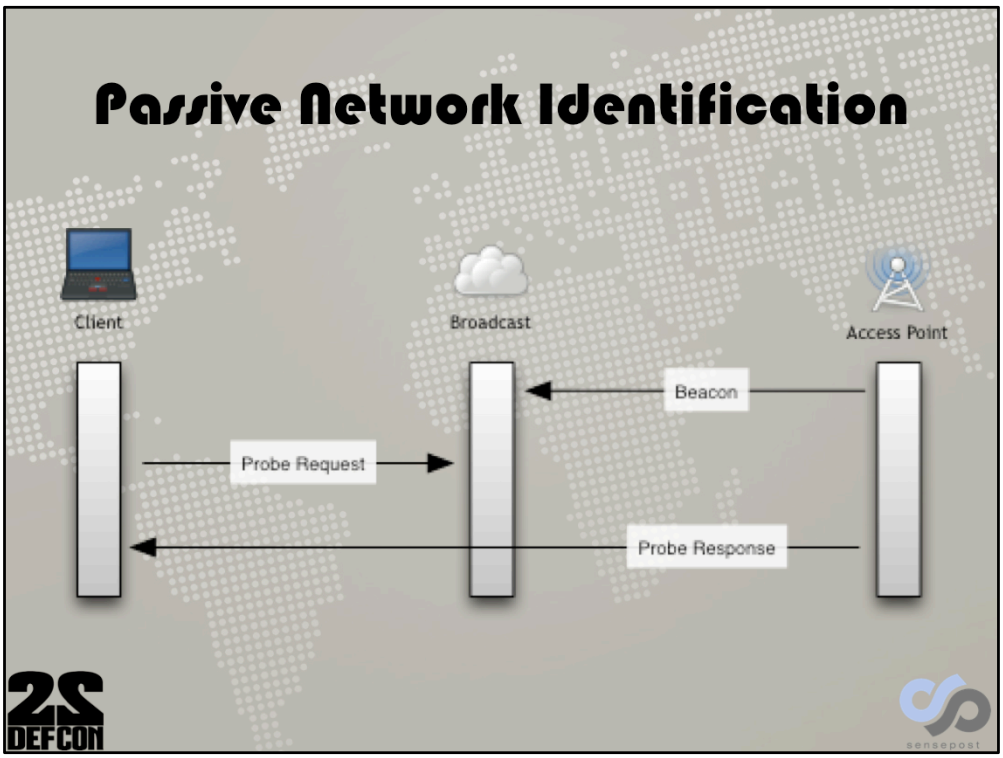
In trying to figure out the issue, we went to the place we should always see probes, hidden networks. Hidden networks don't return the ESSID in response to broadcast probes.



The AP only gives up it's name if the device probes for it specifically (i.e. you must know the name already).

iOS Hidden Net Hrrmm?

- Devices with hidden networks on their PNL need to probe for them **all the time**
- But iOS devices don't
  - This is impossible!
- Turns out, iOS only probes for hidden nets when at least one hidden network is in-range



This means that iOS devices are passively looking for beacons from hidden networks. Why not do that for all networks?

Solution

- Run a hidden network, or beacon out hidden network frames with the normal beacon
- Also, deauth users from currently connected APs to force re-scan
- Rely on other devices to leak network names (e.g. their laptop/tablet, co-workers, fellow airport travellers etc.)
  - "loud mode" changes mana's behaviour to not track PNL per device, but to re-broadcast all networks to all devices
  - Very noisy!

