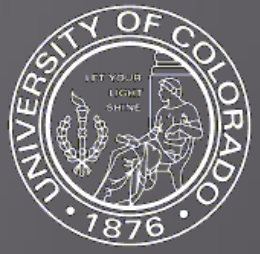


CS 591

FUNDAMENTALS OF COMPUTER AND NETWORK SECURITY

C. EDWARD CHOW

http://cs.uccs.edu/~cs591/

Class Background Poll

- Introduction to computer security?
  - Access control, Web security, sandboxing, virus?
- Cryptography?
  - Public-key and symmetric encryption, digital signatures, cryptographic hash, random-number generators?
- Computer networks?
  - Network architecture, application and transport layer protocols?
  - Configuration of Router? Firewall? IDS?
- Programming in C? Dissemble? I386 assembly?
- OS installation experience?
  - Linux, Fedora Core 6, WinXP, Win2003, Vista, Longhorn, VxWork
  - Virtual machines: VMWare, UML, VPC
- System Admin Experience?
- Network Admin Experience?
- Use Auditor? Ethereal? Nessus/Tenable? MetaSploit? Rootkit?

Useful Book

- Textbook: Ross Anderson. “Security Engineering”. Online version.
- "Security in Computing," by Charles P. Pfleeger, Shari Lawrence Pfleeger, 2003.
- Matt Bishop, “Computer Security”
- William Stallings. “Network Security Essentials: Applications and Standards.”
- Kaufman, Perlman, Speciner. “Network Security: Private Communication in a Public World”.

Lab Exercises

- Break-in to Windows machines using MetaSploit Framework
- Buffer Overflow. Given target.c code, write exploit.c that obtains a shell with root privilege.
- Secure Web Access (password based and certificate based)
- Perform Scanning using Nessus/Tenable NeWT Security Scanner
- Configure/Use Snort IDS, Linux Firewall
- Configure and Secure the perimeter of a Network
- Climax Capstone Project: Capture the Flag, Cyber Defense/Attack exercise! (Need your input)

Lab Resources

- Virtual machines running patched/unpatched WinXP, RH7.2, FC6, Win2000/SQL2000, Win2003 on EAS149 PCs. Require direct access in the labs.
- For remote access, networks of VMWare-server based virtual machines will be available on walden, walrus, and viva. This requires high/medium speed internet connection for decent window gui updates.
  - They consists of DMZ firewalls, IDS, web server, DNS server, mail server, MySQL server, and clients in internal subnet.
  - Download the VMware server client package to access these virtual machines. 2nd Binary Zip file in the following page http://register.vmware.com/content/download.html
  - You can also installed the VMware server package (lst binary .exe in the above web page) to run the virtual machines on your own laptop or desktop without high speed access to UCCS. Required to register http://www.vmware.com/download/server/. You can bring external hard drive or laptop to download files for those virtual machines

Goals

Develop understanding of basic problems underlying computer/network security and the methods available to deal with them.

- Examine the risks of security in computing
- Consider available countermeasures or controls
- Stimulate thought about uncovered vulnerabilities
- Identify areas where more work is needed

Security Engineering

- Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.
- Focuses on the tools, processes, and methods needed
  - to design, implement, and test complete systems, and
  - to adapt existing systems as their environment evolves.
- Security engineering requires cross-disciplinary expertise:
  - cryptography
  - hardware tamper-resistance
  - formal methods
  - a knowledge of applied psychology (Social Engineering),
  - organizational and audit methods and
  - the law.
- System engineering skills deal only with error and mischance :
  - business process
  - software engineering
  - evaluation and testing,
- Need other techniques/processes to deal with malice attacks.

Definitions

- System: It refers to the hardware, software, organization's infrastructure, applications, IT staff, internal users, customers, external users, environment (media, regulators, competitors). Because they all impact on system security.
- Ignore human components → primary causes of security failure.
- Internet Security Glossary: rfc2828 by Bob Shirey of GTE/BBN May 2003
- National Information Assurance (IA) Glossary by CNSS, revised May 2003.
- Which one you prefer?
  1. a trusted system
  2. a trustworthy system

Naming Convention

- A principal is an entity that participates in a security system.
- In Security Protocols, there is a convention to name principals with names chosen with successive initial letters.
- "Alice authenticates herself to Bob"
  Are we sure it's Alice, and not perhaps Cherie to whom Alice lent her card, or David who stole her card, or Eve who hacked her PC?

Group, Role, Identity

- Group: a set of principals.
- Role: a function assumed by different person in succession.
- "Bob acting for Alice in her absence"→
  1. Bob's smartcard representing Bob who is acting for Alice in her absence.
  2. Bob operating Alice's smart card in her absence.

Identity: a correspondence between the names of two principals signifying that they refer to the same person or equipment.

