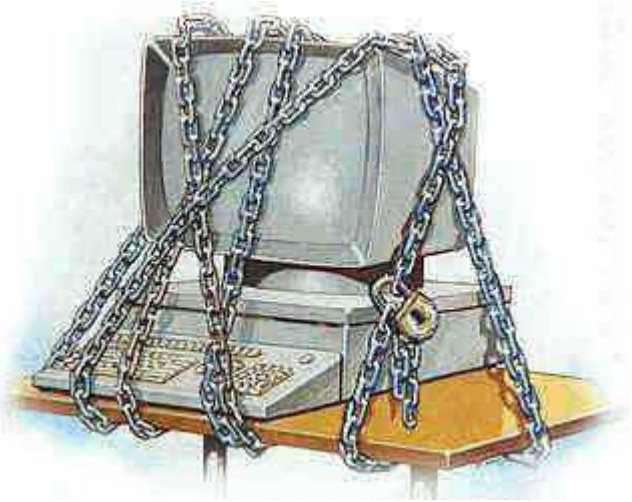
# Introduction to Computer & Networking Security

Dr. Guofei Gu

http://faculty.cse.tamu.edu/guofei/


SECURITY
RISK
HOW SAFE IS YOUR
COMPUTER?




IS IT SAFE?

# Some Bedtime Stories

# Denial of Service

## Estonia recovers from massive denial-of-service attack

*By Jeremy Kirk , IDG News Service , 05/17/2007*



A spree of denial-of-service (DOS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, CSO for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

"Yes, it's serious problem, but we are up and running," Aarelaid said.



Aarelaid said analysts have found postings on Web sites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the United States, Canada, Brazil, Vietnam and others have been used in the attacks, he said.

# Your YouTube Traffic: Pwned!

## Insecure routing redirects YouTube to Pakistan

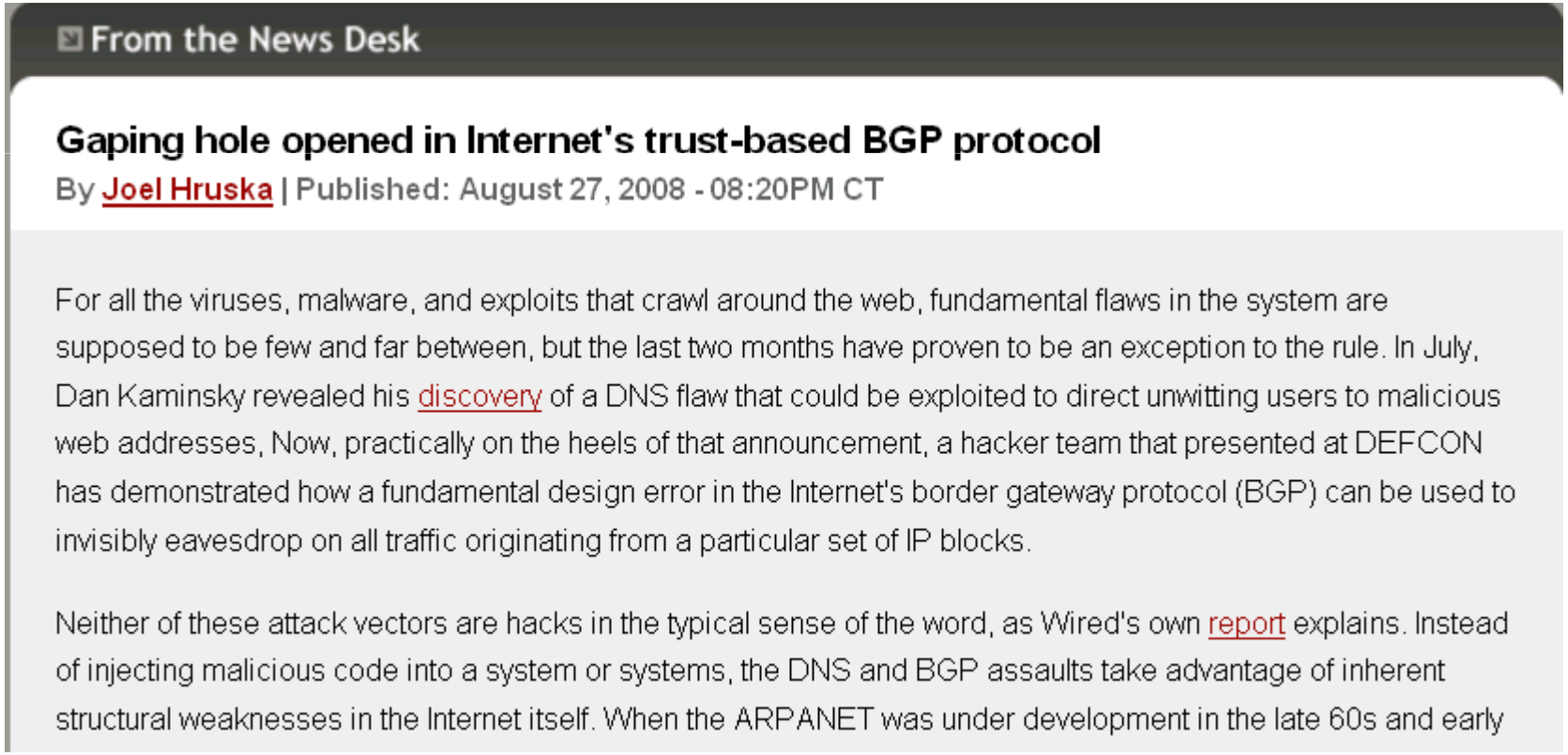
By Iljitsch van Beijnum | Published: February 25, 2008 - 03:31AM CT

On Sunday, YouTube became unreachable from most, if not all, of the Internet. No "sorry we're down" or cutesy kitten-with-screwdriver page, nothing. What happened was that packets sent to YouTube were flowing to Pakistan. Which was curious, because the Pakistan government had just instituted a ban on the popular video sharing site. What apparently happened is that Pakistan Telecom routed the address block that YouTube's servers are into a "black hole" as a simple measure to filter access to the service. However, this routing information escaped from Pakistan Telecom to its ISP PCCW in Hong Kong, which propagated the route to the rest of the world. So any packets for YouTube would end up in Pakistan Telecom's black hole instead.

