

KARMA

(Slides loving ripped from www.theta44.org)

KARMA Attacks Radioed Machines Automatically

Kurt Grutzmacher
grutz@jingojango.net

BayLISA – 02/18/06

Garrett Gee
ggee@srtek.net



Who we are

- Penetration testers for a large financial institution in the Bay area
- Many years combined experience in performing assessments, red teaming, exploring vulnerabilities, etc.



Hackers, Meet Microsoft

"The random chatter of several hundred Microsoft engineers filled the cavernous executive briefing center recently at the company's sprawling campus outside Seattle. Within minutes after their meeting was convened, however, the hall became hushed. Hackers had successfully [lured a Windows laptop onto a malicious wireless network](#). 'It was just silent,' said Stephen Toulouse, a program manager in Microsoft's security unit. 'You couldn't hear anybody breathe.' The demo was part of an extraordinary two days in which outsiders were invited into the heart of the Windows empire for the express purpose of exploiting flaws in Microsoft computing systems. The event, which Microsoft has not publicized, was dubbed 'Blue Hat' -- a reference to the widely known 'Black Hat' security conference, tweaked to reflect Microsoft's corporate color."



KARMA History

- First shown at PACSEC'04
- ImmunitySec Shindig 01/17/05
- Microsoft BlueHat
- CanSec/Core'05
- IEEE Information Assurance Workshop
- Still updating, refining, improving...



Motivation behind KARMA

- Wireless networks are becoming secure
 - Improved Encryption systems (WPA)
 - MAC address filtering
 - Hidden networks (SSID cloaking)
- Mobile clients bridge across time
 - Connect to secure AND insecure networks (conferences, hotels, airports, café)
 - Can be compromised on an airplane and spread to secure work network
 - Security of the most secure network depends upon the security of the least secure network



More Motivation

- Paradigm shift to new wireless threat
 - Attacking the wireless client
- Nightmare scenario
 - Target: Identify wireless clients
 - Position: Get on same network as victim
 - Attack: Exploit client-side vulnerabilities to install persistent agent
 - Subvert: Agent gives attacker remote access to secure networks that client connects to



Recent Wireless Research

- ShmooCon'06
 - “Wi-Fi trickery, or how to secure, break and have fun with Wi-Fi” by Laurent Butti and Franck Veysset
 - “VoIP WiFi phone security analysis” by Shawn Merdinger
 - “The Church of Wi-Fi presents: An Evil Bastard, A Rainbow and a Great Dane!” by Renderman, Thorn, Dutch, and Joshua Wright
 - “Hacking the Friendly Skies” by Simple Nomad
 - “Bitchslapping Wireless IDS/IPS appliances” by Eldon Sprickerhoff

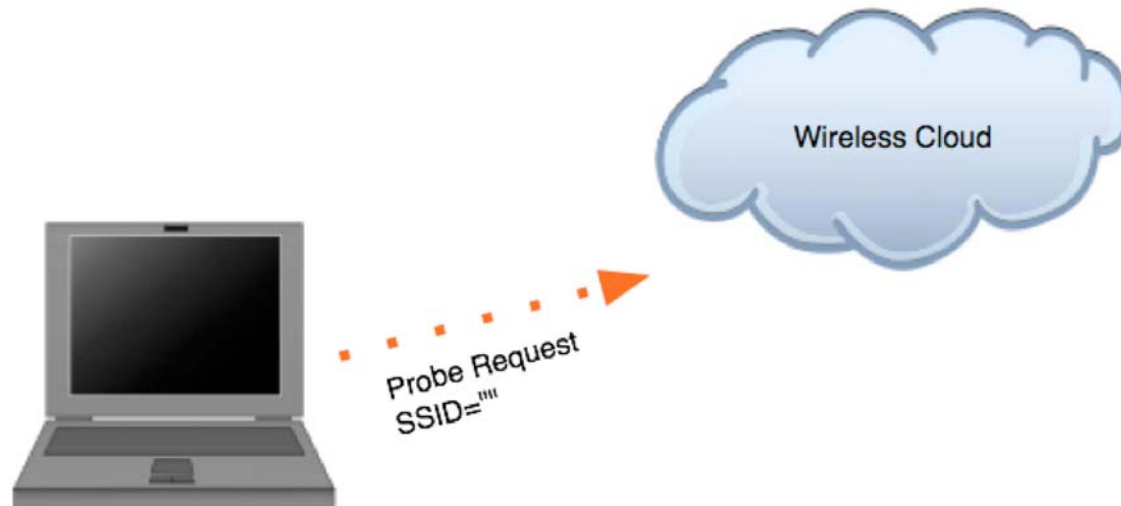


Automatic Wireless Network Selection

- Its purpose is to (re)connect to trusted known wireless networks
- Operating System maintains list of *Trusted/Preferred* wireless Networks
 - Records the SSID and Encryption method
- Preferred networks are automatically connected when available
 - Windows: Continuously searches when the wireless card is on and not associated to another network
 - MacOSX: Search only when user logs on or when returning from sleep mode.



