

ARP Vulnerabilities

Indefensible Local Network Attacks?

Mike Beekey

Overview

- ARP Refresher
- ARP Vulnerabilities
- Types of Attacks
- Vulnerable Systems
- Countermeasures
- Detection
- Tools and Utilities
- Demonstrations

ARP Refresher

ARP Message Formats

- ARP packets provide mapping between hardware layer and protocol layer addresses
- 28 byte header for IPv4 ethernet network
 - 8 bytes of ARP data
 - 20 bytes of ethernet/IP address data
- 6 ARP messages
 - ARP request and reply
 - ARP reverse request and reply
 - ARP inverse request and reply

ARP Request Message

- Source contains initiating system's MAC address and IP address
- Destination contains broadcast MAC address ff.ff.ff.ff.ff.ff

ARP Reply Message

- Source contains replying system's MAC address and IP address
- Destination contains requestor's MAC address and IP address

ARP Vulnerabilities

Unsolicited ARP Reply

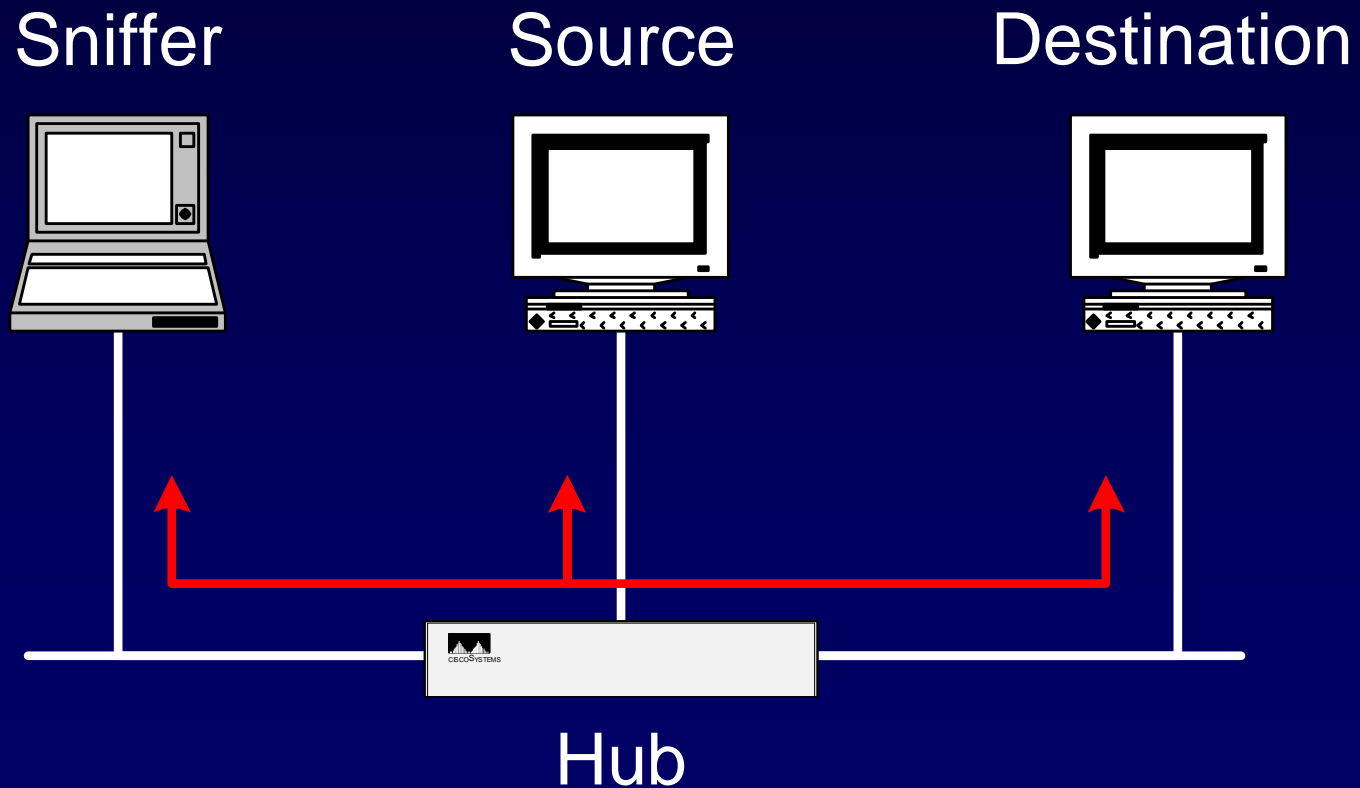
- Any system can spoof a reply to an ARP request
- Receiving system will cache the reply
 - Overwrites existing entry
 - Adds entry if one does not exist
- Usually called ARP poisoning