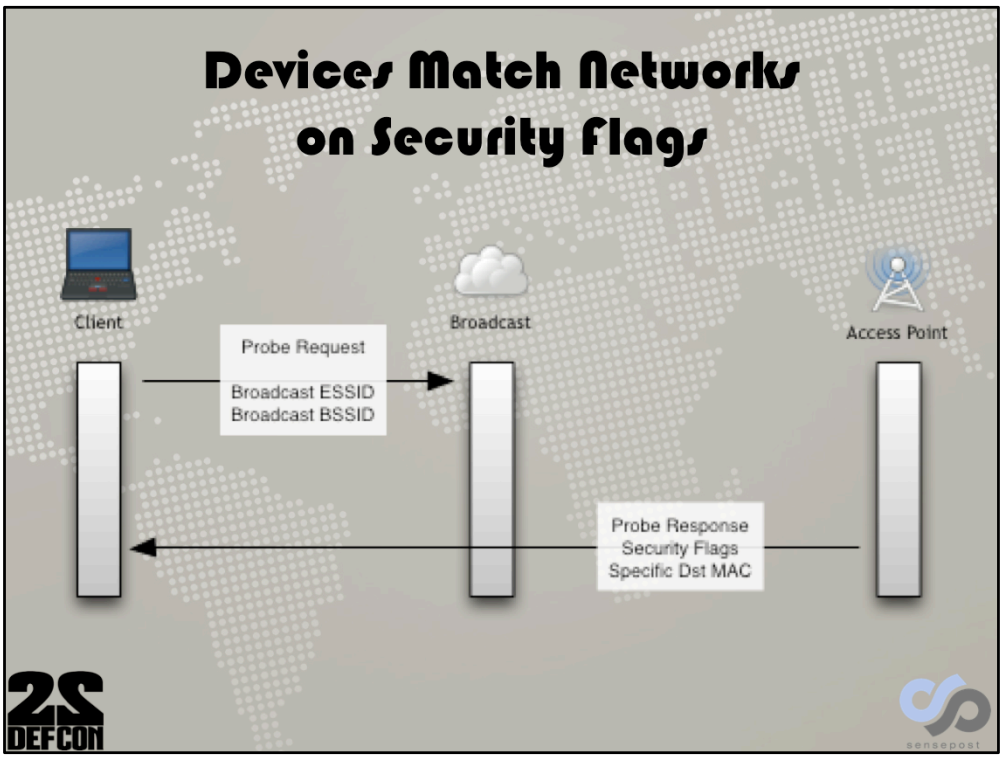
Karma Summary

- Current KARMA attacks don't work well anymore
  - Few devices auto-join rogue networks
  - Networks don't show up as available so mistaken clicks missed
  - Devices probe less
- MANNA improves this
  - Responds to broadcast probes
  - Coaxes iOS hidden networks to be probed
  - Can rely on other, less secure devices to disclose the PNL

Demo Time

- Demo of devices in the room responding to MANA attacks
- We have prevented association to limit legality impacts i.e. you should see the networks in your wifi list

