

Securing ARP

*An overview of threats,
approaches, and solutions*

version 0.2.0

Christoph Mayer
www.chrismc.de

Agenda

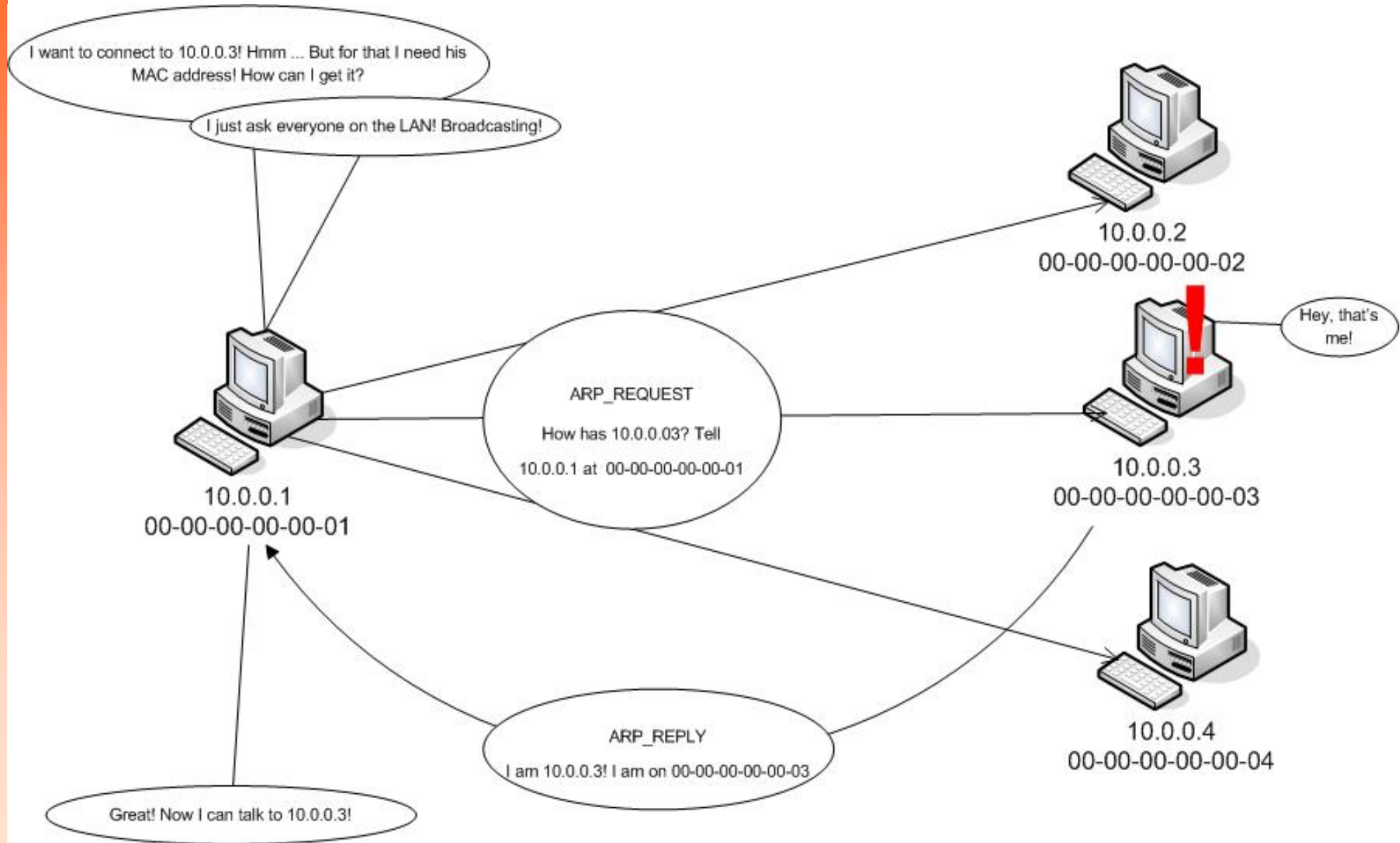
1. ARP basics
2. Attacks on ARP
3. System approaches
4. Hardware approaches
5. Middleware approaches
6. Cryptographic approaches
7. IPv6 Neighbour discovery protocol
8. Conclusions
9. References

- 1. ARP basics -

Address Resolution Protocol (ARP)

- Resolution of IP to MAC addresses
- RFC 826 and extensions [1]
- Stateless request and reply messages
- Essential in Ethernet-based networks

How ARP works (1)