On the North American Network Operators Group (NANOG) mailing list, where many engineers in charge of Internet routing hang out, the consensus is that this was an accident. Only one or two people suggest that it may be a malicious act, possibly a trial of something bigger. So why was this incident so devastating to YouTube's reachability?

# Attack on BGP Routing

- August 2008
- “Man-in-the-middle” attack



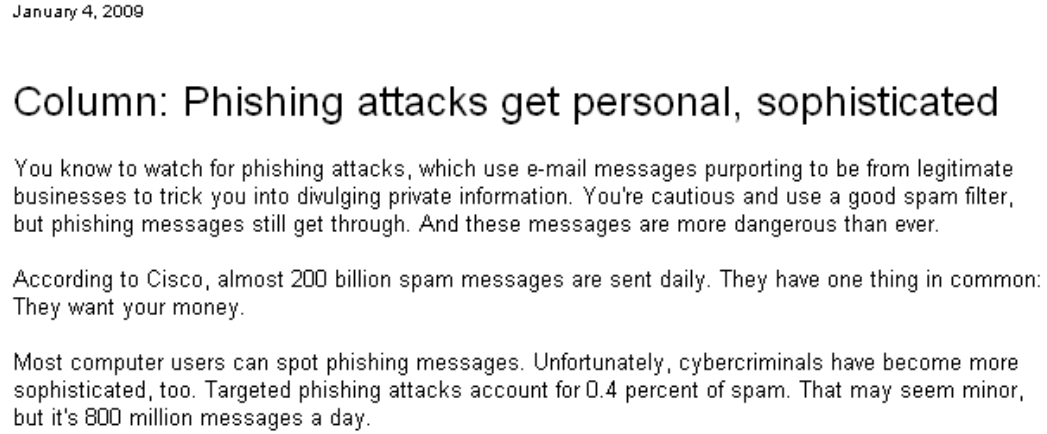
From the News Desk

**Gaping hole opened in Internet's trust-based BGP protocol**

By Joel Hruska | Published: August 27, 2008 - 08:20PM CT

For all the viruses, malware, and exploits that crawl around the web, fundamental flaws in the system are supposed to be few and far between, but the last two months have proven to be an exception to the rule. In July, Dan Kaminsky revealed his discovery of a DNS flaw that could be exploited to direct unwitting users to malicious web addresses, Now, practically on the heels of that announcement, a hacker team that presented at DEFCON has demonstrated how a fundamental design error in the Internet's border gateway protocol (BGP) can be used to invisibly eavesdrop on all traffic originating from a particular set of IP blocks.

Neither of these attack vectors are hacks in the typical sense of the word, as Wired's own report explains. Instead of injecting malicious code into a system or systems, the DNS and BGP assaults take advantage of inherent structural weaknesses in the Internet itself. When the ARPANET was under development in the late 60s and early



January 4, 2009

## Column: Phishing attacks get personal, sophisticated

You know to watch for phishing attacks, which use e-mail messages purporting to be from legitimate businesses to trick you into divulging private information. You're cautious and use a good spam filter, but phishing messages still get through. And these messages are more dangerous than ever.

According to Cisco, almost 200 billion spam messages are sent daily. They have one thing in common: They want your money.

Most computer users can spot phishing messages. Unfortunately, cybercriminals have become more sophisticated, too. Targeted phishing attacks account for 0.4 percent of spam. That may seem minor, but it's 800 million messages a day.

- Spam: 95+% of all email traffic on the Internet (200 billion spam messages per day, as of January 2009)
- Unique phishing attacks rose 13% (to over 28k!) in for second quarter 2008
- 294 hijacked brands
- 442 unique malicious application variants in May 2008