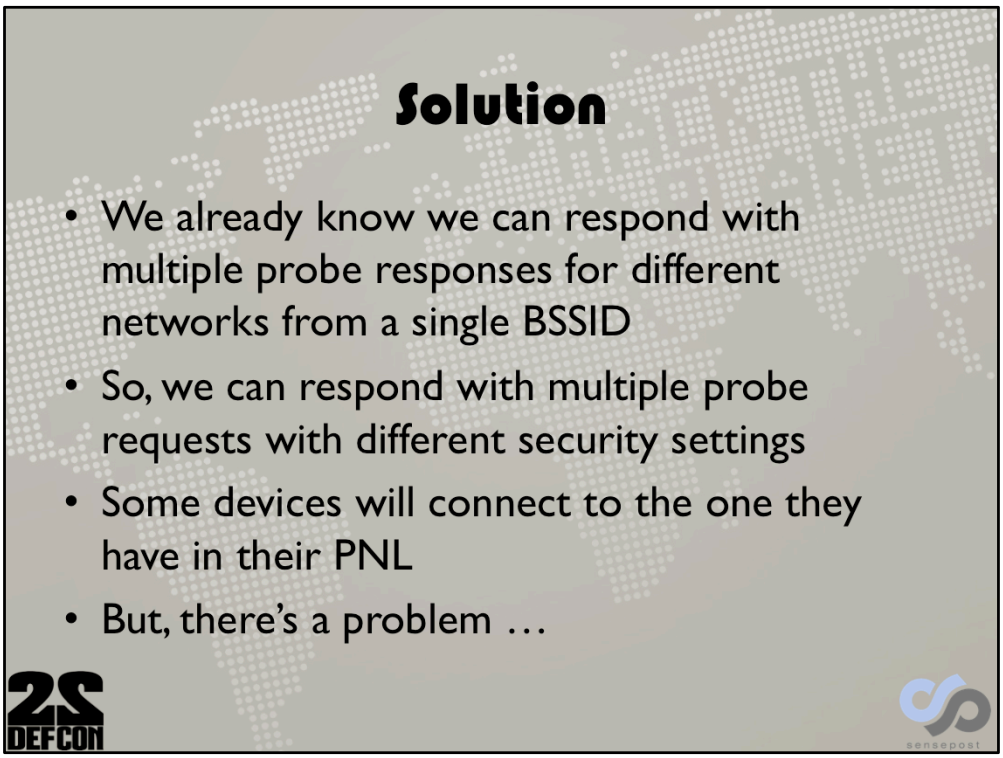

EXTENDING KARMA TO SECURE NETS
DEFCON
sensepost



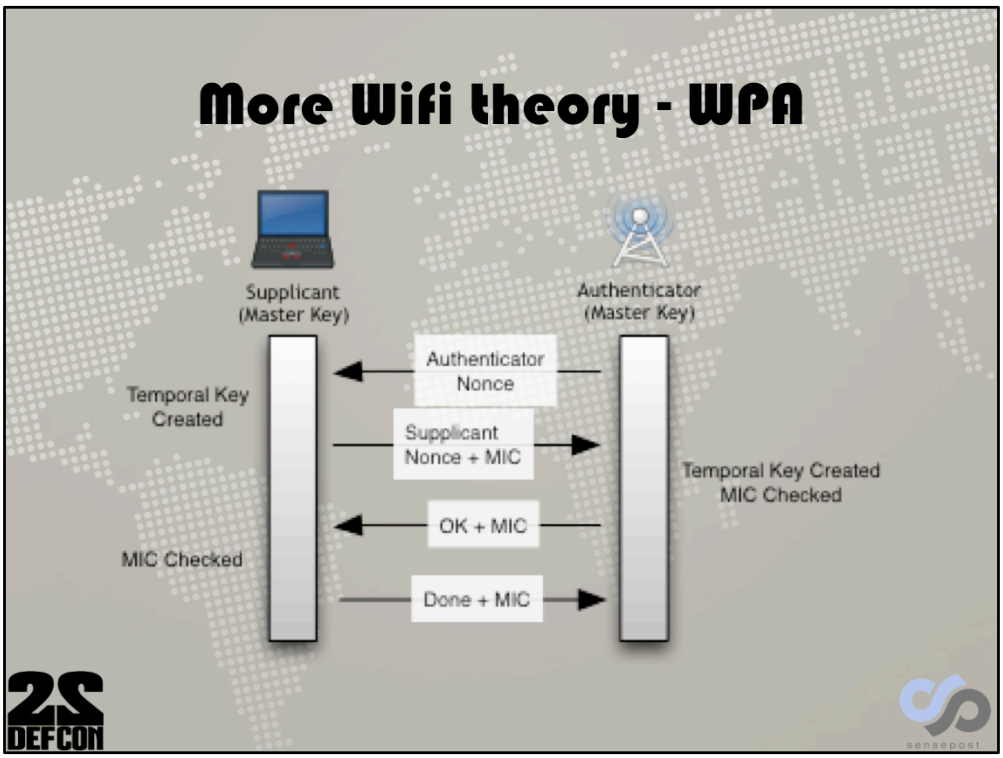
Probe responses contain a flag indicating whether they are WEP, WPA/2 PSK, WPA/2 EAP etc. This is used as part of the “uniqe” match for PNL networks.