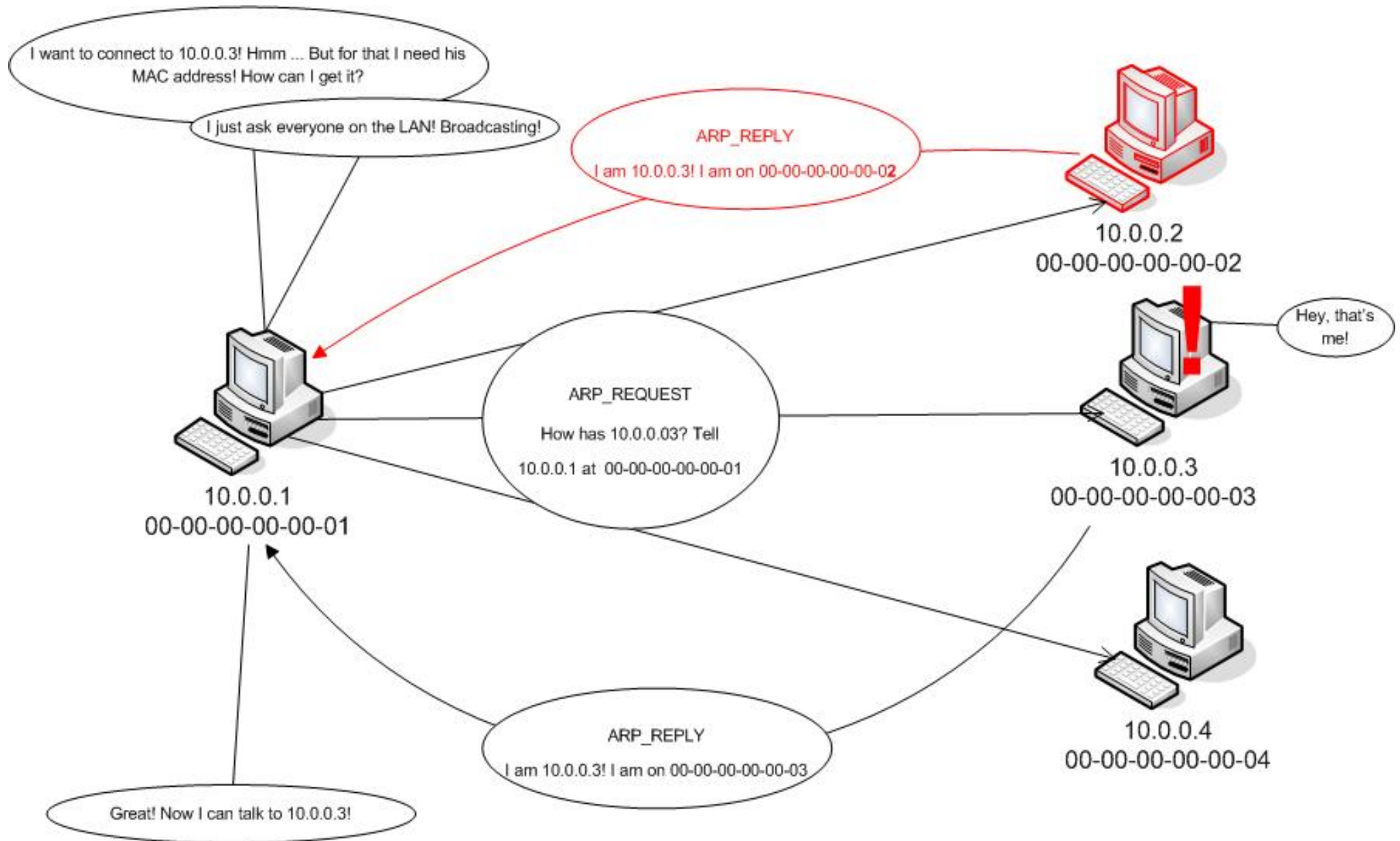


How ARP works (2)

- Why
 - Ethernet-based communication through MAC addresses
 - Resolution of IP to MAC addresses necessary
- How
 - Broadcasted requests include destination IP address
 - Machine with configured IP address replies with its MAC address
- For an excessive introduction see [2,3]