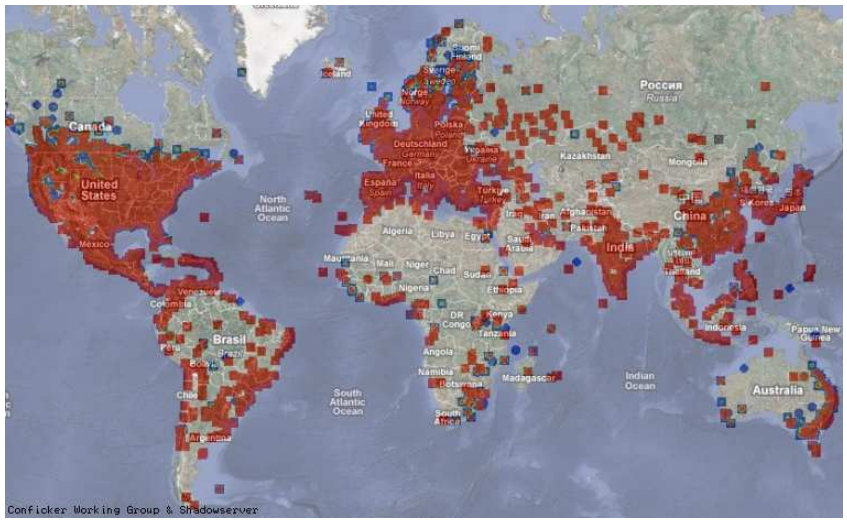
# Malware

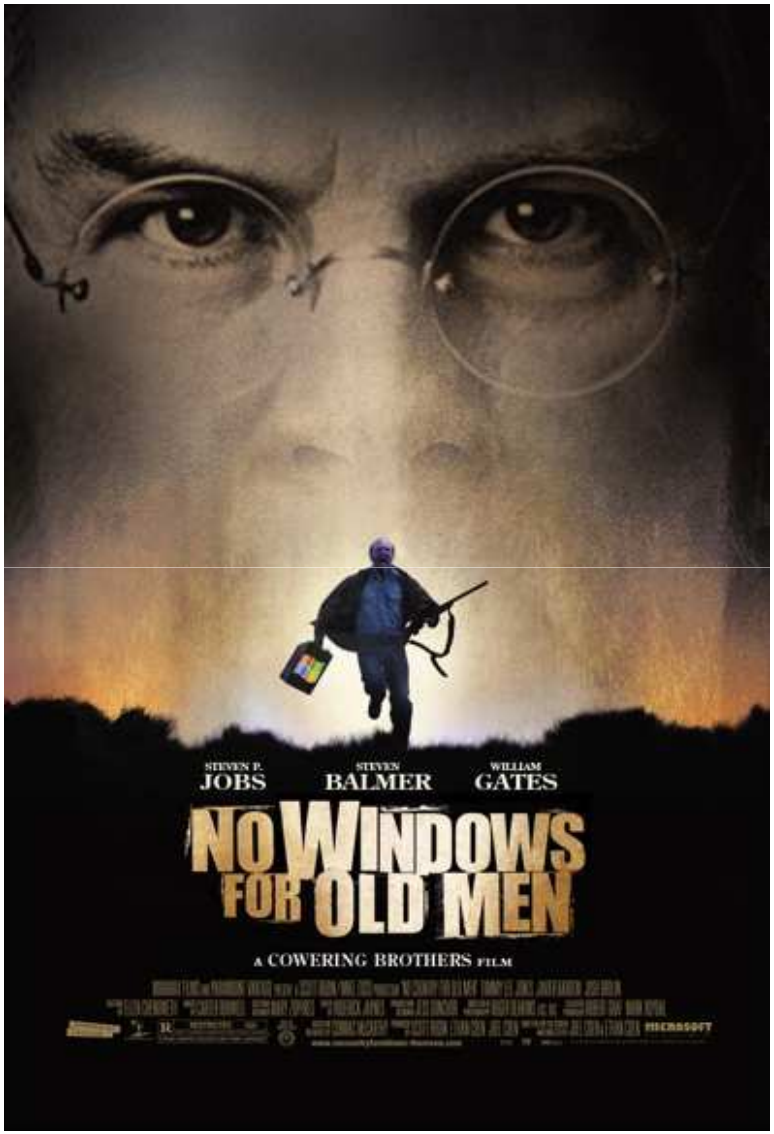

Hijackers
Malware
CWSI
Spyware
Adware


Spyware:
it's not what every well-dressed
spy is wearing
Spy-wear

# More…

- “Attack of the tweets: Major Twitter Flaw Exposed” – UK researcher says vulnerability in Twitter API lets an attacker take over a victim’s account – with a tweet. Aug 27, 2009 [Darkreading]
- Conficker worm:




STEVEN P.
JOBS
STEVEN
BALMER
WILLIAM
GATES
NO WINDOWS FOR OLD MEN
A COWERING BROTHERS FILM
MICROSOFT


System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
Local Disk (C:)
Security threat
Local Disk (D:)
DVD-RAM Drive (E:)
Security threat
100% files - System scan
Total files 4581
Your Computer is Infected!
WARNING! Spyware thr
C:\Documents and Settings\user\Lo
C:\Documents and Settings\user...
C:\Documents and Settings\user\Co
C:\Documents and Settings\user\Co
C:\WINDOWS\Temp\Temporary Int
Full system cleanup
WARNING!!!
Scan results
WARNING!
Windows has been infected
Name
Type
Alert level
System Soap Pro
Spyware
Avarage
AntiLamer Light
Spyware
Avarage
MC 30 Day
Spyware
Danger
SoftEther
Spyware
High
I-Worm.NetSky.q
Virus
High
I-Worm.Bagle.n
Virus
High
Tofger-A
Virus
Critical
Zinx-A
Spyware
Critical
B-S Spy 1.90
Spyware
Critical
KrAIMer 1.1
Virus
Critical
Warning!!! 364 infected files found
Click the "Erase all threats" button to erase all spyware and viruses from Windows
Erase all threats

# Botnet – New Rising Threat

# Sea-Change in Internet Attacks

- Computers on the Internet used to be *mere targets*
  - For fun and fame
- Now they are *Resources/Platforms*
  - For profit
- How big is the problem now?

# Top 5 Super Computer

- June 2008 survey of super computers from http://www.top500.org/list/2008/06/100

| Rank | Site | Computer/Year Vendor | Cores | $R_{max}$ | $R_{peak}$ | Power |
|---|---|---|---|---|---|---|
| 1 | DOE/NNSA/LANL<br>United States | Roadrunner - BladeCenter QS22/LS21 Cluster, PowerXCell 8i 3.2 Ghz / Opteron DC 1.8 GHz , Voltaire Infiniband / 2008<br>IBM | 122400 | 1026.00 | 1375.78 | 2345.50 |
| 2 | DOE/NNSA/LLNL<br>United States | BlueGene/L - eServer Blue Gene Solution / 2007<br>IBM | 212992 | 478.20 | 596.38 | 2329.60 |
| 3 | Argonne National Laboratory<br>United States | Blue Gene/P Solution / 2007<br>IBM | 163840 | 450.30 | 557.06 | 1260.00 |
| 4 | Texas Advanced Computing Center/Univ. cf Texas<br>United States | Ranger - SunBlade x6420, Opteron Quad 2Ghz, Infiniband / 2008<br>Sun Microsystems | 62976 | 326.00 | 503.81 | 2000.00 |
| 5 | DOE/Oak Ridge National Labcratory<br>United States | Jaguar - Cray XT4 QuadCore 2.1 GHz / 2008<br>Cray Inc. | 30976 | 205.00 | 260.20 | 1580.71 |

# Storm Worm for Comparison

- "…the Storm cluster has the equivalent of one to 10 million 2.8 GHz Pentium 4 processors with one to 10 million petabytes worth of RAM. ... To put the size of a petabyte into perspective, Google, as of Aug. 2007, uses between 20 and 200 petabytes of disk space,according to Wikipedia.com. In comparison, Gutmann said, BlueGene/L currently contains 128,000 computer processor cores, and has a paltry 32 terabytes of RAM. A terabyte is about 1,000 times smaller than a petabyte."
- Brian Kreb's WashingtonPost report (http://blog.washingtonpost.com/securityfix/2007/08/storm_worm_dwarfs_worlds_top_s_1.html)

