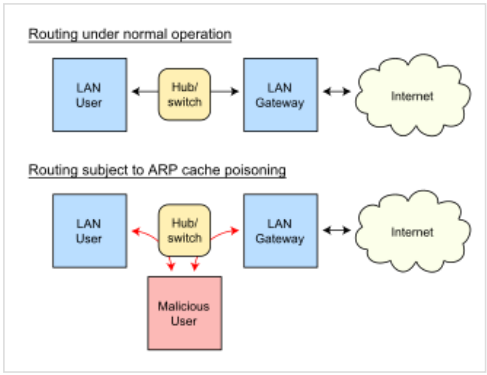
WIKIPEDIA
The Free Encyclopedia

ARP spoofing

In computer networking, **ARP spoofing** (also **ARP cache poisoning** or **ARP poison routing**) is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.[1]

The attack can only be used on networks that use ARP, and requires the attacker to have direct access to the local network segment to be attacked.[2]



A successful ARP spoofing (poisoning) attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack.

ARP vulnerabilities

The Address Resolution Protocol (ARP) is a widely used communications protocol for resolving Internet layer addresses into link layer addresses.

When an Internet Protocol (IP) datagram is sent from one host to another in a local area network, the destination IP address must be resolved to a MAC address for transmission via the data link layer. When another host's IP address is known, and its MAC address is needed, a broadcast packet is sent out on the local network. This packet is known as an *ARP request*. The destination machine with the IP in the ARP request then responds with an *ARP reply* that contains the MAC address for that IP.[2]

ARP is a stateless protocol. Network hosts will automatically cache any ARP replies they receive, regardless of whether network hosts requested them. Even ARP entries that have not yet expired will be overwritten when a new ARP reply packet is received. There is no method in the ARP protocol by which a host can authenticate the peer from which the packet originated. This behavior is the vulnerability that allows ARP spoofing to occur.[1][2][3]

Attack anatomy

The basic principle behind ARP spoofing is to exploit the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN or from an attacker's machine that is connected directly to the target LAN.[4]

Generally, the goal of the attack is to associate the attacker's host MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's host. The attacker may choose to inspect the packets (spying), while forwarding the traffic to the actual default destination to avoid discovery, modify the data before forwarding it (man-in-the-middle attack), or launch a denial-of-service attack by causing some or all of the packets on the network to be dropped.

Defenses

Static ARP entries

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. IP address-to-MAC address mappings in the local ARP cache may be statically entered. Hosts don't need to transmit ARP requests where such entries exist.[5] While static entries provide some security against spoofing, they result in maintenance efforts as address mappings for all systems in the network must be generated and distributed. This does not scale on a large

network since the mapping has to be set for each pair of machines resulting in n^2-n ARP entries that have to be configured when n machines are present; On each machine there must be an ARP entry for every other machine on the network; n-1 ARP entries on each of the n machines.

Detection and prevention software

Software that detects ARP spoofing generally relies on some form of certification or cross-checking of ARP responses. Uncertified ARP responses are then blocked. These techniques may be integrated with the DHCP server so that both dynamic and static IP addresses are certified. This capability may be implemented in individual hosts or may be integrated into Ethernet switches or other network equipment. The existence of multiple IP addresses associated with a single MAC address may indicate an ARP spoof attack, although there are legitimate uses of such a configuration. In a more passive approach, a device listens for ARP replies on a network, and sends a notification via email when an ARP entry changes.[6]

AntiARP[7] also provides Windows-based spoofing prevention at the kernel level. ArpStar is a Linux module for kernel 2.6 and Linksys routers that drops invalid packets that violate mapping, and contains an option to repoison or heal.