Principle of Easiest Penetration

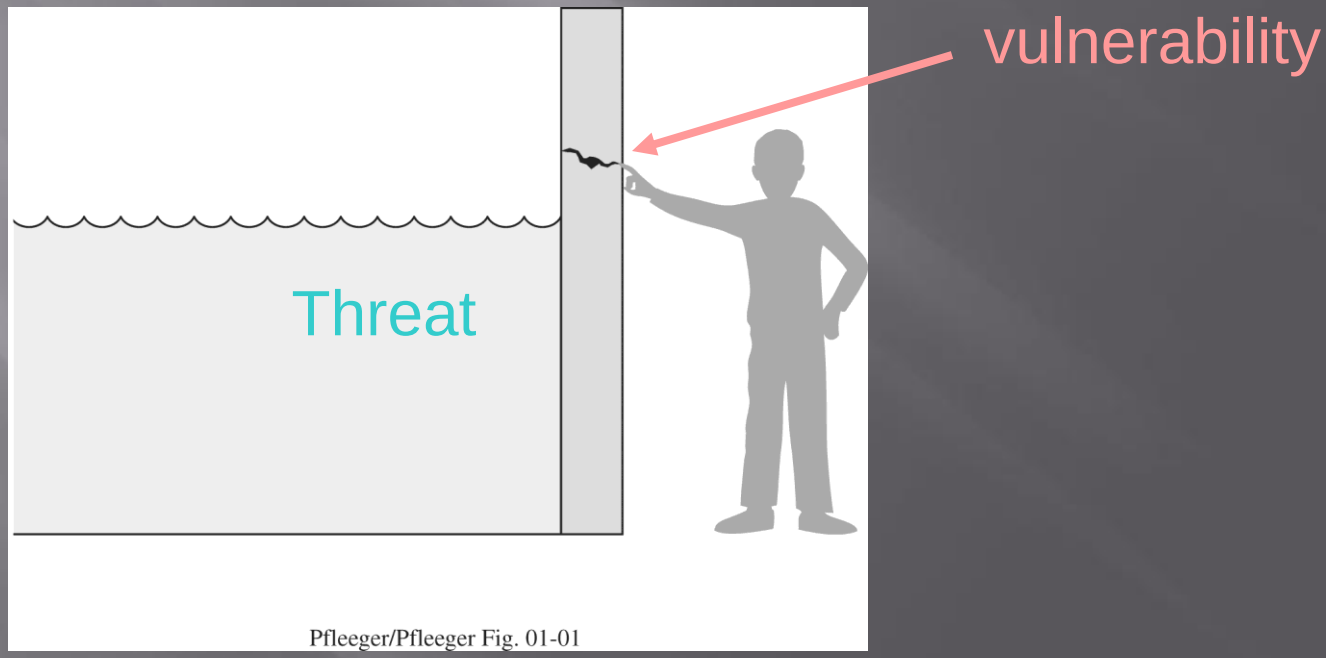
An intruder must be expected to use any available means of penetration. The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense been install.

It implies the computer security specialist must

- Consider ***all possible*** means of penetration.
- Penetration analysis must done repeatedly
- Especially when system and its security change

Vulnerability and Threat

- Vulnerability: A weakness in the security system, e.g., in procedure, design, or implementation, that might be exploited to cause loss or harm.
- Threat to a computer system: a set of circumstances that has the potential to cause loss or harm.



Control Vulnerability

Control: an action, device, procedure, or technique that removes or reduces a vulnerability.

A thread is blocked by control of vulnerability.

We will discuss variety of controls and the degree to which they enhance a system's security.

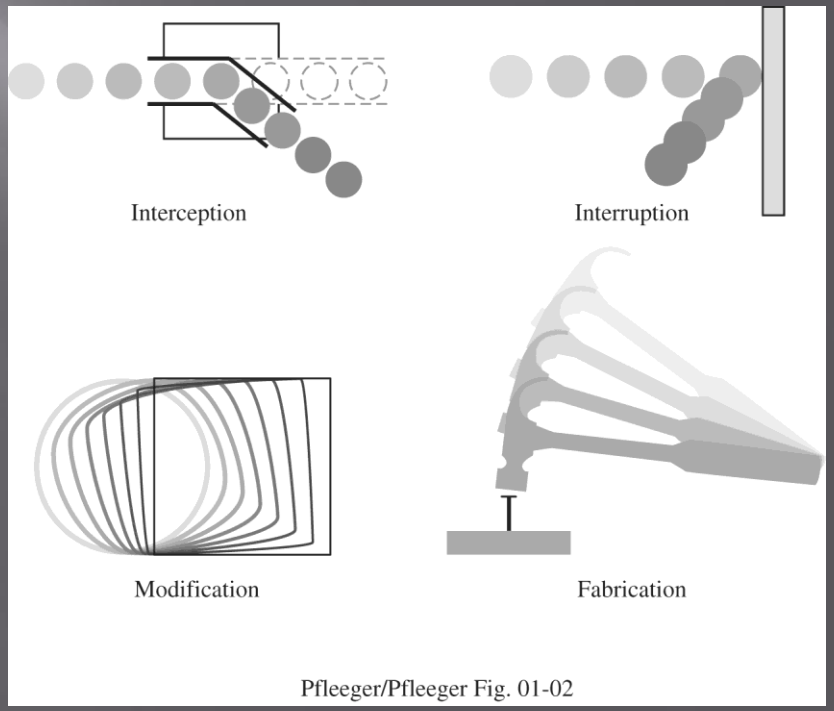
Security Policy: a succinct statement of a system's protection strategy. (e.g. >$1000 requires two mgr signatures.)

Types of System Security Threats

- Interception: some unauthorized party has gained access to an asset.
- Interruption: a situation where an asset of the system becomes lost, unavailable, unusable.
- Modification: an unauthorized tempering with an asset.
- Fabrication: unauthorized creation of counterfeit objects on a computing system.

I like Bob Shirey's definition of threat better:

- Disclosure.
- Deception.
- Disruption.
- Usurpation



MOM: Method, Opportunity, Motive

- Method: the skill, knowledge, tools and other things with which to be able to pull off the attack.
- Opportunity: the time and access to accomplish attack
- Motive: a reason to want to perform this attack against this system.

Deny any of those three things and the attack will not occur. However it is not easy to cut these off!

- Knowledge/specification/source code available on Internet
- Access to computer systems available, through purchase of same type of systems, Internet access
- Motives: show prowess of attackers; easy attacks; random; financial; revenge

Why Universities are Prime Targets?