# What is Storm?

- A malware instance, more precisely, a botnet
- Using P2P techniques for its C&C channels
- Mainly used to send spam

- We are lucky because Storm is mainly used for sending spam…

# Botnets: Current Single largest Internet Threat

- “Attack of zombie computers is growing threat”

  (New York Times)
- “Why we are losing the botnet battle”

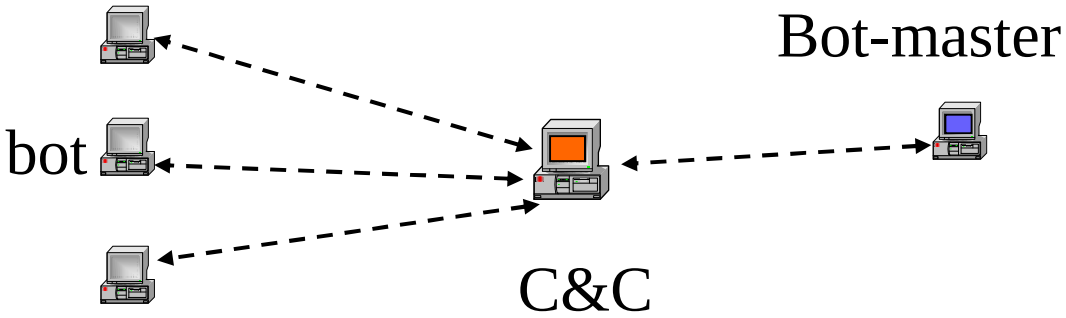
  (Network World)
- “Botnet could eat the internet”

  (Silicon.com)
- “25% of Internet PCs are part of a botnet”

  (Vint Cerf)

# What are Bots/Botnets?

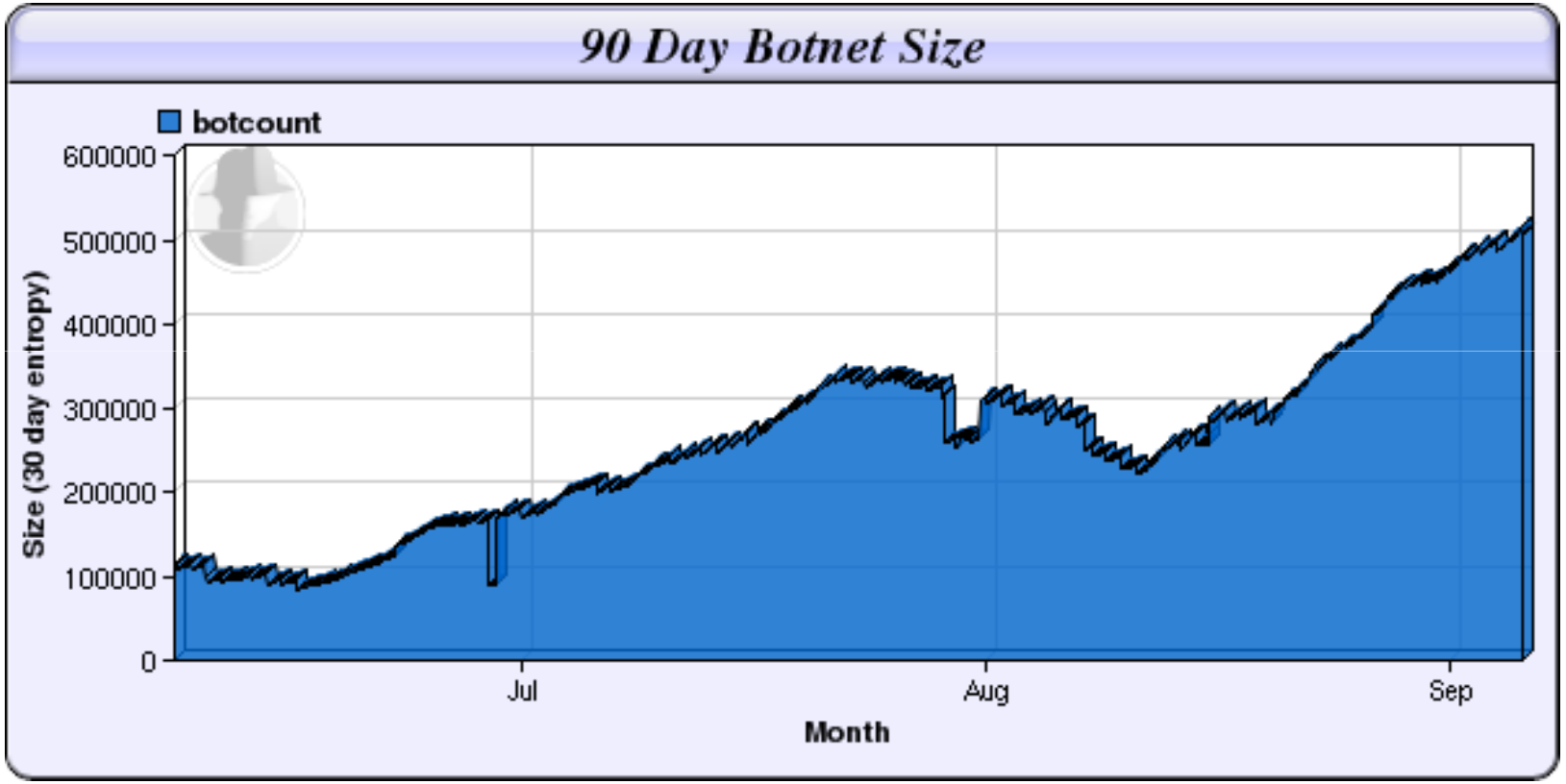
- Bot (Zombie)
  - Compromised computer controlled by botcode (malware) without owner consent/knowledge
  - Professionally written; self-propagating
- Botnets (Bot Armies): Networks of bots controlled by criminals
  - Definition: "A coordinated group of malware instances that are controlled via C&C channels".
  - Architectures: centralized (e.g., IRC,HTTP), distributed (e.g., P2P)
  - Key platform for fraud and other for-profit exploits