- 2. Attacks on ARP -

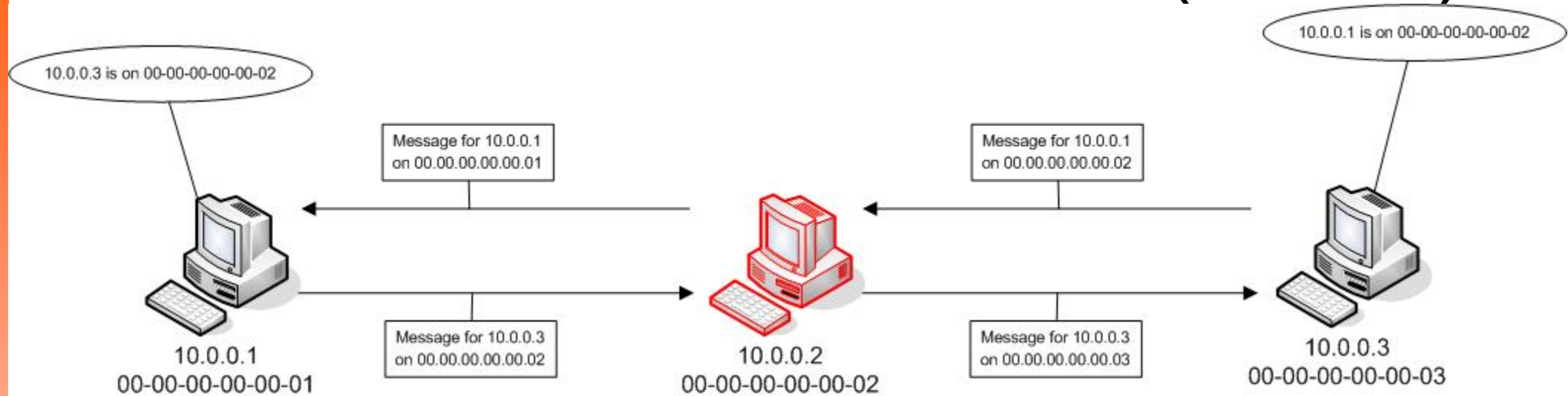
ARP spoofing (1)



ARP spoofing (2)

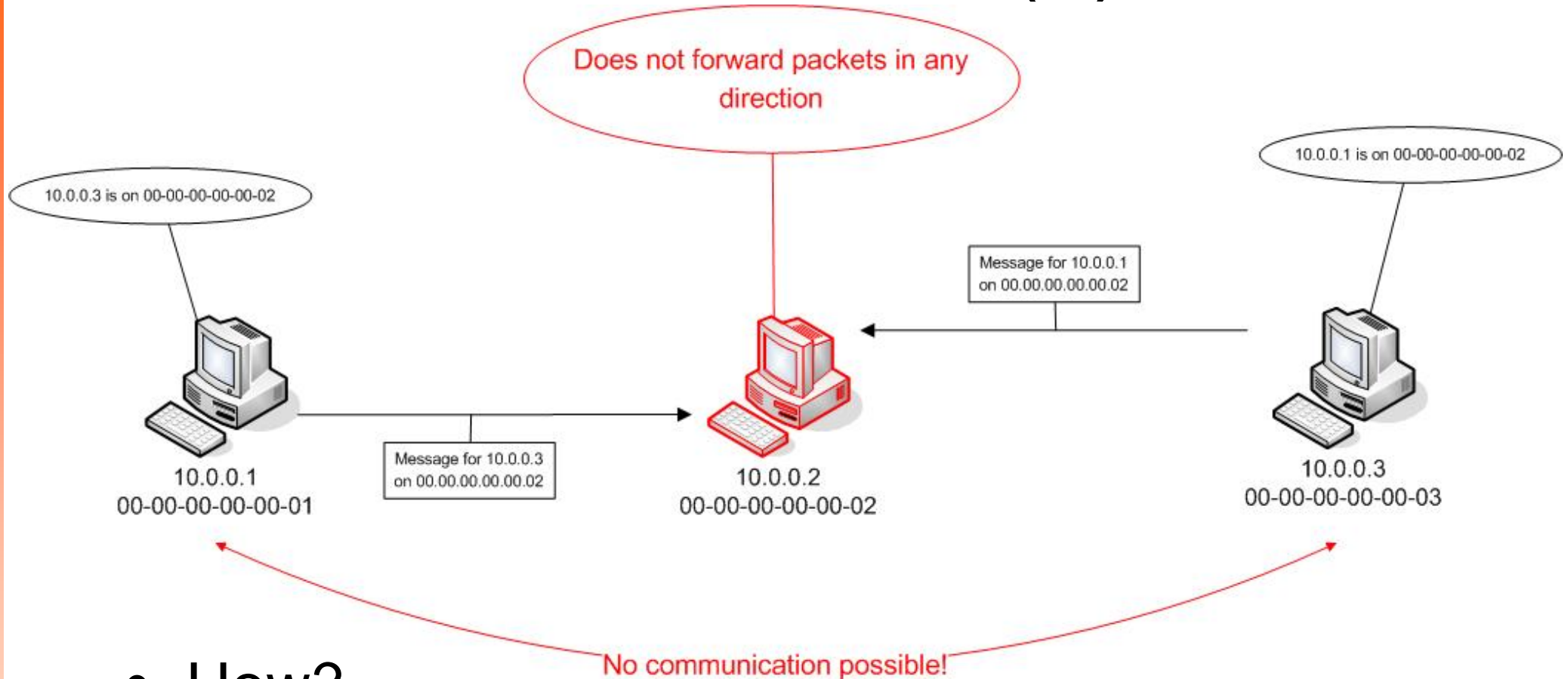
- Attacker manipulates victims ARP mappings
 - IP to MAC mappings cached in local ARP cache
 - Most OS update cache even if no request was sent
 - Most OS overwrite cache entries silently
- Impact: Masquerade as someone else
 - *10.0.0.2* masquerades as *10.0.0.3*
 - All traffic from *10.0.0.1* to *10.0.0.3* will be sent to *10.0.0.2*
 - *10.0.0.2* can sniff, manipulate, inject traffic!