WindowsXP Wireless Auto Configuration Algorithm



- Client builds a list of available networks
 - Send broadcast Probe Request on each channel



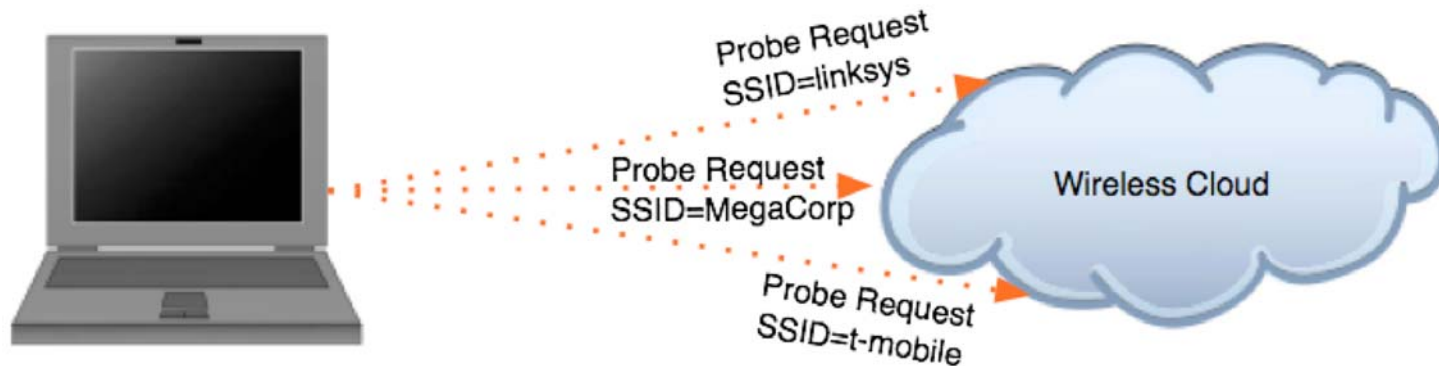
Wireless Auto Configuration Algorithm



- Access Points within range respond with Probe Responses



Wireless Auto Configuration Algorithm



- If Probe Responses are received for networks in preferred networks list:
 - Connect to them in preferred networks list order
- Otherwise, if no available networks match preferred networks:
 - Specific Probe Requests are sent for each preferred network in case networks are “hidden”



Wireless Auto Configuration Algorithm



- If still not associated and there is an ad-hoc network in preferred networks list, create the network and become first node
 - Uses self-assigned IP address (169.254.Y.Z)



Wireless Auto Configuration Algorithm



- Finally, if “Automatically connect to non-preferred networks” is enabled (**disabled by default**), connect to networks in order they were detected
- Otherwise, wait for user to select a network or preferred network to appear
 - Set card’s desired SSID to random 32-char value, Sleep for minute, and then restart algorithm



Weaknesses in Wireless Auto Configuration

- *Information Disclosure*
 - Specific 802.11 Probe Requests reveal SSIDs of preferred networks
- *Spoofing*
 - Unencrypted networks are identified and authenticated only by SSID
- *Unintended Behavior*
 - An ad-hoc network in Preferred Networks List turns a wireless client into an Access Point

