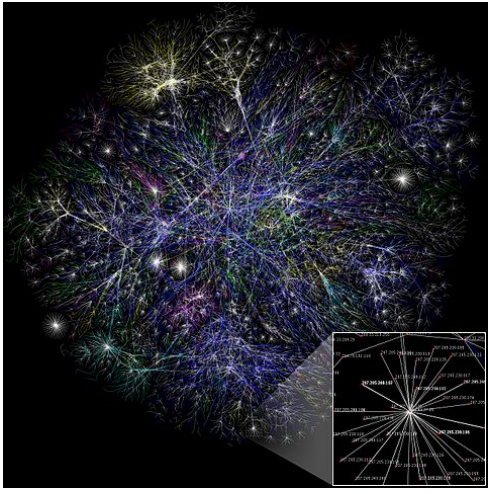
Computer Security (aka, Cybersecurity)

Dr. Chris Mayfield

Department of Computer Science
James Madison University

Sep 30, 2014

WWW stands for "World Wide Web"



WWW stands for "Wild Wild West"

Reality check

The Internet is an open network

- Designs are in the public domain
- Built by the people, for the people

Anyone can send a packet anywhere

- Endpoints don't have to receive them
- Principle of Network Neutrality
  - All data/packets should be treated equally
  - ISPs and governments should not discriminate

Openness drives innovation

- Side effect: "anything goes" (good/bad)
- New applications coming out all the time

What does “security” mean?

Access control

As a human being, you have the right to control

- your information (data, files, identity, ...)
- your property (computers, phones, TVs, ...)

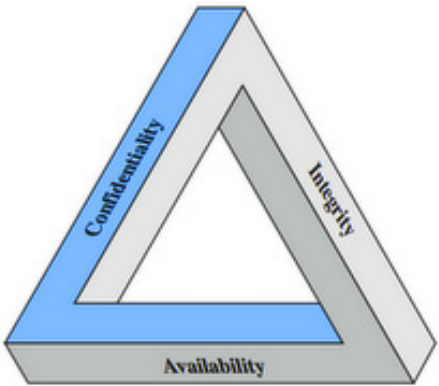
Control means to allow or to restrict access

- in an environment where "anything goes"

Computer security is part of information security (InfoSec)

- See http://en.wikipedia.org/wiki/Information_security
- "Defend from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction."

CIA triad



Source: digitalthreat.net

Three fundamental aspects of information security

Affects the way information is:

- Stored
- Processed
- Transmitted

What can go wrong?

And what can be done about it?

(Terminology: threats and solutions)

OS security

Threats

- Unauthorized access
- Insecure passwords
- Malicious processes
- Vulnerabilities in OS
- Key loggers, sniffers

Solutions

- User accounts, permissions
- Password policies, auditing
- CPU privileged instructions
- Security updates, patches
- Trusted software sources

Network security

Threats

- Unauthorized access
- Virus, worm
- Trojan horse
- Spyware, phishing
- Denial of service

Solutions

- Firewall (hardware/software)
- Antivirus software (maybe)
- Intrusion detection system
- Content filtering, education
- Redirection/dropping packets

Spoiler Alert!

Perfect security is impossible

Possible, but worth preparing for?

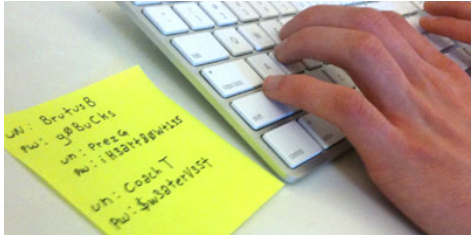
Security in practice

Securing a system is a continual process

- Cost/benefit analysis of threats/solutions

Trade-off of functionality and security

- Too invasive $\rightarrow$ users undermine the system

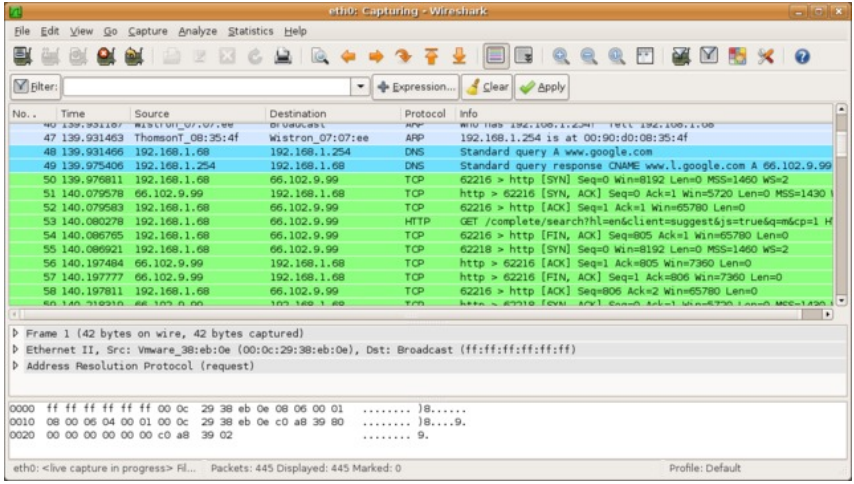


Source: digitalunion.osu.edu

Two more problems

(that encryption can solve)

Sniffing


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
No.. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Cryptography

Symmetric encryption

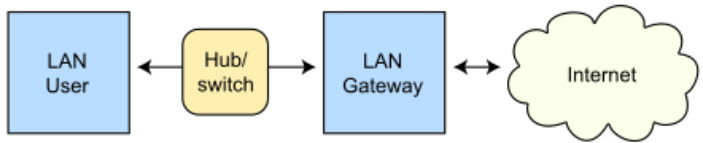
- Secret key (mathematical formula) encodes data
- Chances of guessing the key is nearly impossible
- Problem: how do a server/client agree on a key?

Public-key encryption

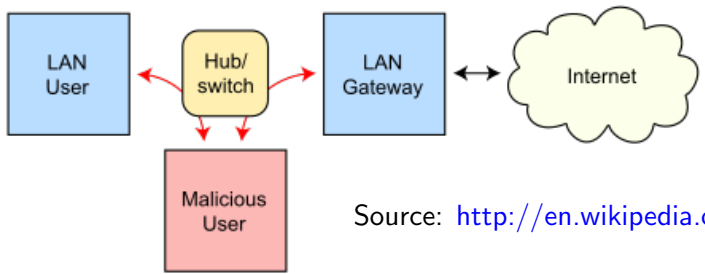
- Generate a pair of keys (make one public, one private)
  - You can't figure out one, given the other
  - But the keys are "inverses" of each other
- Anyone can use your public key to send you a message
  - And you use your private key to decrypt it
  - Also useful for establishing your identify

Spoofing

Routing under normal operation



Routing subject to ARP cache poisoning



Source: http://en.wikipedia.org/wiki/ARP_spoofing

Digital signatures

Certificate authorities

- Symantec (VeriSign, Thawte, Geotrust)
- Comodo Group
- Go Daddy

Solution: verify the identify of servers

- When you use HTTPS, you browser gets certificate of server
- The certificate has been encrypted with a CA's private key
- Your browser uses the CA's public key to decrypt the cert
- If everything checks out, you know you have the right server

How do we prosecute the bad guys?

Legal approaches

Problems

- Information theft
- Eavesdropping
- Distributed DoS
- Cybersquatting

Legislation

- "Anything of value" (CFAA)
- Information privacy (ECPA)
- Monitoring (USA PATRIOT)
- Registered trademarks (ACPA)

Advice and tips

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

http://www.us-cert.gov/ncas/tips