Some virtualized environments such as KVM also provide security mechanisms to prevent MAC spoofing between guests running on the same host.[8]

Additionally some Ethernet adapters provide MAC and VLAN anti-spoofing features.[9]

OpenBSD watches passively for hosts impersonating the local host and notifies in case of any attempt to overwrite a permanent entry.[10]

OS security

Operating systems react differently. Linux ignores unsolicited replies, but, on the other hand, uses responses to requests from other machines to update its cache. Solaris accepts updates on entries only after a timeout. In Microsoft Windows, the behavior of the ARP cache can be configured through several registry entries under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, ArpCacheLife, ArpCacheMinReferenceLife, ArpUseEtherSNAP, ArpTRSingleRoute, ArpAlwaysSourceRoute, ArpRetryCount.[11]

Legitimate usage

The techniques that are used in ARP spoofing can also be used to implement redundancy of network services. For example, some software allows a backup server to issue a gratuitous ARP request in order to take over for a defective server and transparently offer redundancy.[12][13] Circle[14] and CUJO are two companies that have commercialized products centered around this strategy.

ARP spoofing is often used by developers to debug IP traffic between two hosts when a switch is in use: if host A and host B are communicating through an Ethernet switch, their traffic would normally be invisible to a third monitoring host M. The developer configures A to have M's MAC address for B, and B to have M's MAC address for A; and also configures M to forward packets. M can now monitor the traffic, exactly as in a man-in-the-middle attack.

Tools

Defense

Name	OS	GUI	Free	Protection	Per interface	Active/passive	Notes
Agnitum Outpost Firewall	Windows	Yes	No	Yes	No	passive	
AntiARP	Windows	Yes	No	Yes	No	active+passive	
Antidote[15]	Linux	No	Yes	No	?	passive	Linux daemon, monitors mappings, unusually large number of ARP packets.
Arp_Antidote[16]	Linux	No	Yes	No	?	passive	Linux Kernel Patch for 2.4.18 – 2.4.20, watches mappings, can define action to take when.
Arpalert	Linux	No	Yes	No	Yes	passive	Predefined list of allowed MAC addresses, alert if MAC that is not in list.
ArpON	Linux	No	Yes	Yes	Yes	active+passive	Portable handler daemon for securing ARP against spoofing, cache poisoning or poison routing attacks in static, dynamic and hybrid networks.
ArpGuard	Mac	Yes	No	Yes	Yes	active+passive	
ArpStar	Linux	No	Yes	Yes	?	passive	
Arpwatch	Linux	No	Yes	No	Yes	passive	Keep mappings of IP-MAC pairs, report changes via Syslog, Email.
ArpwatchNG	Linux	No	Yes	No	No	passive	Keep mappings of IP-MAC pairs, report changes via Syslog, Email.
Colasoft Capsa	Windows	Yes	No	No	Yes	no detection, only analysis with manual inspection	
cSploit[17]	Android (rooted only)	Yes	Yes	No	Yes	passive	
elmoCut[18]	Windows	Yes	Yes	No	?	passive	EyeCandy ARP spoofer for Windows
Prelude IDS	?	?	?	?	?	?	ArpSpoof plugin, basic checks on addresses.
Panda Security	Windows	?	?	Yes	?	Active	Performs basic checks on addresses
remarp	Linux	No	Yes	No	No	passive	
Snort	Windows/Linux	No	Yes	No	Yes	passive	Snort preprocessor Arpspoof, performs basic checks on addresses
Winarpwatch	Windows	No	Yes	No	No	passive	Keep mappings of IP-MAC pairs, report

Name	OS	GUI	Free	Protection	Per interface	Active/passive	Notes
							changes via Syslog, Email.
XArp[19]	Windows, Linux	Yes	Yes (+pro version)	Yes (Linux, pro)	Yes	active + passive	Advanced ARP spoofing detection, active probing and passive checks. Two user interfaces: normal view with predefined security levels, pro view with per-interface configuration of detection modules and active validation. Windows and Linux, GUI-based.
Seconfig XP	Windows 2000/XP/2003 only	Yes	Yes	Yes	No	only activates protection built-in some versions of Windows	
zANTI	Android (rooted only)	Yes	Yes	No	?	passive	
NetSec Framework	Linux	No	Yes	No	No	active	
anti-arpspoof[20]	Windows	Yes	Yes	?	?	?	
DefendARP:[21]	?	?	?	?	?	?	A host-based ARP table monitoring and defense tool designed for use when connecting to public wifi. DefendARP detects ARP poisoning attacks, corrects the poisoned entry, and identifies the MAC and IP address of the attacker.
NetCutDefender:[22]	Windows	?	?	?	?	?	GUI for Windows that can protect from ARP attacks