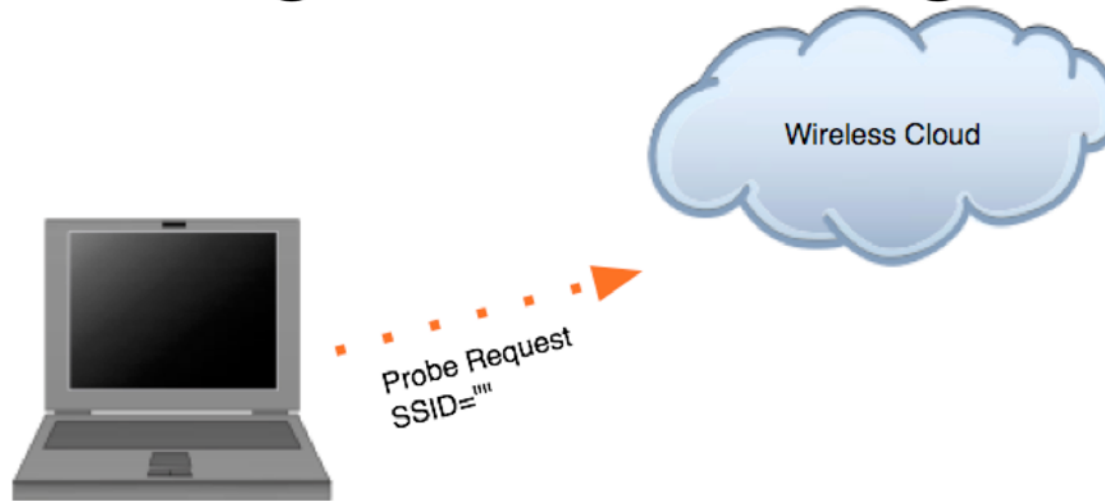


Getting Ready for Attack

- Join ad-hoc network created by target
 - Sniff network to discover self-assigned IP (169.254.Y.Z)
- Create a stronger signal for currently associated network
 - While associated to a network, clients send Probe Requests for same network to look for stronger signal
- Create a (more) Preferred Network
 - Spoof disassociation frames to cause clients to restart scanning process
 - Sniff Probe Requests to discover Preferred Networks
 - Create a network with SSID from Probe Request



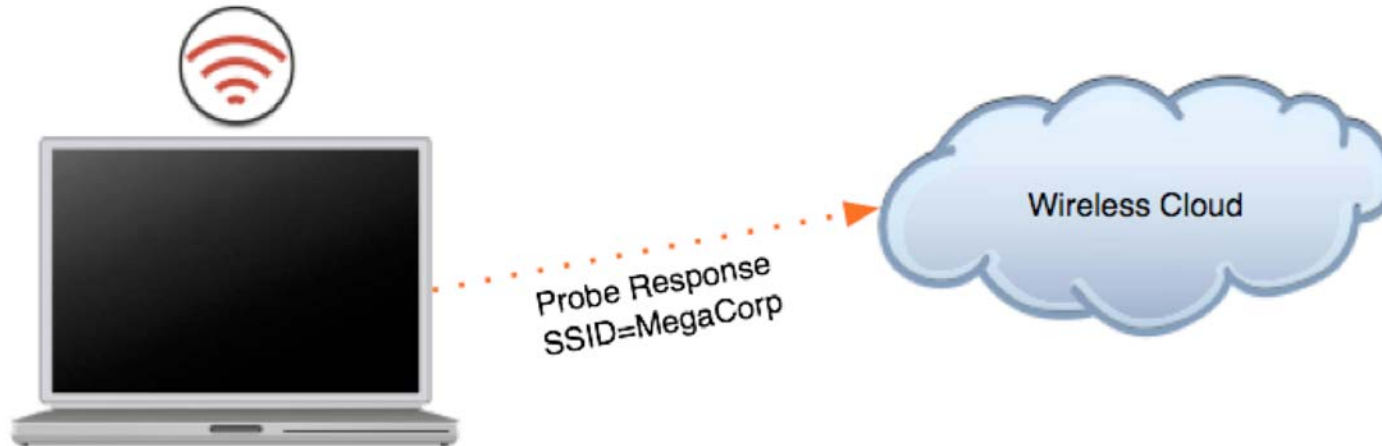
Attacking Auto Configuration



- Attacker spoofs disassociation frame to victim
- Client sends broadcast and specific Probe Requests again
 - Attacker discovers networks in Preferred Networks list (e.g. linksys, MegaCorp, t-mobile)



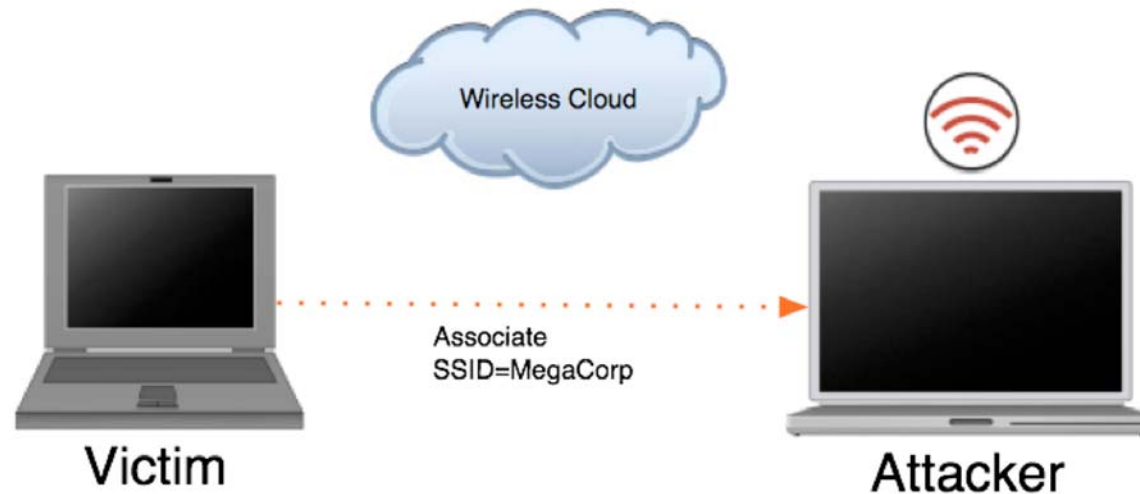
Attacking Auto Configuration



- Attacker creates a rogue access point with SSID *MegaCorp*



Attacking Auto Configuration



- Victim associates to attacker's fake network
 - Even if preferred network was WEP (XP SP 0)
- Attacker can supply DHCP, DNS, ..., servers
- Attacker exerts a significant amount of control over victim