Man in the middle attack (MITM)



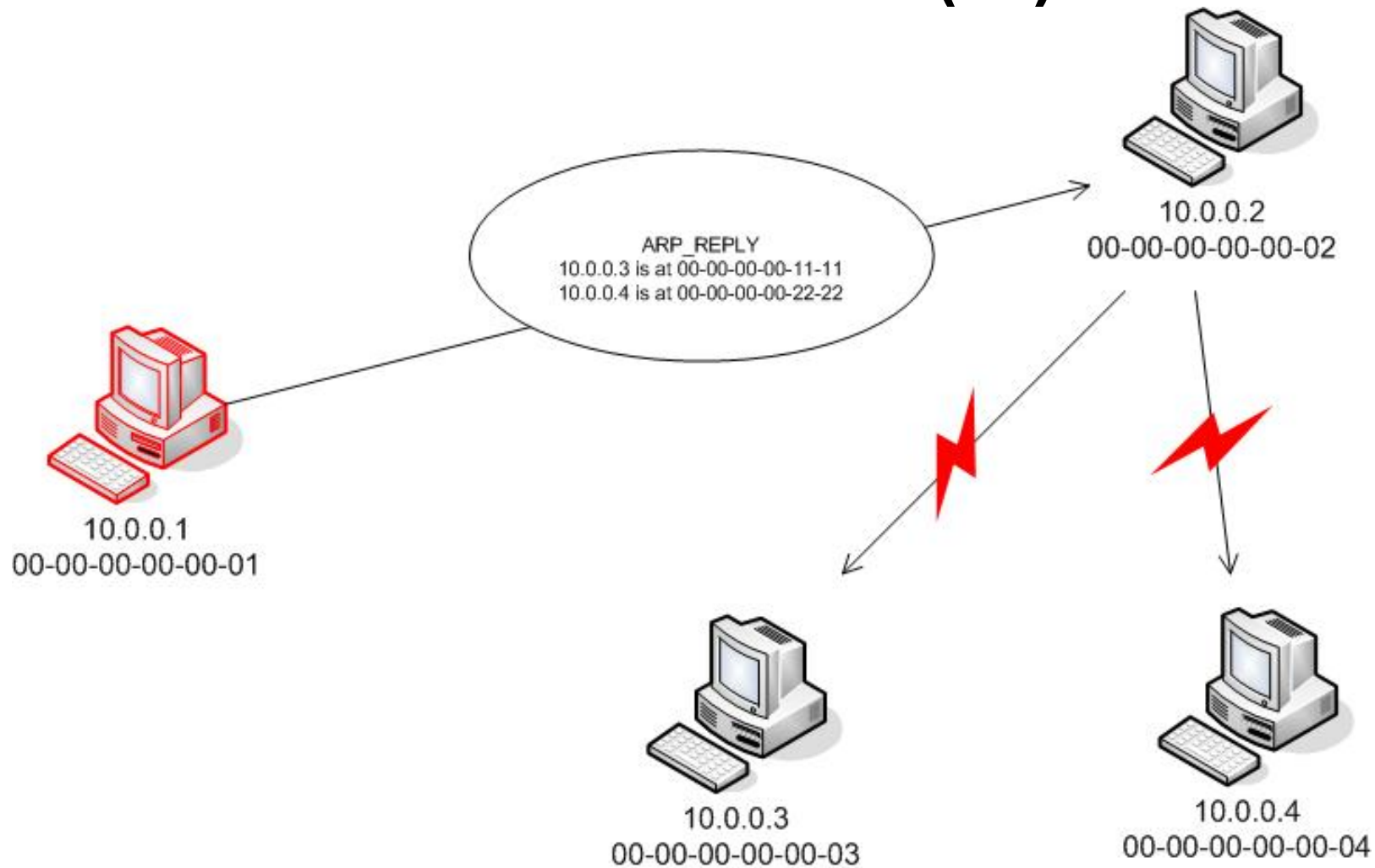
- How?
 - *10.0.0.2* can poison ARP cache of *10.0.0.1* and *10.0.0.3*
- Impact
 - Attacker can eavesdrop/modify the communication between the two hosts
 - Even attacks on SSL and SSH [22]