Problem

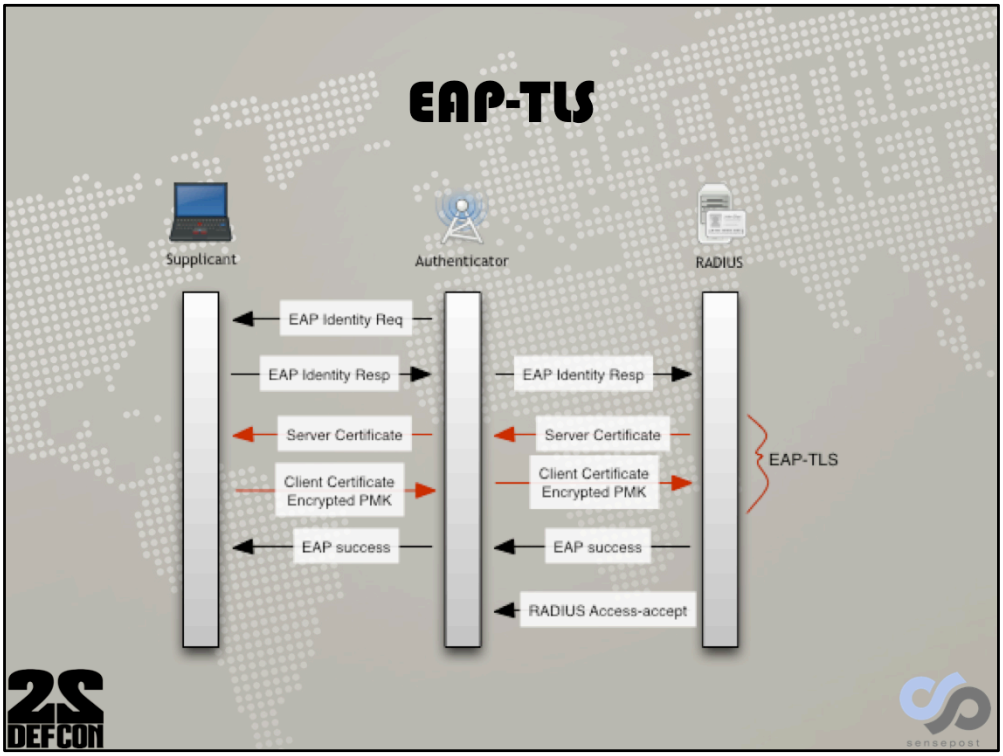
- No support for secured networks in KARMA
- Devices expecting a "secured" network won't connect
  - User can manual connect
  - Android shows as different network
  - iOS shows as open, can click with no warning
  - OSX shows as open, connecting gives warning



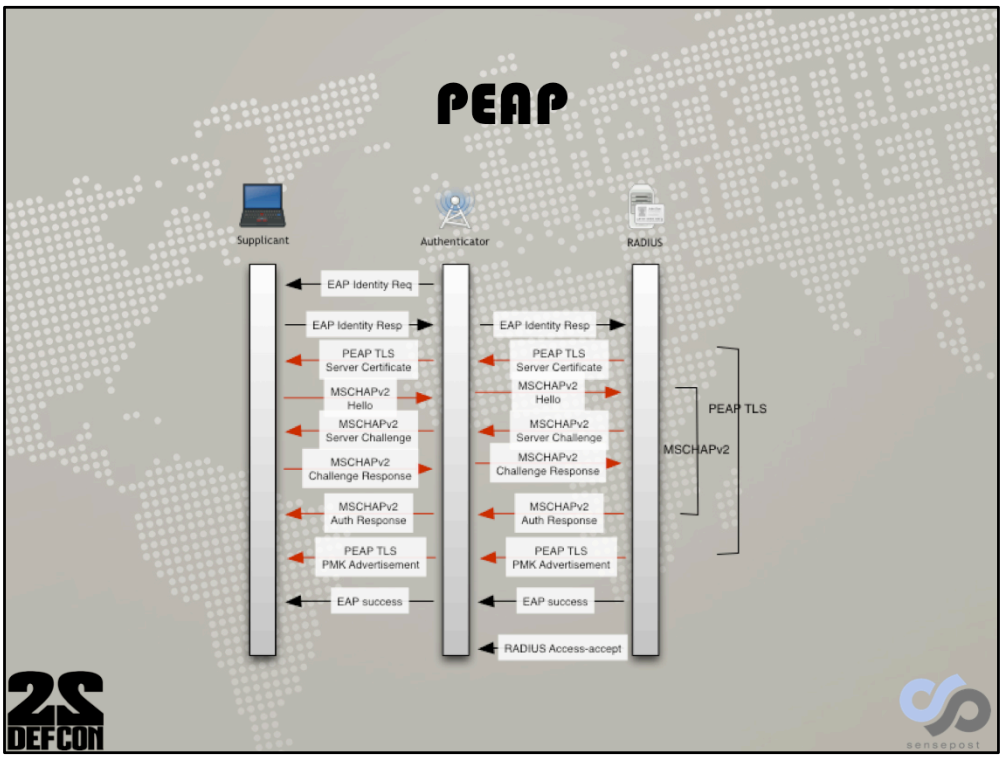
This specific part is still under heavy testing at the time of writing.



We don't have the creds. But, we can have our rogue AP act as a WPA/2 network and send the first packet, and we capture the second. We don't have the right key, and can't generate the Temporal key, but we have anonce and snonce and a MIC from the client, so we can attempt to brute the key until we can generate a MIC for the snonce that matches the clients. Josh Wright's coWPAtty tool first did this.