Types of Attacks

Types of Attack

- Sniffing Attacks
- Session Hijacking/MiM
- Denial of Service

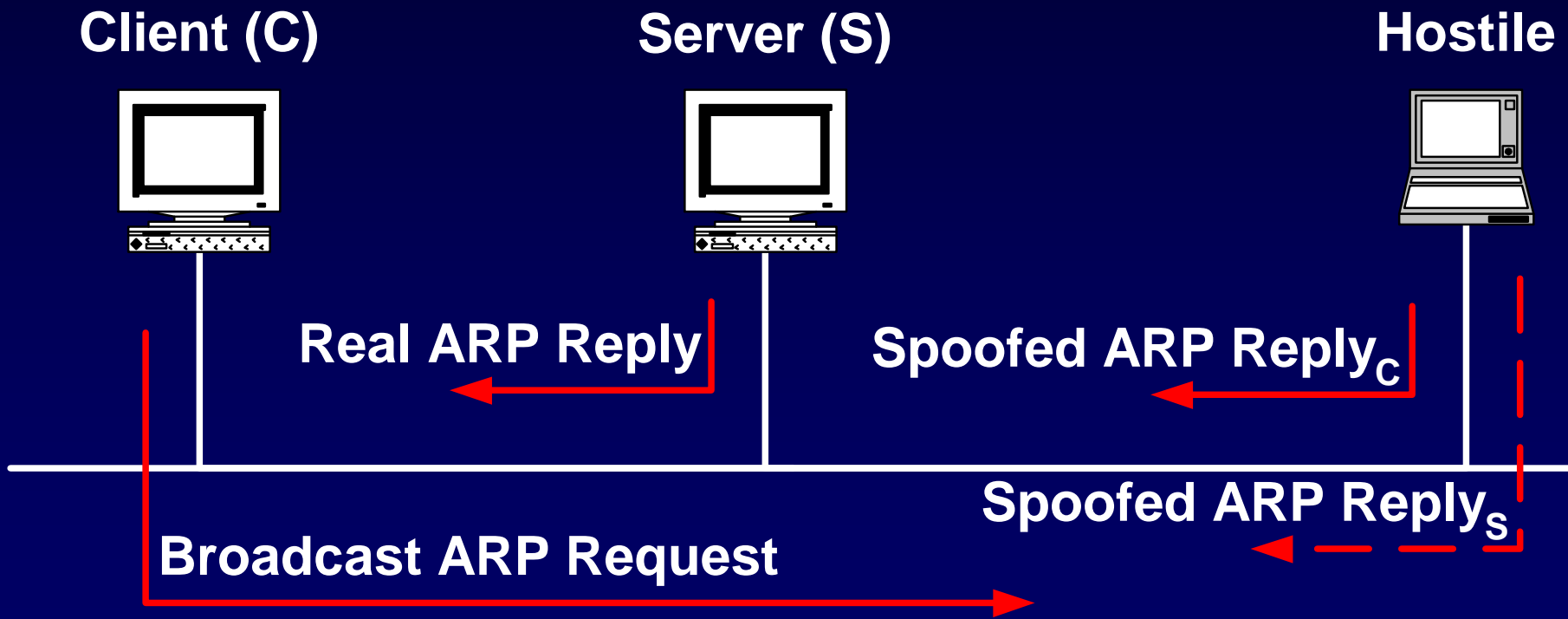
Sniffing on a Hub



Switch Sniffing

- Normal switched networks
 - Switches relay traffic between two stations based on MAC addresses
 - Stations only see broadcast or multicast traffic
- Compromised switched networks
 - Attacker spoofs destination and source addresses
 - Forces all traffic between two stations through its system

Host to Host Exploit



Host to Router Exploit

Client (C)

Gateway Router (R)

Hostile



Real ARP Reply

Spoofed ARP Reply_C

Broadcast ARP Request

Spoofed ARP Reply_R

Relay Configuration

Attacker

0:c:3b:1a:7c:ef- 10.1.1.10



Alice

0:c:3b:1c:2f:1b- 10.1.1.2

0:c:3b:1a:7c:ef- 10.1.1.7



Bob

0:c:3b:9:4d:8- 10.1.1.7

0:c:3b:1a:7c:ef- 10.1.1.2

Sniffing Comments

- Depending on traffic content, attacker does **NOT** have to successively corrupt cache of both endpoints
- Useful when “true” permanent ARP entries are used or OS is not vulnerable to corruption