# Botnet Epidemic

- More than 95% of all spam
- All distributed denial of service (DDoS) attacks
- Click fraud
- Phishing & pharming attacks
- Key logging & data/identity theft
- Distributing other malware, e.g., spyware
- Anonymized terrorist & criminal communication

# Number of Bots Are Increasing!

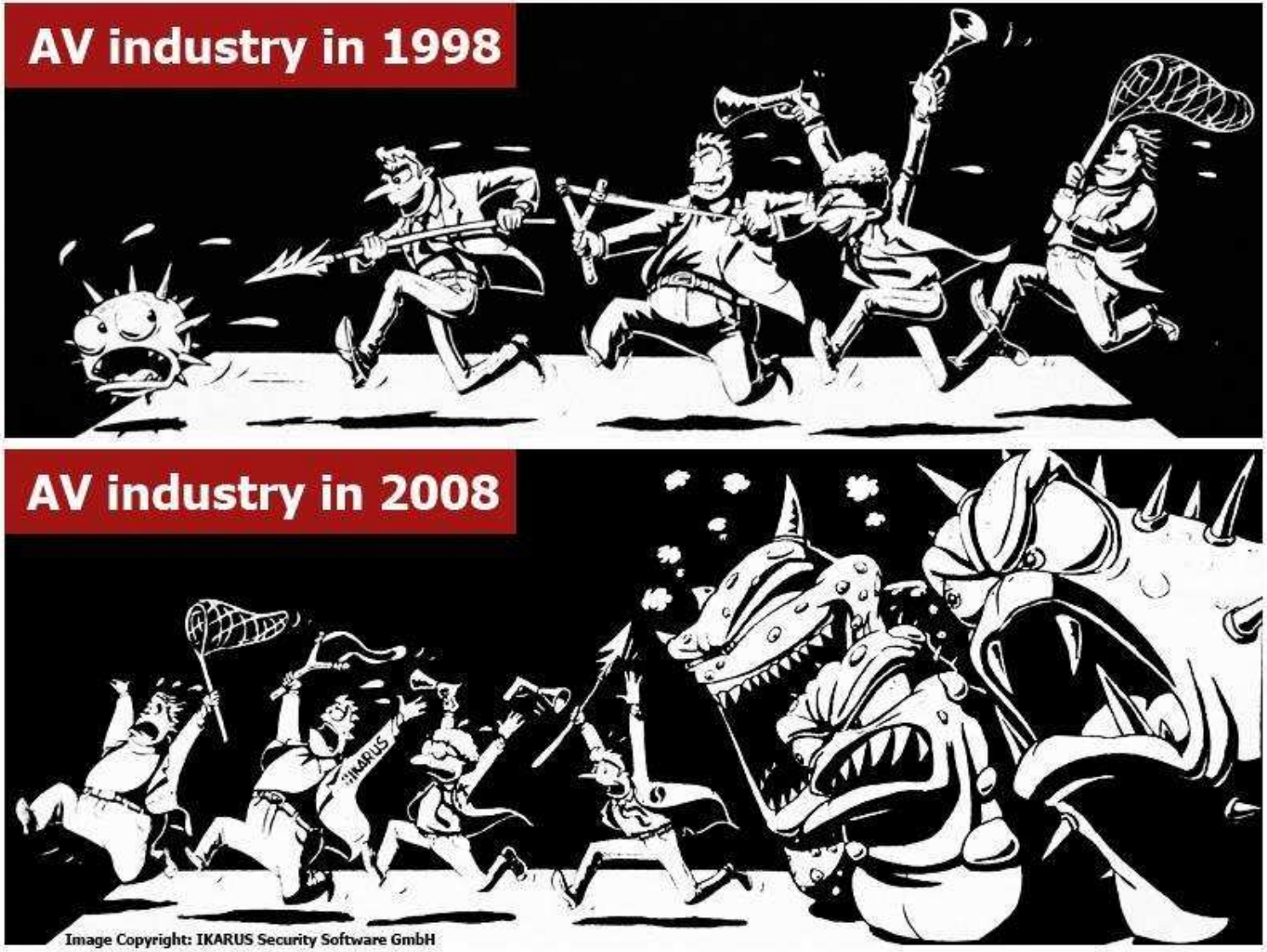



Source: shadowserver.org, 2008

# Internet Security: Broken Assumptions

- Internet infrastructure (e.g., DNS, BGP) is trustworthy
  - DNS is more vulnerable than you think …
- Computers are secure when using up-to-date AV tools and firewall
  - Not really
- Attackers are for fun and fame
  - Profit, profit, profit!
- Attackers have limited/bounded computing power
  - They hare almost unbounded(?) power
- Attacks from isolated computers
  - The network is attacking you

- Where are we? Any hope to win this game?


AV industry in 1998
AV industry in 2008
IKARUS
Image Copyright: IKARUS Security Software GmbH

# Security (Very) Basics

# What is Security?

- [Informally] Security is the *prevention* of certain types of *intentional* actions from occurring

  - These potential actions are **threats**
  - Threats that are carried out are **attacks**
  - Intentional attacks are carried out by an **attacker**
  - Objects of attacks are **assets**

# Security: Definition

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable

- Security rests on confidentiality, authenticity, integrity, and availability

# Basic Components

- **Confidentiality** is the concealment of information or resources
  - Keeping data and resources hidden.  Privacy.
- **Authenticity** is the identification and assurance of the origin of information
- **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes
  - Preventing unauthorized changes to data or resources.
- **Availability** refers to the ability to use the information or resource desired
  - Enabling access to data and resources

# Security Threats and Attacks

- A threat is a *potential* violation of security
  - Flaws in design, implementation, and operation