DoS attacks (1)



- How?
 - Man-in-the-middle attack
 - Attacker does not forward data
- Impact
 - No communication between *10.0.0.1* and *10.0.0.3*

DoS attacks (2)



- Even easier than DoS attack shown in (1)
- Poison cache of host with fake MAC addresses

DoS attacks (3)

- Summary of ARP-based DoS attacks
 - Attacker can completely cut off communication between arbitrary hosts
 - Cut off communication to routers, servers, gateway, ...
 - Debugging an ARP-posioned network can be hard

Highjacking

- What?
 - Take over a communication session
- How?
 - Using simple ARP spoofing
- E.g. take over a telnet session after the user has logged in

Overview of ARP Attacks

- Attack methods
 - Man-in-the-middle attack
 - Denial of Service
 - Session hijacking
- Further reading
 - Introduction to ARP spoofing [6]
 - ARP attacks on SSH1, IPSec, HTTPS [15]
 - ARP attacks first mentioned by Yuri Volobuev [27]

Q: *„But I am using a firewall!“*

A: *„Unfortunately hardly any firewall protects against ARP-driven attacks!“*

ARP attack tools

- Ettercap
 - Inbuilt data manipulation, password sniffing
 - GUI-based and user written script support
- Cain&Abel [4]
 - Inbuilt password sniffing and cracking
 - GUI-based and very excessive and easy to use
- Dsniff: Suite for ARP related attacks
- Parasite: Can perform DoS
- Brian [24]: Disable switching on switched LAN
- More? Arppoison, Seringe, Arp-sk, ... lots more!

How real is the threat? (1)

- Performing ARP attacks
 - Very easy to perform
 - Excessive tools, GUI support (e.g. Cain&Abel [4])
- Impact of ARP-based attacks
 - Eavesdropping, DoS, data manipulation, hijacking
- Detection of ARP attacks
 - No OS security, firewall security very rudimentary
 - ARP security often ignored, no one cares about lower layer security

→ *ARP attacks are real threat with high impact*

How real is the threat? (2)

Q: *„ARP attacks are only possible from inside the network, so why worry?“*

A: *„Experts say insider hacking represents about 70% of all malicious attacks and causes \$1 billion in damages each year to U.S. businesses“ [9,10,11]*

- 3. System approaches -

Static ARP cache entries

- Add static entries to local ARP cache
 - Static entries can not be manipulated through ARP spoofing
- Huge administrative effort
 - Lots of hosts to configure
 - One new/changed host affects all hosts
- Good for individuals to secure ones gateway
- On Windows 2000/XP patches are needed, otherwise static entries are overwritten [5]

OS security

- General
 - Every OS has different network stack and behaviour
 - Each network card has different drivers and firmware with their own behaviour
 - Even the same OS may behave differently depending on network stack version, driver, and firmware version
- Linux
 - Kernel 2.4 does not react to unsolicited replies
 - But: Inserts mappings from requests into cache
- Solaris
 - Only accepts ARP updates after timeout period [6]

OS security (2)

- Windows
 - No inbuilt ARP security, not even in Vista [28]
 - Registry settings affect ARP behaviour [29]
 - *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters*
 - *ArpCacheLife, ArpCacheMinReferenceLife, ArpUseEtherSNAP, ArpTRSingleRoute, ArpAlwaysSourceRoute, ArpRetryCount*
 - Windows 2000/XP need the right patches to preserve static ARP entries [5]

- 4. Hardware approaches -

Switches

- How does it protect against ARP attacks?
 - Switch learns the port where a MAC address is connected to
 - Frames are only forwarded to the correct port, not broadcasted
- Drawback
 - Widespread misunderstanding that switches protect against ARP attacks
 - Easy to execute ARP attacks on switched network
 - Provides security that can easily be tricked