Three Basic Security Service and Desirable Security Properties

Three Basic Security Services (CIA):

- Confidentiality: the concealment of information or resources.
- Integrity: the trustworthiness of data and resources
- Availability: the ability to use the information or resources desired

Other Desirable Security Properties

- Authenticity = integrity+ freshness (e.g. rogue wireless replay msg)
- Non-repudiation
- Freshness
- Access control
- Privacy of collected information
- Anonymity (e.g. e-voting)
- Accountability

More exorbitant list from NIST

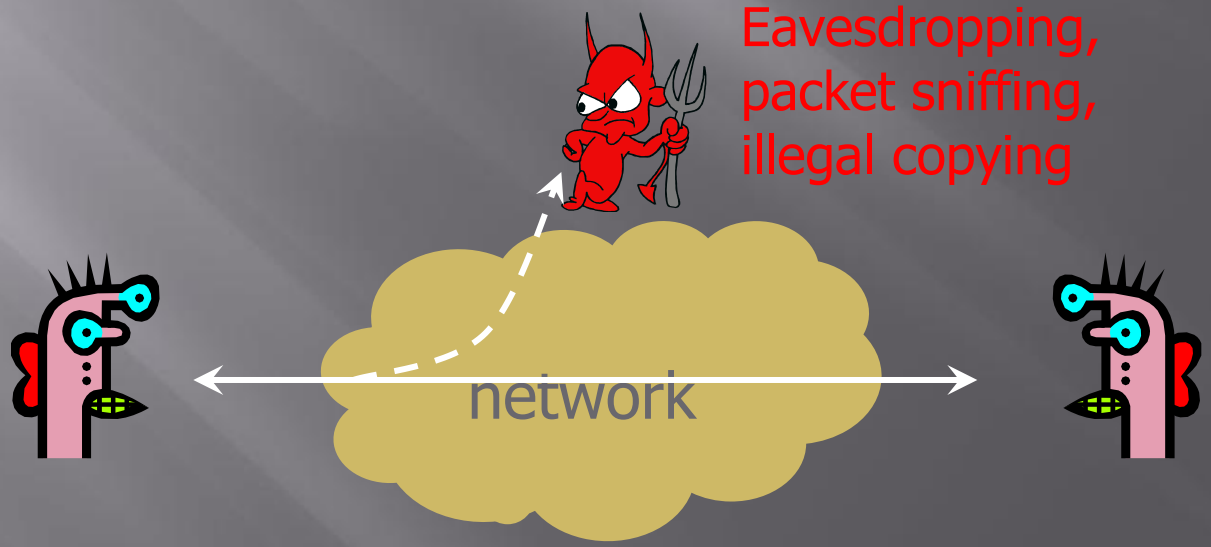
Confidentiality, Secrecy, Privacy

- They overlaps and not the same.
- Secrecy: the effect of mechanisms used to limit the number of principals who can access info.
- Confidentiality: it involves an obligation to protect some other person's or organization's secrets if you know them.
- Privacy is the ability and/or the right to protect your personal secrets/space.
- To protect privacy, it is not sufficient to keep content of msg secret. Route/Source/Destination also valuable info. How to protect that?.
  - A person contacts STD clinic.
  - Heavy encrypted msgs route to/from location 128.198.60.194.

Attack on Confidentiality

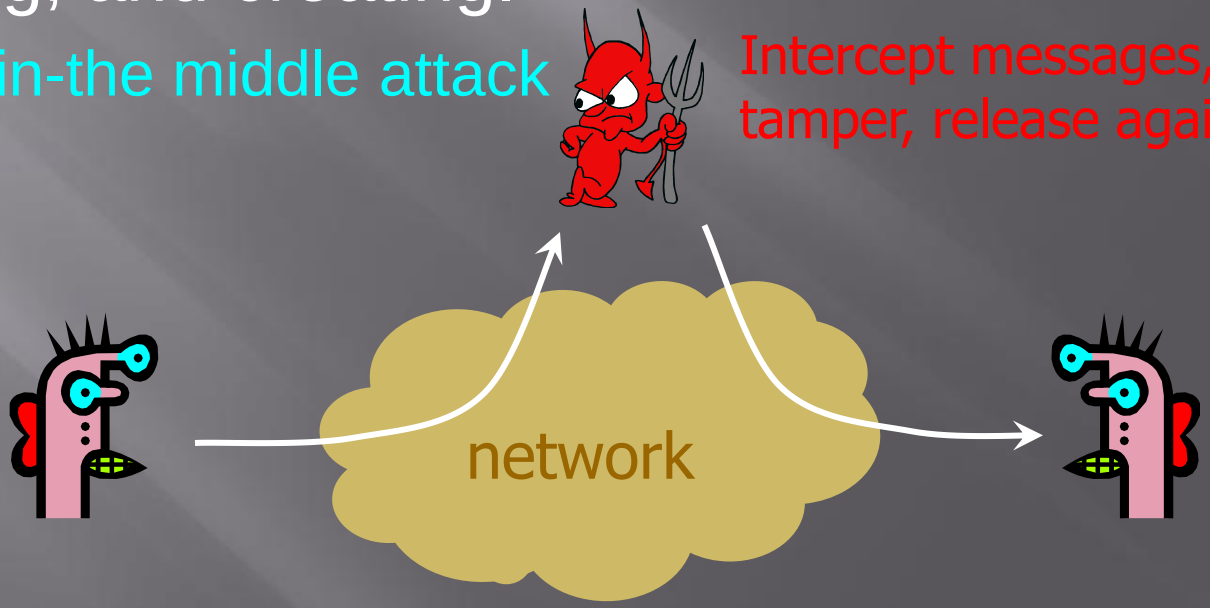
from Prof. Vitaly Shmatikov's nice viewgraph

- Confidentiality is concealment of information ensure that computer-related assets are accessed only by authorized parties.