Session Hijacking/MiM

- Natural extension of sniffing capability
- “Easier” than standard hijacking
 - Don’t have to deal with duplicate/un-sync’d packets arriving at destination and source
 - Avoids packet storms

Denial of Service

- Spoofing the destination MAC address of a connection will prevent the intended source from receiving/accepting it
- Benefits
 - No protocol limitation
 - Eliminates synchronization issues
- Examples
 - UDP DoS
 - TCP connection killing instead of using RST's

DoS MAC Entries

Attacker

0:c:3b:1a:7c:ef- 10.1.1.10



Alice

0:c:3b:1c:2f:1b- 10.1.1.2

a:b:c:1:2:3- 10.1.1.7



Bob

0:c:3b:9:4d:8- 10.1.1.7

0:c:3b:1c:2f:1b 10.1.1.2

Denial of Service Examples

Web Surfing

- *Web surfers require gateway router to reach Internet*
- Method
 - Identify surfer's MAC address
 - Change their cached gateway MAC address (or DNS MAC address if local) to “something else”

Network-based IDS

- *Poorly constructed (single homed) IDS network systems relay auditing data/alerts to management/admin consoles*
- Method
 - Identify local IDS network engine
 - Modify gateway MAC address
 - Modify console/management station address

Hostile Users

- *Attacker continuously probing/scanning either your system or other target*
- Method
 - Scanning you
 - Scanning a system under your protection

Switch Attacks

- *Certain attacks may overflow switch's ARP tables*
- Method
 - A MAC address is composed of six bytes which is equivalent to 2^{48} possible addresses
 - See how many randomly generated ARP-replies or ARP requests it takes before the switch “fails”

Switch Attacks (cont.)

- Switches may
 - Fail open- switch actually becomes a hub
 - Fail- no traffic passes through the switch, requiring a hard or soft reboot

Network “Bombs”

- *“Hidden” application installed on a compromised system*
- Method
 - Passively or actively collects ARP entries
 - Attacker specifies timeout or future time
 - Application transmits false ARP entries to its list

Vulnerable Systems

Operating Systems

- Windows 95
- Windows 98
- Windows NT
- Windows 2000
- AIX 4.3
- HP 10.2
- Linux RedHat 7.0
- FreeBSD 4.2
- Cisco IOS 11.1
- Netgear

Not Vulnerable

- Sun Solaris 2.8
 - Appears to resist cache poisoning

Countermeasures

Firewalls

- Most “personal” firewalls are not capable of defending against or correctly identifying attacks below IP level
- UNIX
 - ipfw
 - ipf (IP Filter)
- Windows environments
 - Network Ice/Black Ice[©]

Session Encryption

- Examples
 - Establishing VPNs between networks or systems
 - Using application-level encryption
- Effects
 - Prevents against disclosure attacks
 - Will not prevent against DoS attacks

Strong Authentication

- Examples
 - One-time passwords
 - Certificates
- Effects
 - None on disclosure attacks
 - None on DoS attacks

Port Security

- Cisco switches

- `set port security ?/? enable <MAC address>`

- Restricts source MAC addresses

- Hard coded ones

- “Learned” ones

- Ability to set timeouts

- Ability to generate traps

- Ability to “shutdown” violating port

Port Security (Cont.)

- Issues
 - Only restricts source MAC addresses
 - Will not prevent against ARP relay attacks
 - Will only prevent against ARP source spoofing attacks

Hard Coding Addresses

- Example
 - Individual systems can hard code the corresponding MAC address of another system/address
- Issues
 - Management nightmare
 - Not scalable
 - Not supported by some OS vendors