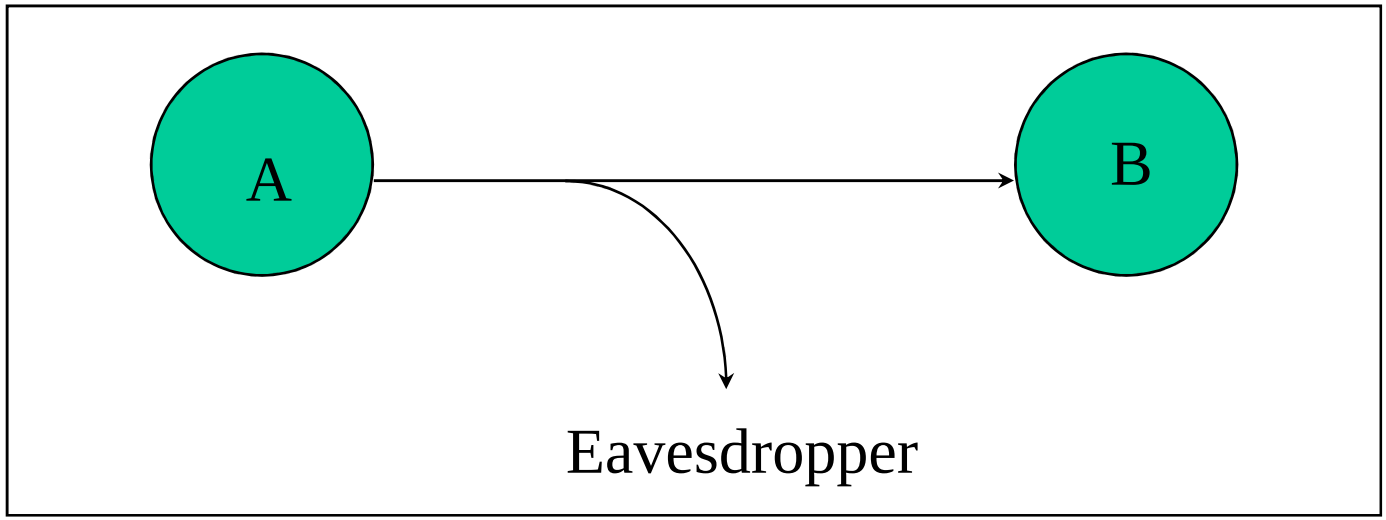
- An attack is any *action* that violates security
  - Active vs. passive attacks

# Vulnerabilities (Attack Vectors)

- A vulnerability is a systematic artifact that exposes the user, data, or system to a threat
  - E.g., buffer-overflow, WEP key leakage
- What is the source of a vulnerability?
  - Bad software (or hardware)
  - Bad design, requirements
  - Bad policy/configuration
  - System Misuse
  - Unintended purpose or environment
    - E.g., student IDs for liquor store

# Eavesdropping - Message Interception (Attack on Confidentiality)

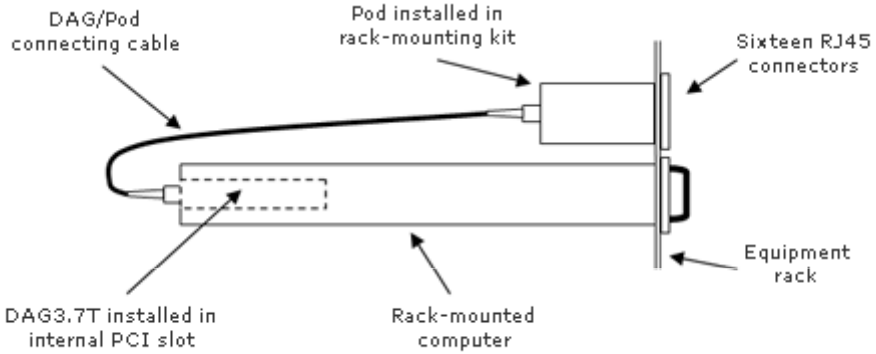
- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs



# Full Packet Capture (Passive)

**Example:** OC3Mon

- Rack-mounted PC
- Optical splitter
- Data Acquisition and Generation (DAG) card



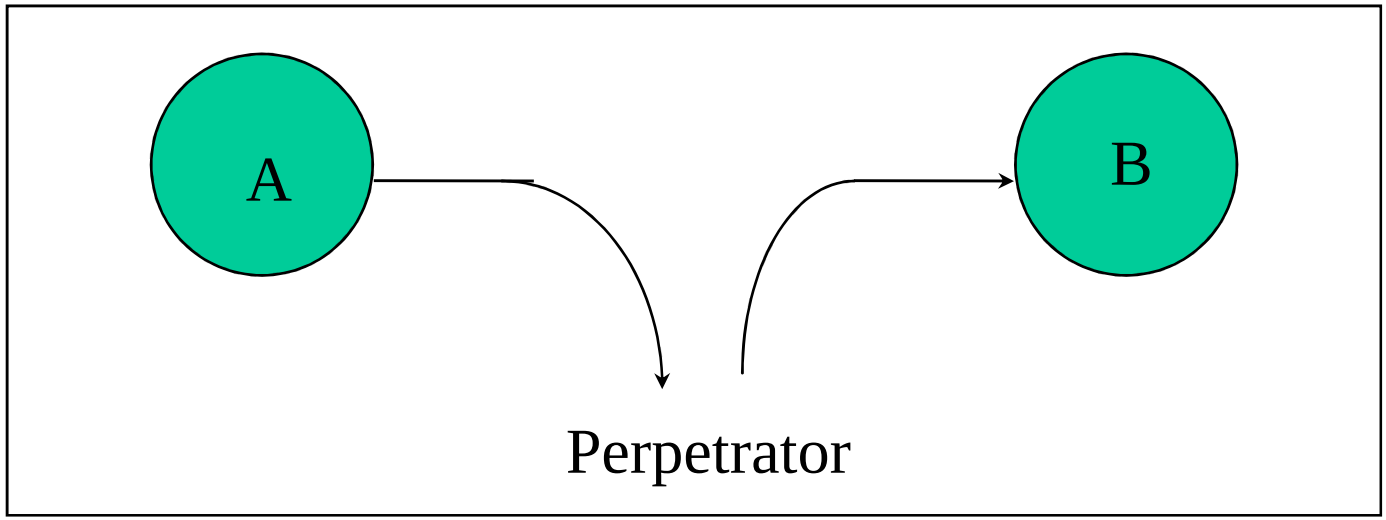

Source: endace.com

# Eavesdropping Attack: Example

- tcpdump with promiscuous network interface
  - On a switched network, what can you see?
- What might the following traffic types reveal about communications?
  - DNS lookups (and replies)
  - IP packets without payloads (headers only)
  - Payloads