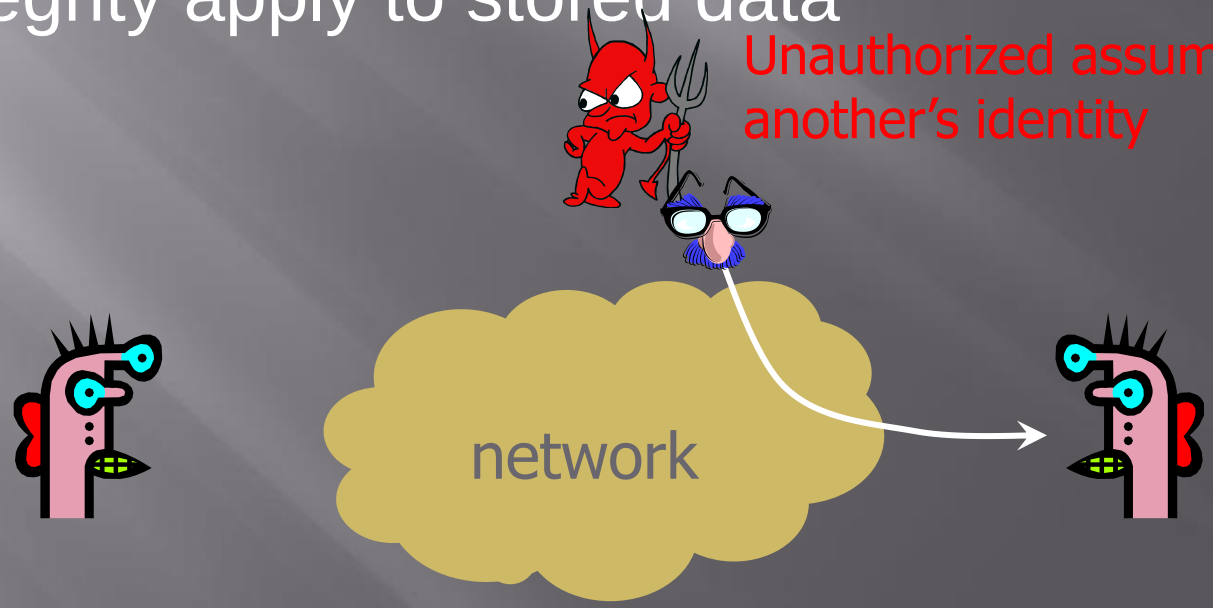
Attack on Integrity

- Integrity is prevention of unauthorized changes assets can be modified only by authorized parties or only in authorized ways. Modification include writing, changing, changing status, deleting, and creating.
  - Man-in-the middle attack



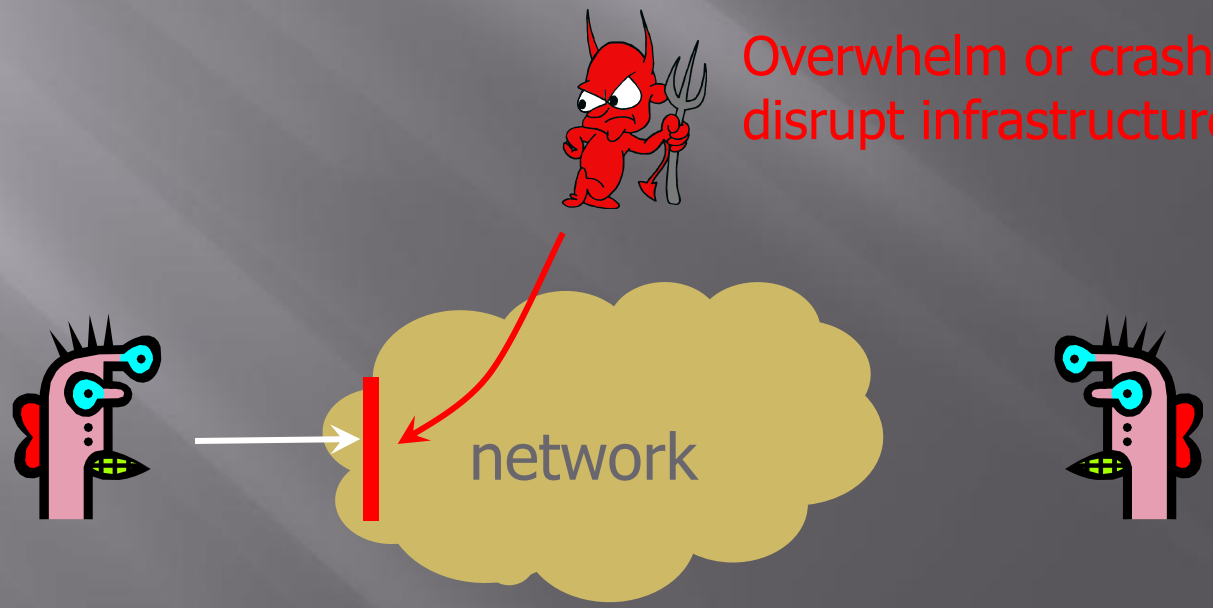
Attack on Authenticity

- Authenticity is identification and assurance of origin of information
- Authenticity apply to the identify of principals and the order they gave.
- Integrity apply to stored data