Virtual LANs (VLANs)

- How does it prevent ARP attacks?
 - Segmentation of broadcast domain
 - No ARP used between segments, only inside a segment
 - Separate critical hosts from possible users
- Drawbacks
 - Some switches allow only limited number of VLANs
 - Denial of Service still possible [8]
 - VLANs have their own set of vulnerabilities
 - Administrative effort which can only lower, but not eliminate the risk

Port Security

- How does it prevent ARP attacks?
 - Security feature on highend switches
 - Bind switch port to specified MAC address
 - Manual binding or intelligent learning
- Drawback
 - Easy to circumvent [6,7]
 - Prevents only against some simple ARP attacks Provides only low security

ARPDefender

- How does it prevent ARP attacks?
 - Hardware box running Arpwatch
 - Arpwatch does the actual work
 - Do mistake as ArpDefender software by Nick Dickerson
- Drawback
 - Why would you buy a blade with nothing but Arpwatch running for over 500\$?
 - Same security as Arpwatch

ArpGuard

- How does it prevent ARP attacks?
 - Keeps track of MAC-IP mappings
 - Alerts changes and invalid mappings
- Drawback
 - Very expensive
 - Can not prevent ARP attacks, only detect
 - Administrative interface over https, can be attacked using ARP MITM [15]

- 5. Middleware approaches -

Detecting ARP attacks using middleware approaches

- How to detect ARP spoofing
 - Don't change/extend ARP protocol
 - Watch the local ARP cache for changes
 - Analyze ARP packets
 - Actively validate mappings
- Examples of suspicious ARP behaviour
 - Was a request sent to a given reply?
 - ARP packet valid in regard to static mappings?
 - Invalid MAC addresses, e.g. broadcast, in reply?
 - Does an ARP packet break current mappings?

Arpwatch/Arpwatch NG/Winarpwatch

- Arpwatch
 - Keep database of IP-MAC mappings
 - Report changes via Syslog/Email
- Extended version Arpwatch NG
- Windows port Winarpwatch
 - Not available for Windows XP

Antidote

- Demon for Linux that detects ARP attacks
- Analytics modules
 - Unusually large number of ARP packets
 - IP-MAC mapping changes
 - Difference between ARP and Ethernet MAC
- Report suspicious activity using Syslog, Email

remarp

- Remarp: Remote Arpwatch
- SNMP-based ARP monitoring
 - Collect ARP mapping from devices using SNMP
 - Check mappings for changes and alert

Arp_Antidote

- Linux Kernel Patch for 2.4.18 - 2.4.20
- Watches IP-MAC mappings
- Define action when mapping changes
 - Update cache, validate mapping through ARP request, report, make mapping static, mark mapping banned
- Security and actions can be tricked [15]
- More information available in [12, 13, 14]

Anticap

- Kernel patch for Linux 2.2/2.4, FreeBSD 4.6, NetBSD 1.5
- Prevents mappings from being overwritten with
 - No security if mapping not yet in cache
- Pure kernel mode processing
 - Linux Kernel 2.2/2.4 not preemptive
- Available in [16]

ArpStar

- Linux module for kernel 2.6 and Linksys router
 - Filter hook for ARP handling
 - All processing in kernel mode
 - Susceptible to system stability and DoS
- Drops invalid packets and prevent ARP attacks
- Option to repoison and thus heal other hosts
- Different analytic modules and heuristics
- Packet inspection directly as packets arrive
 - No queueing, thus decreasing network performance

SnoopNetCop

- Monitoring of local ARP cache
 - Periodicall fetch mappings from local ARP cache
 - Alert changes and invalid mappings
 - Similar to XArp 0.1.5
- Product website is no longer available

Snort

- Snort preprocessor Arpspoof
- Perform security checks
 - Ethernet MAC matches ARP MAC
 - Sender MAC is Unicast address
 - Few more
- Too few checks performed
 - Can only detect trivial ARP attacks [30]

XArp 0.1.5

- Periodically request local ARP cache for mappings
 - Build up database of active and old mappings
- Analytic modules
 - Changed IP-MAC mappings
 - Suspicious IP, or MAC address (broadcast MAC, etc.)
- GUI driven and very easy to use
- Can detect most ARP attacks
- Available for Windows [26]