Hard Coding Results

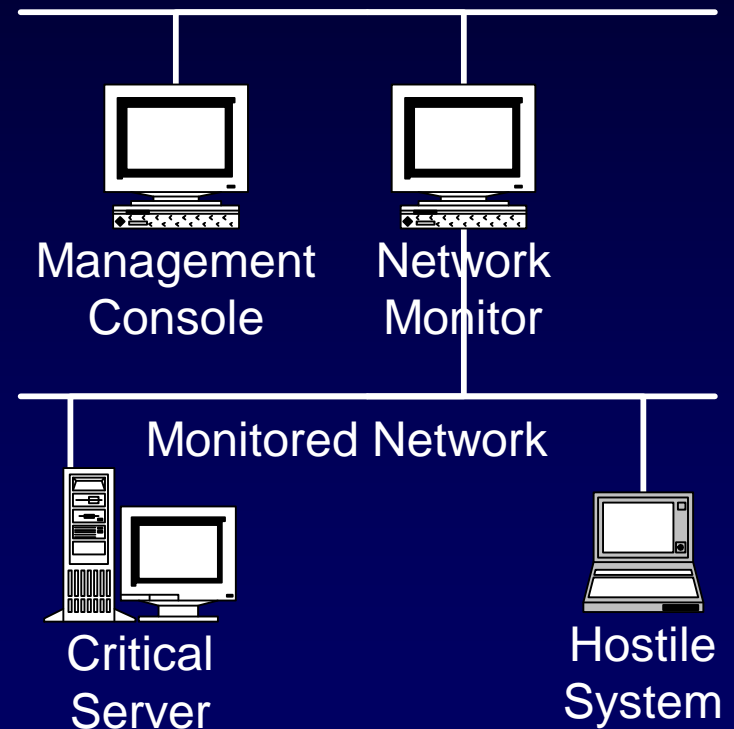
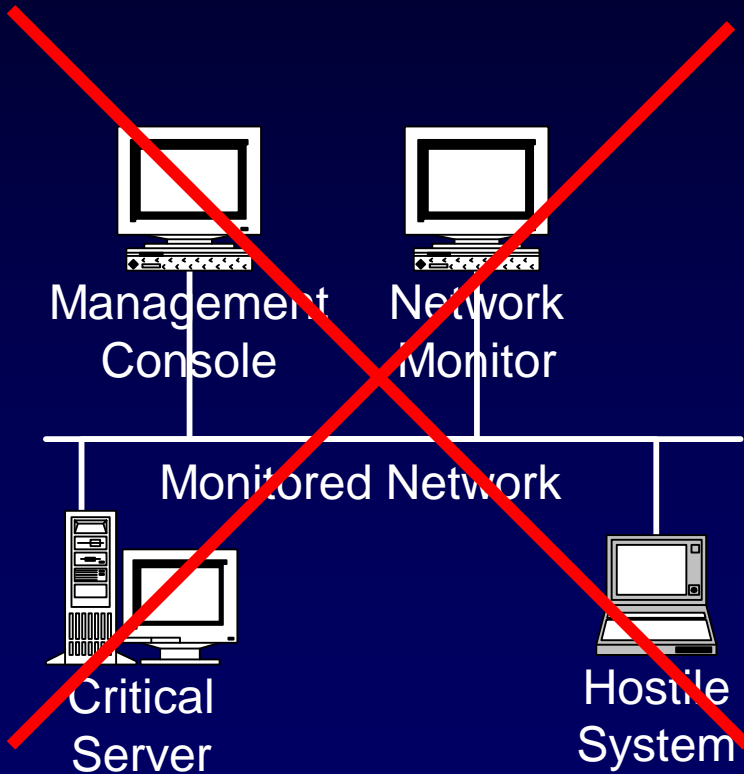
Operating System	Results
Windows 95	FAIL
Windows 98	FAIL
Windows NT	FAIL
Windows 2000	FAIL
Linux RedHat 7.0	YES
FreeBSD 4.2	YES
Solaris 2.8	YES

Countermeasure Summary

	Sniffing	Session Hijacking	Denial of Service
Firewalls	●	●	●
Session Encryption	●	●	●
Strong Authentication	●	●	●
Port Security	●	●	●
Hard Coding	●	●	●

Detection

IDS Architecture Issues



OS Level Detection

Operating System	Detection
Windows 95	NO
Windows 98	NO
Windows NT	NO
Windows 2000	NO
Linux RedHat 7.0	NO
FreeBSD 4.2	YES

Hypothetical Detection Application

- Purpose
 - Track and maintain ARP/IP pairings
 - Identify non-standard ARP-replies versus acceptable ones
 - Timeout issues
 - OS must withstand corruption itself
 - Fix broken ARP entries of systems
 - Transmission of correct ARP replies