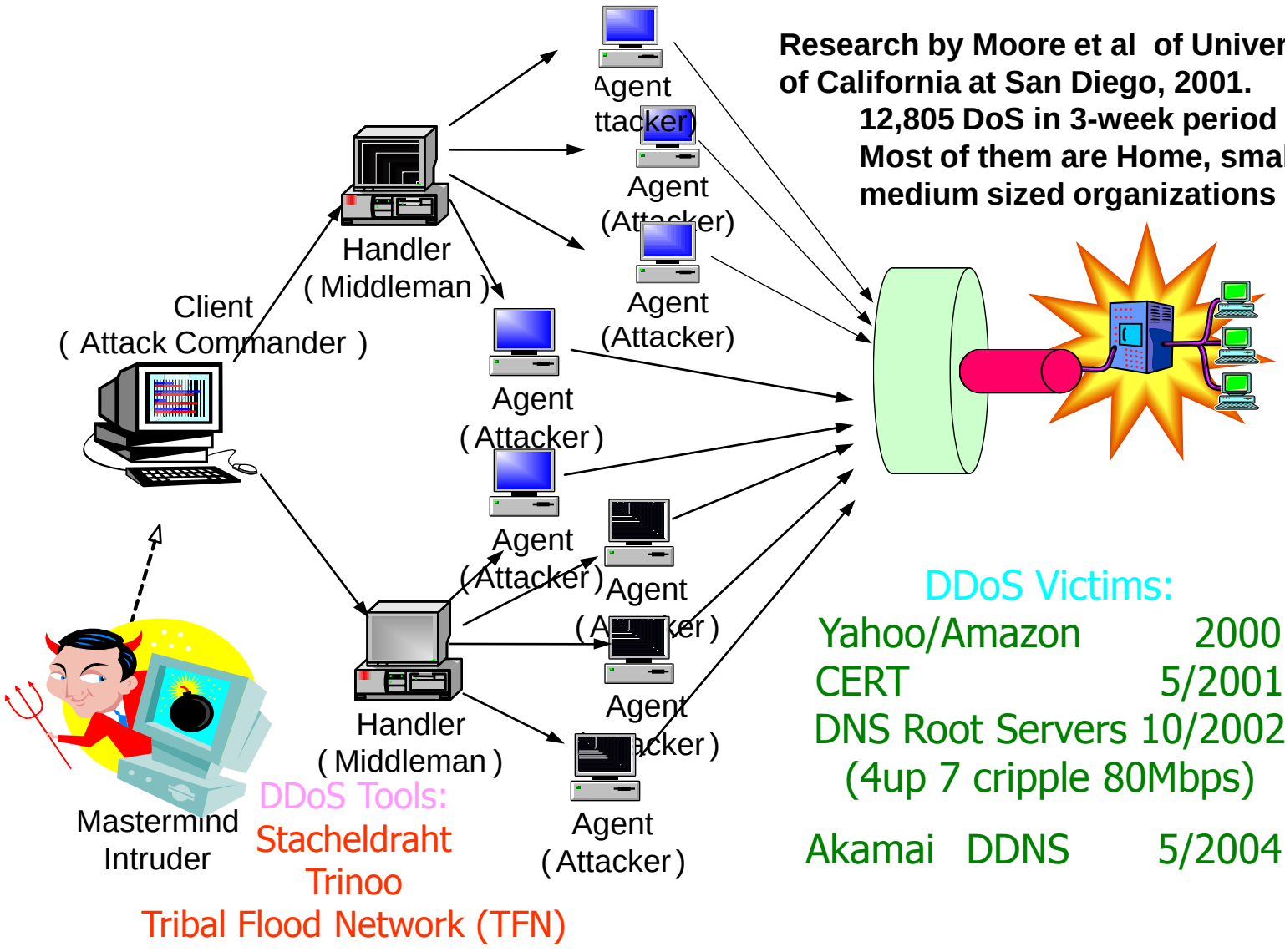


Attack on Availability

- Availability is ability to use information or resources desired. Assets are accessible to authorized parties at appropriate times.
  →Denial of Service Attack