Improving the Attack

- Parallelize
 - Attack multiple clients at once
- Expand scope
 - Act as any networks that any client is looking for
- Simplify
 - Don't require learning preferred networks before beginning attack
- Increase availability
 - Attack continuously



Performing the Attack

- Laptop runs software base station
 - Possibly with antenna, amplifiers
- AP responds to any Probe/Assoc Request
- Clients within range join what they think is one of their Preferred Networks
 - Client A thinks it is on “linksys”
 - Client B thinks it is on “t-mobile”
 - Client C thinks it is on “hhonors”
- Any client with at least one unencrypted preferred network will join if no legitimate preferred networks are present



Back to Wireless Auto Config

- Remember how SSID is set to random value?
- The card sends out Probe Requests for it
- We respond w/ Probe Response
- Card associates
- Host brings interface up, DHCPs an address, etc.
- Verified on Windows XP SP2 w/ PrismII and Orinoco (Hermes) cards
- Fixed in Longhorn



Vulnerable PNL Configurations

- If there are no networks in the Preferred Networks List, random SSID will be joined
- If all networks in PNL are encrypted, random SSID will have left-over WEP configuration (attacker will have to guess key)
 - We supply the challenge, victim replies with challenge XOR RC4 keystream
 - Our challenge is 00000000000000000000...
 - We get first 144 bytes of keystream for a given IV
- If there are *any* unencrypted networks in PNL, host will associate to our modified Access Point.



Apple MacOS X

- MacOS X AirPort (but not AirPort Extreme) has similar issues
- MacOS X maintains list of trusted wireless networks
 - User can't edit it, it's an XML file base64-encoded in another XML file
- When user logs in or system wakes from sleep, a probe is sent for each network
 - Only sent once, list isn't continuously sent out
 - Attacker has less of a chance of observing it
- If none are found, card's SSID is set to a dynamic SSID
 - With 40-bit WEP enabled
 - ... but to a static key
- After waking from sleep, SSID is set to "dummy SSID"
 - Will associate as plaintext or 40-bit WEP with above key
- MacOS X 10.4 ("Tiger") has GUI to edit list of trusted wireless networks



Defenses?

- Keep wireless card turned off when not using a wireless network
- Only keep secure networks in Preferred Networks List
- Remove insecure network from PNL immediately after done using it
- Prevent mobile clients from connecting to sensitive networks



Lets get some KARMA

- Track clients by MAC address
 - Identify state: scanning/associated
 - Record preferred networks by capturing Probe Requests
 - Display signal strength of packets from client
- Allows targeting a specific client
 - Create a network they will automatically associate to
- Identify insecure wireless clients that will join rogue networks
- “*Kismet*” for wireless clients



KARMA Probe Monitor

```

KARMA
Hardware Address  Sig  Probe Requests
00:0e:35:51:1a:cf 210  theta44
08:00:46:df:11:14 201  WNR2004 <broadcast>
00:0c:f1:16:34:98 213  Wireless <broadcast>
00:03:93:e8:d2:e7 222  <broadcast> offhollywood GORELAN cafe.com bryantpark.org d
00:11:f5:0d:17:3b 026  <broadcast> Wireless
00:0e:35:5e:61:97 008  Wireless <broadcast>
    
```



KARMA

- Wireless and client-side attack and assessment toolkit
- Modules attack multiple layers as hostile server or Man-in-the-Middle
 - 802.11: Modified MADWiFi driver answers all Probe/Assoc Requests
 - DHCP: Rogue DHCP server points client at our DNS server
 - DNS: Rogue DNS Server responds to all queries with our IP address
 - POP3/FTP: Servers capture plaintext credentials
 - HTTP: Attack web server redirects any query to browser exploits or acts as transparent proxy



DEMO?



...and in conclusion

- Demonstrated weaknesses and vulnerabilities in Automatic Wireless Network Selection
 - Allows attacker to put victim on hostile subnet
- Firewalls commonly on by default, but clients still initiate a lot of traffic
 - Automatic updates
 - Browsing (NetBIOS, Rendezvous/Bonjour)
- Rise in client-side vulnerabilities
- Mobile clients are a risk to secure networks
- Assess risk of wireless clients with KARMA
 - <http://www.theta44.org/karma/>



Questions?