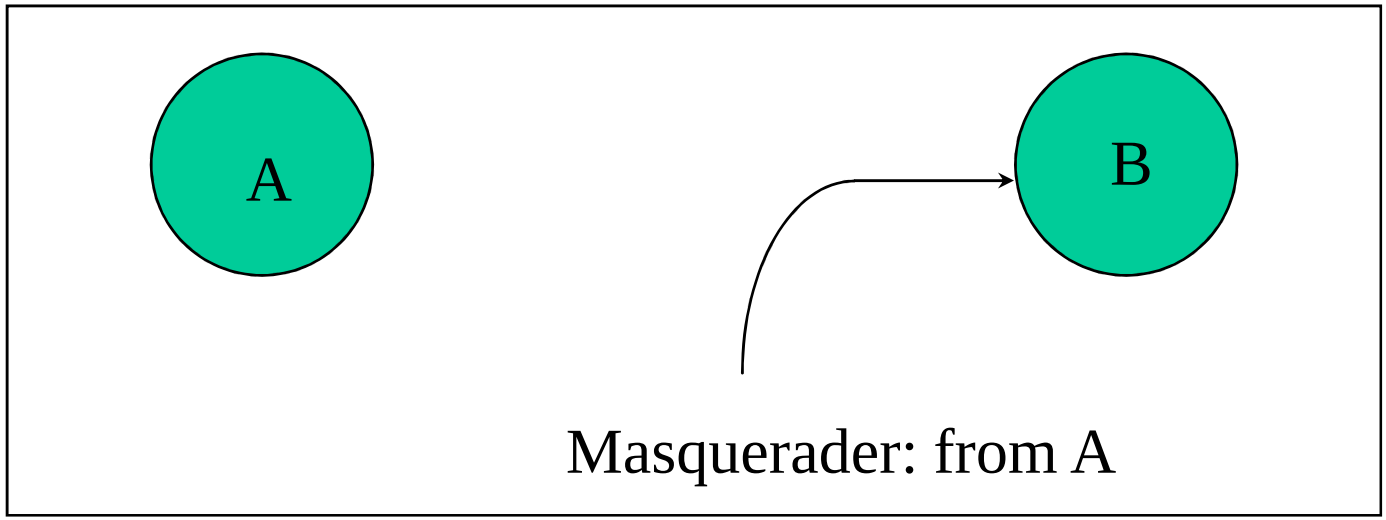
# Integrity Attack - Tampering

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



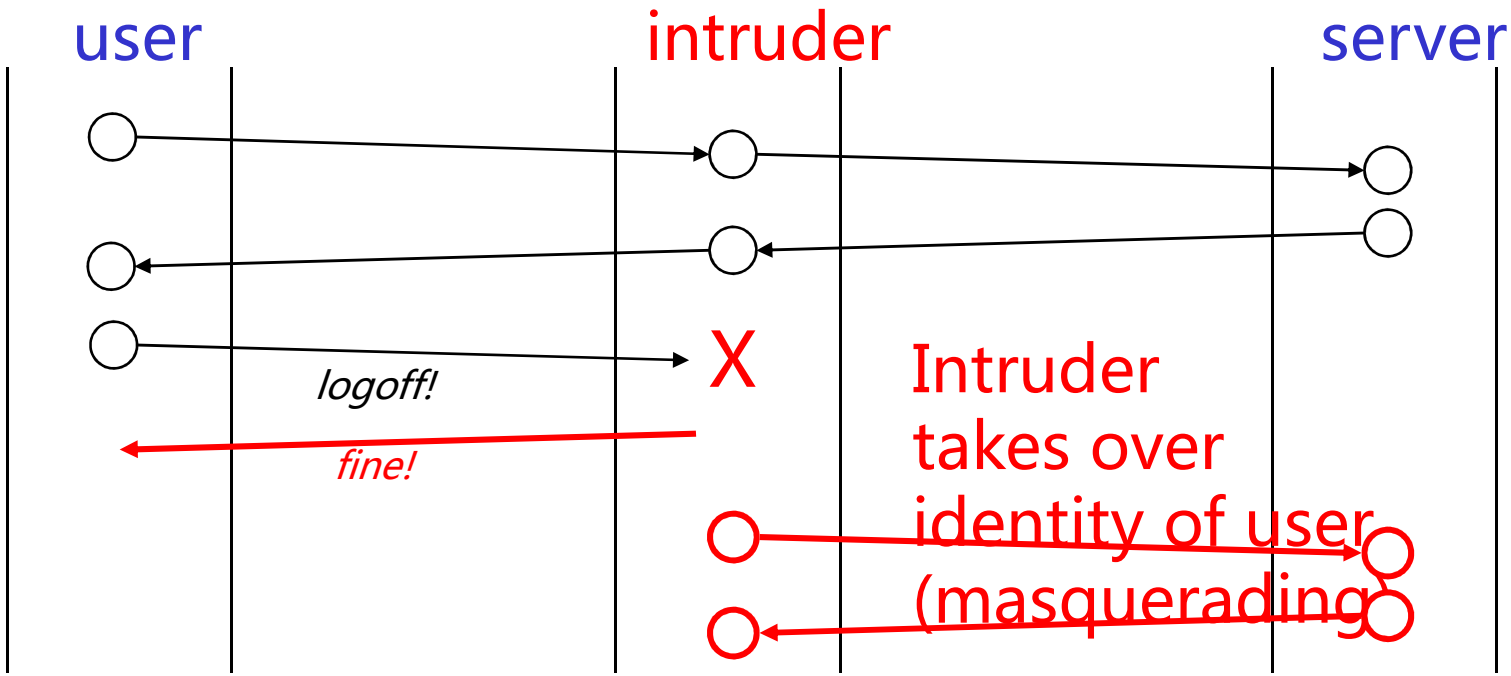
# Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