DDoS: Distributed Denial of Service Attack

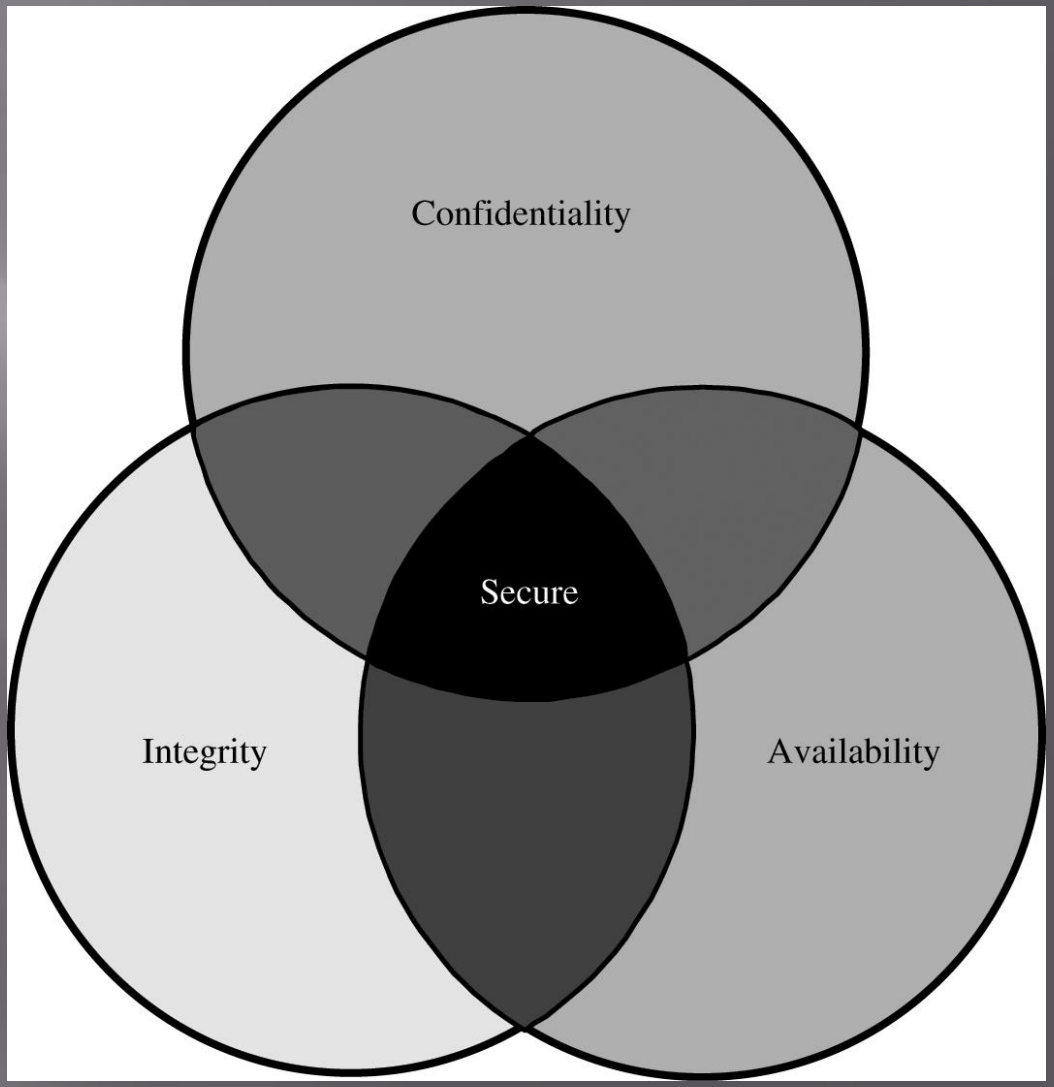


Relationship among Confidentiality, Integrity, and Availability

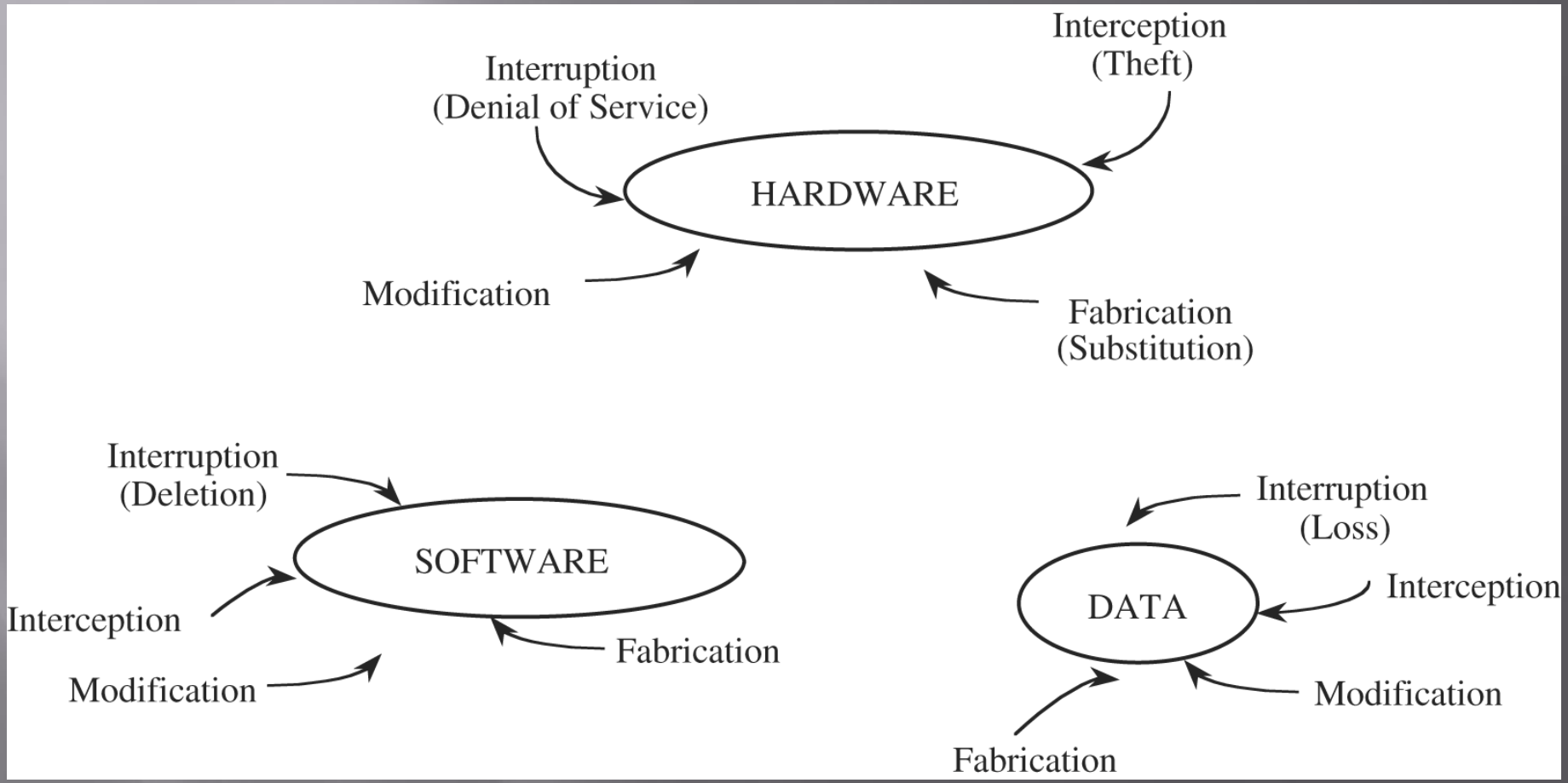
- Independent
- Overlap
- Mutual Exclusive

Computer security's past success has focused on confidentiality and integrity.

"Full Implementation of availability is security's next great challenge"



Vulnerability of Computer Systems



Software Modification

- Logic bomb: program modified to fail when certain conditions are met or when a certain date/time is reached.
- Trojan horse: a program that overtly does one thing while covertly doing another.
- Virus: a specific type of Trojan horse that can be used to spread its “infection” from one computer to another.
- Trapdoor: a program that has a secret entry point.
- Information leaks in a program: code that makes information accessible to unauthorized people or programs.

Data Security
Principle of Adequate Protection

Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.