Spoofing

Some of the tools that can be used to carry out ARP spoofing attacks:

- Dsniff
- Ettercap
- arping[23]
- Cain and Abel

See also

- Cache poisoning
- DNS spoofing
- IP address spoofing
- MAC spoofing
- Proxy ARP

References

1. Ramachandran, Vivek & Nandi, Sukumar (2005). "Detecting ARP Spoofing: An Active Technique" (https://books.

google.com/books?id=4LmERFxBzSUC&pg=PA239). In Jajodia, Suchil & Mazumdar, Chandan (eds.). *Information systems security: first international conference, ICISS 2005, Kolkata, India, December 19–21, 2005 : proceedings*. Birkhauser. p. 239. ISBN 978-3-540-30706-8.

2. Lockhart, Andrew (2007). *Network security hacks* (https://archive.org/details/networksecurityh02edunse). O'Reilly. p. 184 (https://archive.org/details/networksecurityh02edunse/page/184). ISBN 978-0-596-52763-1.
3. Steve Gibson (2005-12-11). "ARP Cache Poisoning" (https://www.grc.com/nat/arp.htm). GRC.
4. Moon, Daesung; Lee, Jae Dong; Jeong, Young-Sik; Park, Jong Hyuk (2014-12-19). "RTNSS: a routing trace-based network security system for preventing ARP spoofing attacks" (https://dx.doi.org/10.1007/s11227-014-1353-0). *The Journal of Supercomputing*. **72** (5): 1740–1756. doi:10.1007/s11227-014-1353-0 (https://doi.org/10.1007%2Fs11227-014-1353-0). ISSN 0920-8542 (https://search.worldcat.org/issn/0920-8542). S2CID 18861134 (https://api.semanticscholar.org/CorpusID:18861134). Archived (https://web.archive.org/web/20210123000940/https://link.springer.com/article/10.1007/s11227-014-1353-0) from the original on 2021-01-23. Retrieved 2021-01-23.
5. Lockhart, Andrew (2007). *Network security hacks* (https://archive.org/details/networksecurityh02edunse). O'Reilly. p. 186 (https://archive.org/details/networksecurityh02edunse/page/186). ISBN 978-0-596-52763-1.
6. "A Security Approach to Prevent ARP Poisoning and Defensive tools" (https://www.researchgate.net/publication/282568321). *ResearchGate*. Archived (https://web.archive.org/web/20190503221834/https://www.researchgate.net/publication/282568321_A_Security_Approach_to_Prevent_ARP_Poisoning_and_Defensive_tools) from the original on 2019-05-03. Retrieved 2019-03-22.
7. AntiARP (http://www.antiarp.com/english.html) Archived (https://web.archive.org/web/20110606051646/http://www.antiarp.com/english.html) June 6, 2011, at the Wayback Machine
8. "Daniel P. Berrangé » Blog Archive » Guest MAC spoofing denial of service and preventing it with libvirt and KVM" (https://www.berrange.com/posts/2011/10/03/guest-mac-spoofing-denial-of-service-and-preventing-it-with-libvirt-and-kvm/). Archived (https://web.archive.org/web/20190809113318/https://www.berrange.com/posts/2011/10/03/guest-mac-spoofing-denial-of-service-and-preventing-it-with-libvirt-and-kvm/) from the original on 2019-08-09. Retrieved 2019-08-09.
9. "Archived copy" (https://downloadmirror.intel.com/26556/eng/README.txt). Archived (https://web.archive.org/web/20190903084638/https://downloadmirror.intel.com/26556/eng/README.txt) from the original on 2019-09-03. Retrieved 2019-08-09.
10. "Arp(4) - OpenBSD manual pages" (https://man.openbsd.org/arp.4). Archived (https://web.archive.org/web/20190809120053/https://man.openbsd.org/arp.4) from the original on 2019-08-09. Retrieved 2019-08-09.