XArp 2

- XArp 2 - Advanced ARP spoofing detection
- Different detection/validation methods
 - Active: Discover the network and validate
 - Quick and intense discovery methods
 - Passive: Analyze all ARP packets
 - Lots of different analytical modules that can be employed
- Strong graphical support with two GUIs
 - Normal user GUI: Choose security level
 - Advanced user GUI: Select each active and passive module with lots of configuration details
- Can even detect attacks against remote machines in the network

ArpDefender

- Master thesis [19], University of Maryland
- Command line Perl script using Tetheral
- Implementation or source not available

Prelude IDS

- ArpSpooF plugin
 - Is request sent to unicast address?
 - Ethernet source/destination MAC different from ARP source/destination MAC
 - Cooperation with Arpwatch
- Drawback
 - Only small advantage over arpwatch itself
 - Too less checks on ARP packets

Agnitum Outpost Firewall

- Outpost Firewall Pro v3.0
- „Smart ARP filtering“: Reply only accepted if request sent
 - First reply to request is accepted
 - Race condition that an attacker can win easily
 - Further attacks possible

AntiARP

- ARP spoofing prevention for Windows
 - Use NDIS driver for ARP packet drop
- Drawback
 - Unknown which checks are performed
 - Only passive methods, no mapping validation
 - NDIS driver looks unprofessional
 - Derived from the DDK samples (comments included)
 - Driver can crash the OS easily
 - Website does not give much information, mostly in Chinese

Arpalert

- Predefined list of authorized MAC addresses
- Alert if unauthorized MAC address is seen
- Can detect abnormal ARP behaviour
 - E.g. ARP flood
- Available for Linux, Solaris and BSD [25]

Colasoft Capsa

- Network troubleshooting application
- Can alert
 - ARP storms
 - Unbalanced number of ARP request and reply packets
- Drawback
 - ARP storms are no indicator for ARP attacks
 - Neither are unbalanced request/reply packets
 - Cain&Abel e.g. uses very small number of packets for an ARP attacks
 - Seringe does only answer to requests with spoofed mapping

Further interesting papers

- Carnut and Gondim. *ARP spoofing detection on switched ethernet networks: a feasibility study*
- Altunbasak, Krasser, Sokol, Grimminger, Huth. *Addressing the weak link between layer 2 and layer 3 in the internet architecture*

- 6. Cryptographic approaches -

S-ARP

- Public key crypto, keys signed by LAN CA
- ARP packets signed digitally
- Drawback
 - Does only authenticate Link layer
 - Can use IPSec which provides higher layer security
- Available in [21]

T-ARP

- <http://siis.cse.psu.edu/tools/tarp.tar>
- TODO

O-ARP

- TODO

Secure Link Layer (SSL)

- Provide authentication and encrypted communication at link layer
- Need Certificate Authority (CA)
- Encryption slows down network and does not provide additional security for link layer
- Kernel patch
 - All keys are kept in kernel space memory
 - All cryptographic operations in kernel mode
 - Thus impact on system performance
- Available in [20]

L2Auth

- Research project, University California
 - ARP-requests have limited lifetime to prevent unsolicited ARP
 - Validate ARP-response through third-party
 - Third-party sends signed resolution reply
 - Third-party public key must be distributed
- Proof-of-concept implementation in Java using virtual networking environment [18]

Secarp

- TODO

Arptree

- **A New Architecture for Address Resolution**

A secure address resolution protocol

- [http://citeseer.ist.psu.edu/cache/papers/cs/30116/http:zSzzSzwww.cs.utexas.eduSzuserszSzchuangzSzcomnet0103.pdf/a-secure-addressresolbb-u.pdf](http://citeseer.ist.psu.edu/cache/papers/cs/30116/http%3A%2F%2Fwww.cs.utexas.edu%2Fusers%2Fchuang%2Fcomnet0103.pdf/a-secure-address-resolbb-u.pdf)

- Tripunitara and Dutta - A middleware approach to asynchronous and backward compatible detection and prevention of arp cache poisoning.

IEEE 802.1x Working Groups

- 802.1AR - Secure Device Identity
 - <http://www.ieee802.org/1/pages/802.1ar.html>
 - Draft 0.7, 10 Nov 2006
- 802.1af - Media Access Control Key Security
 - <http://www.ieee802.org/1/pages/802.1af.html>
 - Draft 1.0, 12 Nov 2006
- 802.11i - TODO

7. IPv6 Neighbor Discovery Protocol

- <http://tools.ietf.org/id/draft-ietf-v6ops-security-overview-02.txt>
- <http://www.ietf.org/rfc/rfc2461.txt>
- <http://www.ietf.org/rfc/rfc3756.txt>
- <http://www.securityfocus.com/bid/23293>
- <http://tools.ietf.org/html/draft-pashby-ipv6-detecting-spoofing-00>
 - <http://www3.ietf.org/proceedings/05aug/slides/ipv6-8.pdf>
- <http://www.inrialpes.fr/planete/splash/PDF/infocom05.pdf>
- http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf

8. Conclusion

- Take homes
 - ARP attacks pose a real threat in LANs
 - Easy to launch, big impact, hard to defend
 - Ongoing research and development
 - Lots of applications, few satisfying solutions

Protect yourself!