Release of data related to the state of national economy

Personal data/credit card info

Computer Criminals

- Amateurs computer criminals
- Crackers
- Career Criminals

The security community distinguishes between

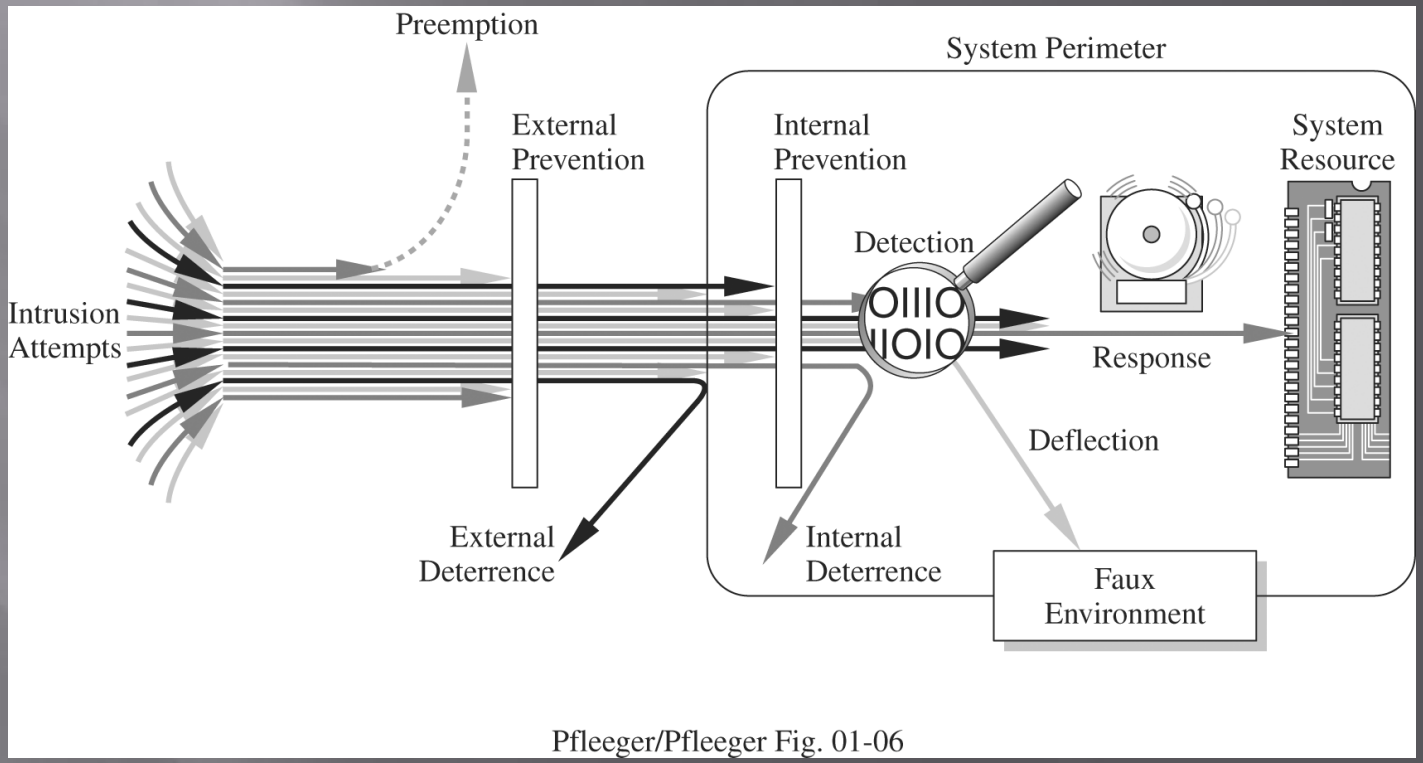
- Hacker: someone who non-maliciously programs, manages, uses computing systems, and
- Cracker: someone who attempts access to computing systems for malicious purposes.

Method of Defense

- Risk: The possibility for harm to occur.

Ways to deal with risks:

- Prevent
- Deter
- Deflect
- Detect
- Recover



Pfleeger/Pfleeger Fig. 01-06

Software Controls

- Internal program controls: parts of the program that enforce security restriction, such as access limitation in a database management program.
- Operating system and network system control: limitation enforced by the OS or network to protect each user from all other users.
- Independent control programs: password checkers, IDS, virus scanners
- Development controls: prevent software faults from becoming exploitable vulnerability

Effectiveness of Controls

- Awareness of Problem
- Likelihood of Use
  - Principle of Effectiveness: Control must be used and used properly to be effective. Efficient, easy to use, and appropriate.
- Overlapping Control (Layered Defense): physical security, restrict program access, file locking.
- Periodic Review: OMB 2001 2/3 government agencies received an F grade (Defense, Justice, Treasure). State Department D+; NSF B+.

Codes of Best Security Practices

- Information Security Forum
- Internet Security Alliance

Sarbanes-Oxley Act of 2002

- The Sarbanes-Oxley Act of 2002 (often shortened to *SOX*) is legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise.
- The Sarbanes-Oxley Act states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." The consequences for non-compliance are fines, imprisonment, or both.
- http://searchcio.techtarget.com/sDefinition/0,,sid19_gci920030,00.html

Severity/Speed of Cyber Attacks

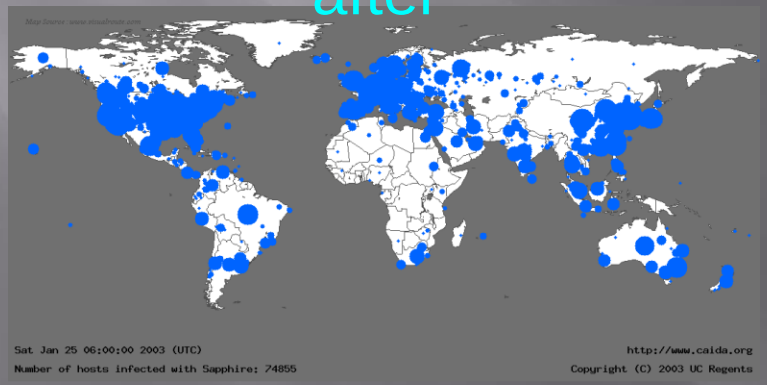
- Pages 6-8 of Prof. Eugene H. Spafford's Keynote Speech, "What Comes Next in Infosec Research?", September 2003.
- Slammed!
- David Moor's paper, http://www.cs.berkeley.edu/~nweaver/sapphire/
- Zotob. http://vil.nai.com/vil/content/v_135433.htm
- It could get worse. Why?