Tools and Utilities

Public Domain Tools

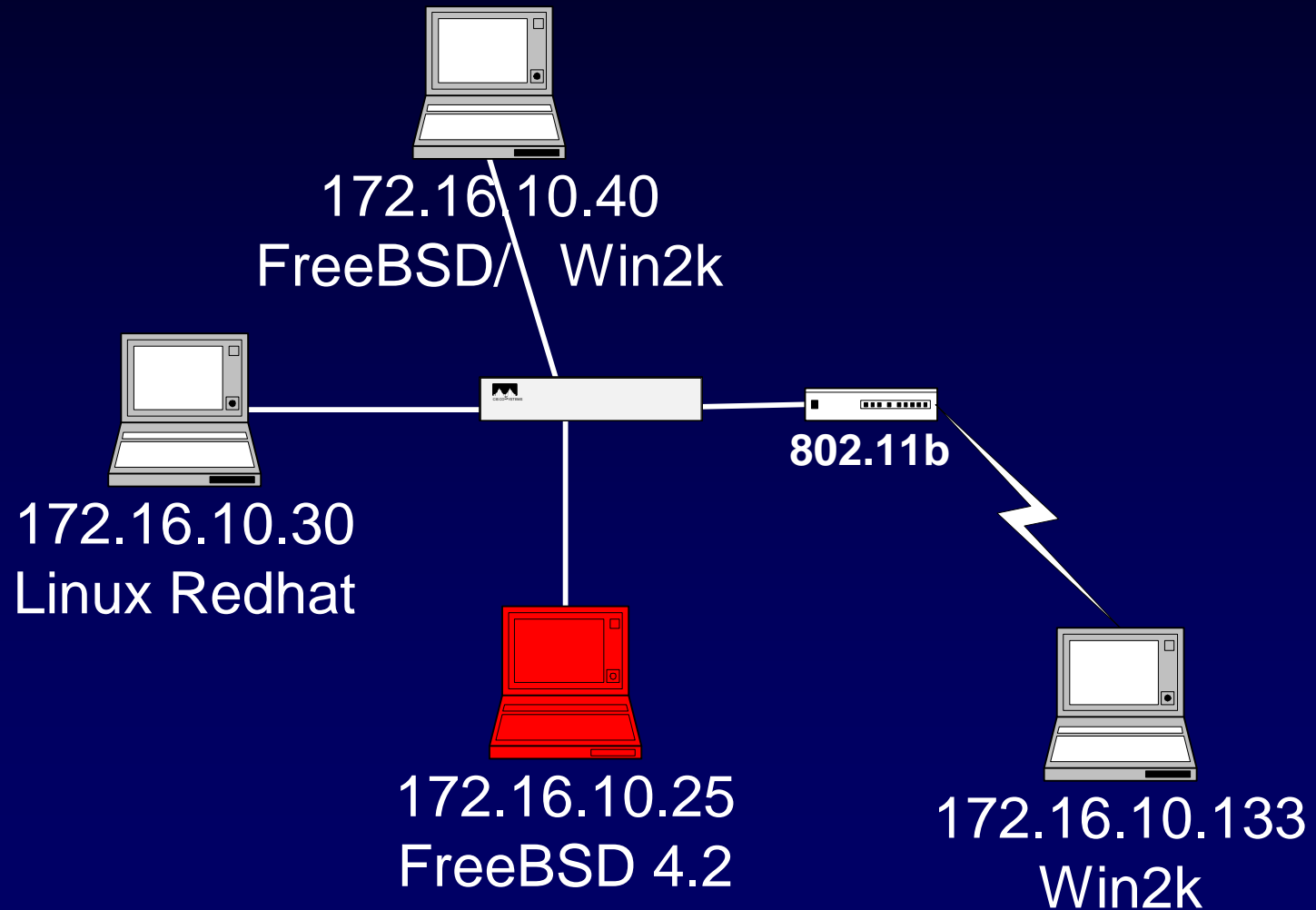
- Manipulation
 - Dsniff 2.3
 - Hunt 1.5
 - Growing number of others
- Local monitoring
 - Arpwatch 1.11

Bibliography

- Finlayson, Mann, Mogul, Theimer, RFC 903 “A Reverse Address Resolution Protocol,” June 1984
- Kra, Hunt 1.5, <http://www.gncz.cz/kra/index.html>, Copyright 2000
- Lawrence Berkeley National Laboratory, Network Research Group, Arpwatch 1.11, <ftp://ftp.ee.lbl.gov/arpwatch.tar.Z>, Copyright 1996
- Plummer, David C., RFC 826 “An Ethernet Address Resolution Protocol,” November 1982
- Russel, Ryan and Cunningham, Stace, “Hack Proofing Your Network,” , Syngress Publishing Inc, Copyright 2000
- Song, Dug, Dsniff 2.3, <http://www.monkey.org/~dugsong/>, Copyright 2000

Demonstrations

Demo Environment



Demonstration Tools

- rfarf 1.1
 - Provides ARP relay capability and packet dump for two selected stations
 - Corrects MAC entries upon exiting
- farf 1.1b
 - Passive and active collection of ARP messages
 - DoS Attacks on single hosts
 - DoS Attacks on entire collection
 - Arbitrary and manual input of spoofed MAC addresses

ARP Attacks

- Disclosure attacks
 - ARP relaying for a single target
 - Sniffing attacks
- DoS related
 - Port scan defense
 - DoS attacks on a single host, group, or subnet

Questions

Mike Beekey
beekey@clark.net