(e.g. with XArp 2)

9. References

- [1] Overview of ARP and ARP related RFC's
<http://www.networksorcery.com/enp/protocol/arp.htm>
- [2] Address Resolution Protocol (arp)
<http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>
- [3] An Ethernet Address Resolution Protocol
<http://www.rfc-archive.org/getrfc.php?rfc=826>
- [4] Cain&Abel
<http://www.oxid.it/cain.html>
- [5] Static ARP more dynamic than you might think! Blog on
<http://www.chrismc.de>
- [6] An Introduction to ARP Spoofing
<http://node99.org/projects/arpspoof/arpspoof.pdf>
- [7] Mailing list article - Re: switch jamming
<http://cert.uni-stuttgart.de/archive/vuln-dev/2002/01/msg00295.html>
- [8] Heise Security – Angriff von innen, Page 4
<http://www.heise.de/security/artikel/55269/3>
- [9] BusinessWeek Online - When the Hacker Is on the Inside
http://www.businessweek.com/bwdaily/dnflash/dec2000/nf20001213_253.htm
- [10] BBC News - Hacking usually "an inside job",
<http://news.bbc.co.uk/1/hi/sci/tech/203547.stm>
- [11] IT-Week - Most computer hacking an 'inside job',
<http://www.itweek.co.uk/vnunet/news/2127220/computer-hacking-inside-job>

References (2)

- [12] Arp_Antidote kernel patch
<http://www.securitylab.ru/tools/antidote.diff.gz>
- [13] Russian article about Arp_Antidote
<http://www.securitylab.ru/analytics/216229.php>
- [14] BugTraq - arp spoofing defence – article about Arp_Antidote
<http://www.securityfocus.com/archive/1/299929/2002-11-13/2002-11-19/0>
- [15] Blackhat Conference 2003 - Man in the middle attacks
<http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf>
- [16] Anticap kernel patch
<http://cvs.antifork.org/cvsweb.cgi/anticap/>
- [17] Daiji Sanai - Promiscuous mode detection using ARP packets
<http://www.blackhat.com/presentations/bh-usa-01/DaijiSanai/bh-usa-01-Sanai.ppt>
- [18] Sean Whalen, Matt Bishop – Layer 2 Authentication
<http://www.node99.org/projects/l2auth/l2auth.pdf>
- [19] Nicholas Dickerson – Detecting and Recovering from ARP Cache Poisoning Attacks
<https://nickdickerson.com/arpdefender/arpdefender.pdf>
- [20] F. Hunleth . Secure Link Layer
<http://www.cs.wustl.edu/fifhunleth/projects/projects.html>
- [21] Brusci, Ornaghi, Rosti – S-ARP: A Secure Address Resolution Protocol
<http://www.acsac.org/2003/papers/111.pdf>
- [22] Peter Burkholder – SSL Man-in-the-Middle Attacks

References (3)

- [23] Spangler - Packet Sniffer Detection with AntiSniff
<http://www.packetwatch.net/documents/papers/snifferdetection.pdf>
- [24] Brian
<http://www.bournemouthbynight.co.uk/tools/>
- [25] Arpalert
<http://www.arpalert.org>
- [26] Xarp
<http://www.chrismc.de>
- [27] ARP and ICMP redirection Games, Yuri Volobuev
<http://insecure.org/sploits/arp.games.html>
- [28] Symantec Vista Security Overview
http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM
- [29] Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference
Thomas Lee and Joseph Davies, Chapter 3: Adress Resolution Protocol (ARP)
- [30] Interner Zugriff: Angriffstechniken im lokalen Netz: ARP-Spoofing und –Poisoning
Linux Magazin 6/2004, Demuth and Leitner
<http://www.linux-magazin.de/Artikel/ausgabe/2004/06>

Detection of rouge machines

- Think you can detect machines that perform ARP spoofing using promiscuous mode detection?
- Don't need to switch to promiscuous mode to perform ARP driven attacks
- So don't bother about detecting this ...
- But: promiscuous nodes can be detected using special crafted ARP packets! [17, 23]