11. "Address Resolution Protocol" (https://technet.microsoft.com/en-us/library/cc940021.aspx). 18 July 2012. Archived (https://web.archive.org/web/20210123000849/https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940021(v=technet.10)?redirectedfrom=MSDN) from the original on 2021-01-23. Retrieved 2017-08-26.
12. "OpenBSD manpage for CARP (4)" (https://man.openbsd.org/carp.4). Archived (https://web.archive.org/web/20180205000848/https://man.openbsd.org/carp.4) from the original on 2018-02-05. Retrieved 2018-02-04., retrieved 2018-02-04
13. Simon Horman. "Ultra Monkey: IP Address Takeover" (http://www.ultramonkey.org/3/ip_address_takeover.html). Archived (https://web.archive.org/web/20121118031514/http://www.ultramonkey.org/3/ip_address_takeover.html) from the original on 2012-11-18. Retrieved 2013-01-04., retrieved 2013-01-04
14. Barrett, Brian. "Circle with Disney Locks Down Kids Devices from Afar" (https://www.wired.com/2015/11/circle-with-disney-locks-down-kids-devices-from-afar). *Wired*. Archived (https://web.archive.org/web/20161012230841/https://www.wired.com/2015/11/circle-with-disney-locks-down-kids-devices-from-afar) from the original on 2016-10-12. Retrieved 2016-10-12., retrieved 2016-10-12
15. "Antidote" (https://antidote.sourceforge.net/). Archived (https://web.archive.org/web/20120313121350/http://antidote.sourceforge.net/) from the original on 2012-03-13. Retrieved 2014-04-07.
16. "Arp_Antidote" (https://web.archive.org/web/20120114185136/http://burbon04.gmxhome.de/linux/ARPSpoofing.html). Archived from the original (http://burbon04.gmxhome.de/linux/ARPSpoofing.html) on 2012-01-14. Retrieved 2011-08-02.
17. "cSploit" (http://www.csploit.org/). tux_mind. Archived (https://web.archive.org/web/20190312042507/http://www.csploit.org/) from the original on 2019-03-12. Retrieved 2015-10-17.
18. "elmoCut: EyeCandy ARP Spoofer (GitHub Home Page)" (https://github.com/elmoiv/elmocut). *GitHub*.
19. "XArp" (http://www.xarp.net/). Archived (https://web.archive.org/web/20200616221850/http://www.xarp.net/) from the original on 2020-06-16. Retrieved 2021-01-23.
20. anti-arpspoof (https://web.archive.org/web/20080831003151/http://sync-io.net/Sec/anti-arpspoof.aspx)

21. "Defense Scripts | ARP Poisoning" (http://arppoisoning.com/defense-scripts/). Archived (https://web.archive.org/web/20130122062207/http://arppoisoning.com/defense-scripts/) from the original on 2013-01-22. Retrieved 2013-06-08.
22. "Netcut defender | Arcai.com" (http://www.arcai.com/netcut-defender/). Archived (https://web.archive.org/web/20190408110511/http://arcai.com/netcut-defender/) from the original on 2019-04-08. Retrieved 2018-02-07.
23. "ARP Vulnerabilities: The Complete Documentation" (https://web.archive.org/web/20110305160956/http://www.l0t3k.org/security/tools/arp/). L0T3K. Archived from the original (http://www.l0t3k.org/security/tools/arp/) on 2011-03-05. Retrieved 2011-05-03.

External links

- Stephanie Reigns (2014-10-07). "Clearing your ARP cache on Linux" (https://web.archive.org/web/20190408110518/https://coderseye.com/how-to-clear-arp-cache-on-linux-or-unix/). Coders Eye. Archived from the original (http://coderseye.com/how-to-clear-arp-cache-on-linux-or-unix/) on 2019-04-08. Retrieved 2018-03-05.