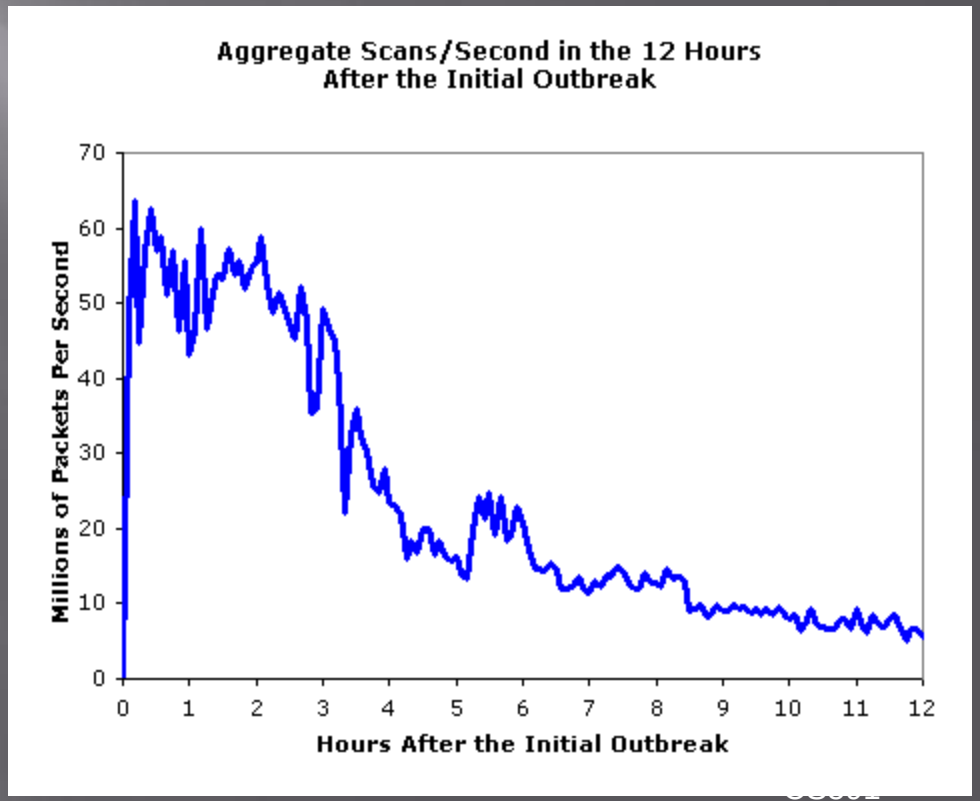
Sapphire/Slammer

- Doubled every 8.5 Seconds
- Infected 90% of vulnerable hosts in 30 minutes -74855 hosts

before

after





Semester Projects

E-Vote: Electronic Voting System

- Develop an E-Vote system based on Brett Wilson's Pailliar Threshold Cryptography web services. Create or improve component of such a system.

SCOLD: Secure Collective Network Defense

- Develop new Internet protocols for supporting multiple path connections and defending against DDoS attacks.

SGFR: Secure Groupware for First Responder.

- Develop efficient secure instant messaging systems based on efficient group key distribution and open source jabber system,

IMPACT: Improve Measurable Performance Against Cyber Threats: Joint work with Drs. Zhou and Boult.

- Develop techniques that utilize efficient intrusion information fusion and enhanced differentiated services on both servers and routers for enterprise cyber defense.

Secure Information Sharing.

- Develop tools and techniques for supporting large scale secure information access/notification among multiple agencies.

Secure First Responder Sensor Networks:

- Develop secure sensor software for supporting the deployment and tracking of first responders under terrorist threats.

SELinux Related Semester Projects

- Those listed http://oss.tresys.com/projects. Learn these open source projects/tools and demonstrate their capabilities:
  - CDS Framework IDE : designed for cross domain solution developers
  - Certifiable Linux Integration Platform (CLIP) :
  - Reference Policy : makes it easier to maintain and apply baseline security policy for Security Enhanced Linux (SELinux)
  - SELinux Policy IDE (SLIDE) : an open source tool to aid in the development and customization of SELinux policies
  - SETools Policy Analysis Suite : http://www.tresys.com/selinux
  - SEEdit, http://seedit.sourceforge.net
  - Polgen, http://www.mitre.org/tech/selinux
- Reconciling differences in policies between SELinux systems
- Extending management to collections of SELinux hosts
- Policy management for Xen policy (shared toolchain).
- Coordination with guest policies.
- Demonstration of SELinux Policy and its capability using virtual machines on various network services:
- Boeing mentored OS Harden project. http://viva.uccs.edu/wiki
- Security Incidence Handling while continuing operation.

Homework#1

See http://cs.uccs.edu/~cs591/homework.html

- Part1: Create Please create a personal web page on CS Unix machines with your personal photo, basic vita, your interests in this class, and including later on the potential semester projects that you may work on. Put it in ~<login>/public_html/cs591/<login>.html and picture in ~<login>/public_html/cs591/images/<login>.jpg.
- Part 2: Access VMWare based Virtual Machines and Launch MS LSASS exploits Using MetaExploit Framework with AddUser and Bind Shell Payload.
- Part 3: Request Personal E-mail certificates from Thawte Certificate Authority for setting up secure email communication (IE/Outlook or Firefox/Thunderbird). https://www.thawte.com/secure-email/personal-email-certificates/index.html