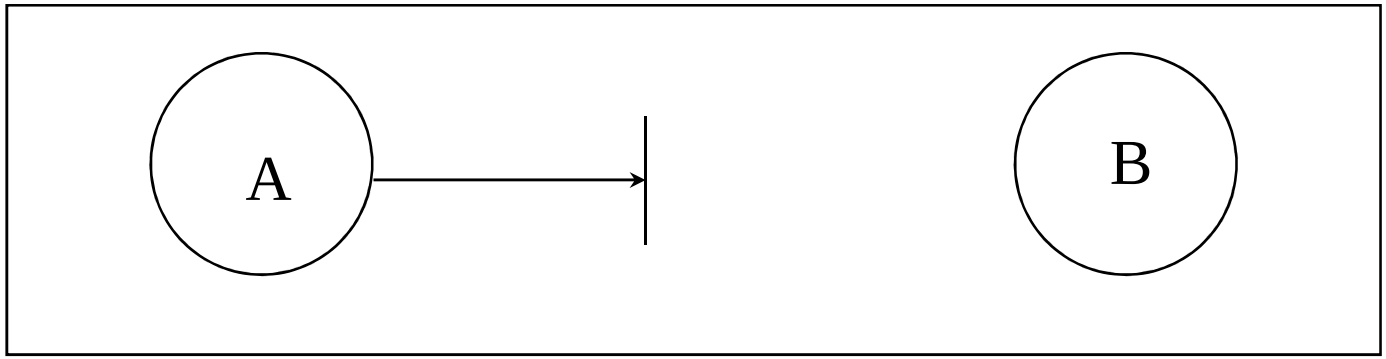
# Man-In-The-Middle: Example

- **Passive tapping**
  - Listen to communication without altering contents.
- **Active wire tapping**
  - Modify data being transmitted
  - Example:



# Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit




- Blatant *denial of service* (DoS):
  - Crashing the server
  - Overwhelm the server (use up its resource)

# Goals of Security

Prevention

- Prevent attackers from violating security policy

Detection

- Detect attackers' violation of security policy

Recovery

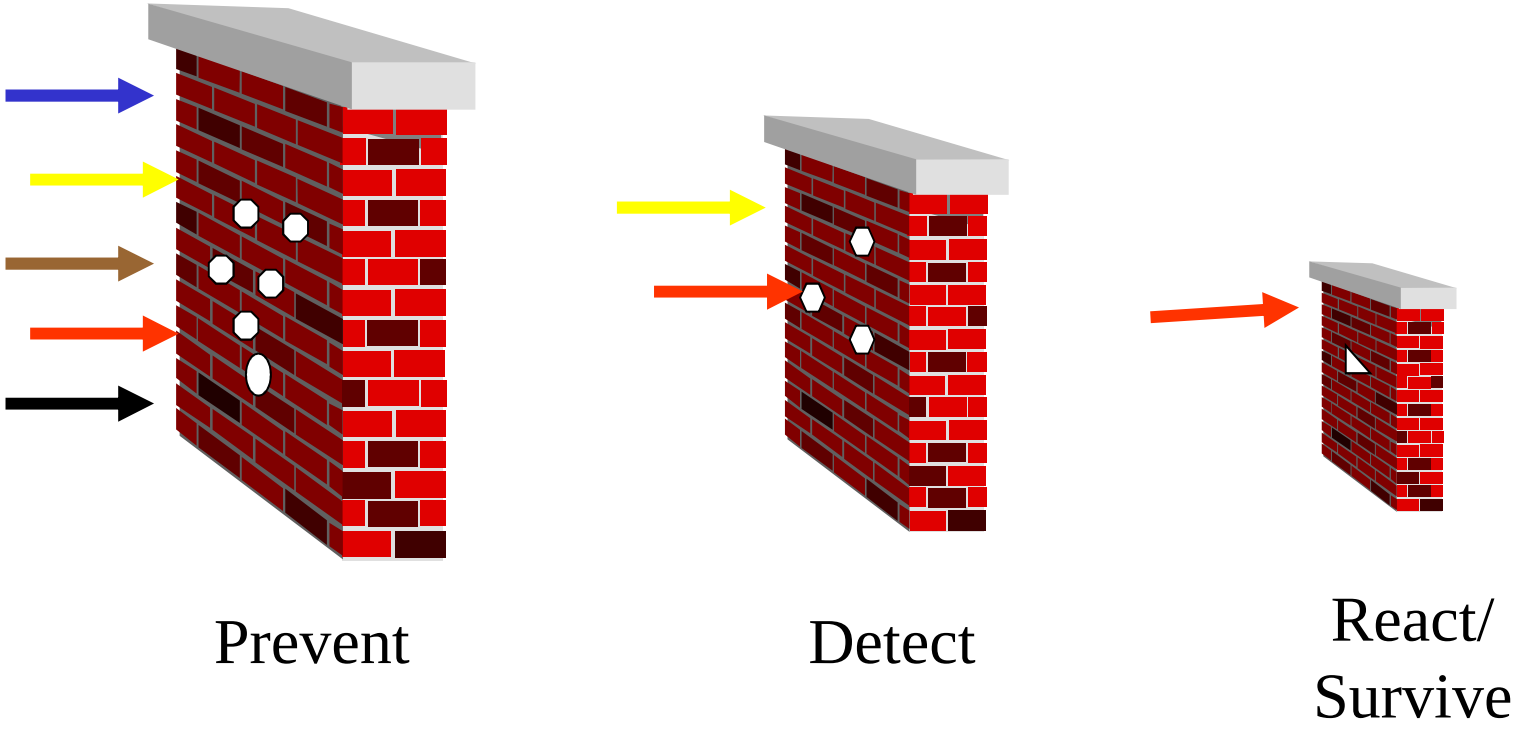
- Stop attack, assess and repair damage

Survivability

- Continue to function correctly even if attack succeeds

# My Overall Research Problems

- How to make our computer, network, and Internet more secure?




***Security principles: Defense–in-Depth, layered mechanisms***

# Interested? Want to know more?

- Consider taking CSCE 465 “Computer & Network Security” next spring that I’ll teach.