With EAP, we have a similar problem, but if the client isn't validating correctly, we can MitM. EAP TLS is mutually authenticated so we can't here (just included for a simpler decription).



We can MitM PEAP and PEAP-like EAPs most of the time. This is because most configurations don't validate the server cert, and even when they do, there is no CN name match, it's purely on authority. A successful MitM gets up an MSCHAPv2 challenge response (depending on setup).

Auto-Crack & Add

- PEAP we can capture the MSCHAPv2 challenge/response if no cert validation
  - Currently, people use freeradius-wpe by Joshua Wright and Brad Antoniewicz
  - But, hostapd has it's own RADIUS server
  - Now, so does mana, no need to run a separate server
    - (initial patch from Brad)
- WPA/2 we can capture the first 2 parts of the handshake
- Send them for cracking with your favourite tool
  - CloudCracker (chapcrack), Asleap, coWPAtty, aircrack-ng, hashcat, john
- Add the results back to manna!
  - i.e. auto create a network with the correct security setting, PSK key or EAP user:password combination
  - Also, **CREDS FROM THE SKY!**
- This only works on "easy" creds, hard take too long

Demo

- Demonstration of a device attempting to connect to a PEAP network
- MANA will rogue-AP it, grab the MSCHAPv2 challenge & crack it
- Will then create the user and re-rogue
- Device will connect


MAN IN THE MIDDLE
DEFCON
sensepost

MitM introduction

- Getting clients to connect is only half the battle
- Benefits of MitM are rapidly declining
  - Devices try to check if connection is legit
  - Tools no longer work (dsniff, firesheep, etc.)
  - Karmetasploit only gives us a handful of mail creds
  - HSTS defeats sslstrip
  - Mobile Apps auto cert validation defeats SSL MitM
  - Cert pinning ruins everything

Am I Online?

- Needed for MitM with no-upstream (e.g. on planes, down mines, in faraday cages ;)
- Devices make a request to a site on public Internet to check if online
  - iOS devices hit 1 of over 200 sites with a random request
  - BlackBerry, Android, Windows all make a single request to a known destination
- MANA includes bundle of apache sites that implement all of these

firelamb

- Firesheep isn't maintained and no longer works
- Enter firelamb
- Simple python script that does the same
- Writes output to firefox profile for easy cookie loading

HSTS Partial Bypass

- Updates to sslstrip by LeonardoNVE @ BlackHat Asia
- Includes intercepting DNS server, dns2proxy
- Process
  - Browser requests http://www.google.com/
  - sslstrip returns redirect to wwww.google.com
  - dns2proxy mirrors DNS for www.google.com -> wwww.google.com
  - sslstrip rewrites links from www.google.com to "alternate" domains
  - Browser has no HSTS setting for wwww.google.com
  - Client continues in plaintext

Malicious iOS Profiles

- Config Profiles allow tons of changes to the device, including
  - New root CA, for MitM
  - New open wifi networks to keep KARMA going
  - Ability to prevent it's removal
- Can push these to the device over HTTP (no need for mail SE, but could do that too)
- Requires users hit install and type their passcode
  - Tough sell ☹
  - But can prevent removal after that
- Allows much better MitM with new root CA
  - http://www.lacoon.com/blog/2014/07/security-disclosure-googles-ios-gmail-app-enables-threat-actor/
- Doesn't defeat cert pinning though

Captive Portal SE

- We want creds dammit!
- Fake captive portal, designed to gather them
- Tricks
  - Don't interfere with normal comms (so we can still mitm auto interactions)
  - Use WISPr to get browser open early
  - Provides chance for iOS profile push & explanation
  - Provide option to go away so user can continue surfing
  - Provides a beef hook
- Ask for creds using OAuth-lookalike
- Our take included in MANA

Demo

- Demo of a device joining our rogue network
  - Getting auto-mail fetch creds (ClearText mail or Microsoft ActiveSync over SSL)
  - Captive Portal demo
  - HSTS bypass on gmail/twitter/facebook
  - Pushing a malicious iOS config
    - Demo of enhanced MitM against well known app (will be disclosed after vendor fixes)
  - Example HTML5 WebView giving us data

Disclaimer & Updates

These are an early version of our slides and the tools, our data and the slides will all be updated by the time of our Defcon talk. You can access these updates at:

- Slides http://slideshare.net/sensepost
- Tools http://github.com/sensepost/manna
- Overview http://www.sensepost.com/blog/