

Cyber Security Through a Defense in Depth Approach

Victor Hazlewood, CISSP

Senior Cyber Security Analyst

April 20, 2007

Cyber Security

- **Intro to Information Assurance**
- **Threats**
- **Defense-In-Depth strategy overview**
- **References**
- **Q&A**

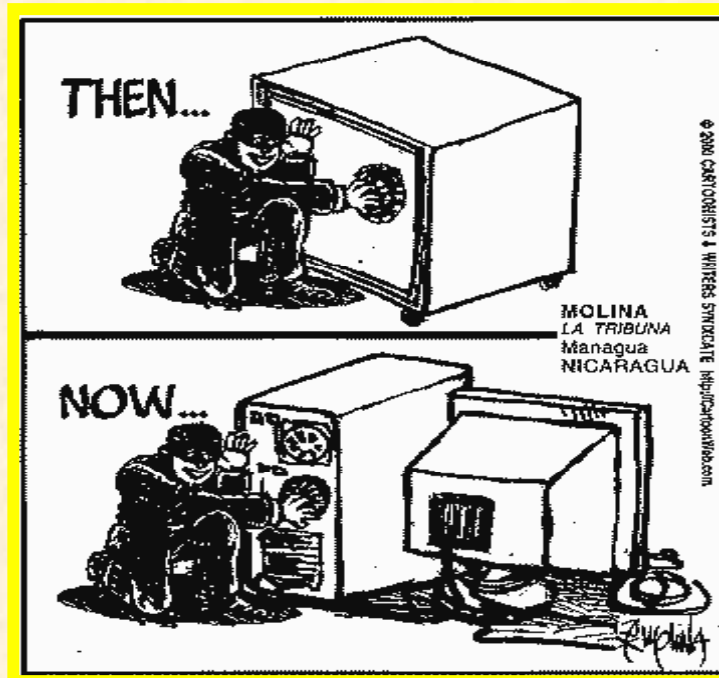
Introduction to Information Assurance

“Information assurance is ensuring that your information is where you want it, when you want it, in the condition that you need it, and available [only] to those that you want to have access to it”

**- Andrew Blyth and Gerald L. Kovacich,
Information Assurance: Surviving in
the Information Environment**

Threats

- External Intruders
- Insiders
- Competitors
- Organized Crime
- Terrorists
- Hardware and software failures



Who... Us Worry?

Saturday, May 08, 2004

Incident: Computer System at U.C. San Diego Hacked

From today's Yahoo News:

[Yahoo! News - Computer System at U.C. San Diego Hacked](#):

"Computer System at U.C. San Diego Hacked
Fri May 7, 11:55 PM ET Add U.S. National - AP to My Yahoo!

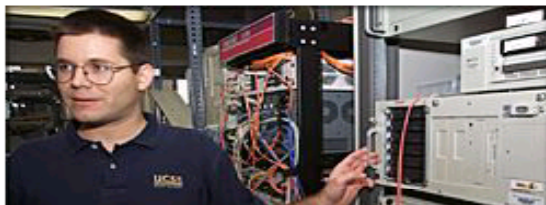
SAN DIEGO - Hackers broke into the computer system of the University of San Diego, compromising confidential information on about 380,000 students, employees, alumni and applicants.



Hackers: Internet could be crippled in half an hour



'Mafiaboy' Arrested Canadian Teen Charged in Web Attacks



InfoWorld LEAD WITH KNOWLEDGE

INDEX: TOP SUBJECTS: CRM | Security

SEARCH: Search Criteria

Home // News // Article

NEWS

REUTERS

PRINT ARTICLE

EMAIL ARTICLE

Qualcomm CEO's laptop missing, police believe stolen

April 19 — A 15-year-old Canadian who goes by the online

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

UT-BATTELLE

Who... Us Worry?

- **The open collaborative nature of the research and academic environment is an inviting target**
- **Let me illustrate in an example...**

Intrusion Example

- **March 2004 – Several universities, gov't labs compromised with suckit kernel rootkit, trojan ssh client**
- **April 04 – SDSC, Stanford, hacker email thanking Berkeley folks, Wash Post story, SDSC begins trace, .mil DoD**
- **May 04 – more universities, gov't labs, SDSC users home dirs wiped, Big Company hit**
- **June 04 – more univ, univ system files wiped**

Intrusion Example

- **July 04 – more univs, encrypted traffic replay method discovered, download site monitored**
- **Aug 04 – rootkit client used to trace, possible suspect id'ed in Sweden, new rootkit in use**
- **Sept 04 – hacker updates trojan ssh client**
- **Oct 04 – foreign law enforcement contacted**

Intrusion Example

- **May 05 – Swedish law enforcement serves search warrant on home of juvenile, intrusion activity stops**
- **Feb 06 – Swedish court proceedings against defendant**
- **Feb 06 – Swedish court acquits defendant!**

Intrusion Example

- **Intruder Infrastructure**

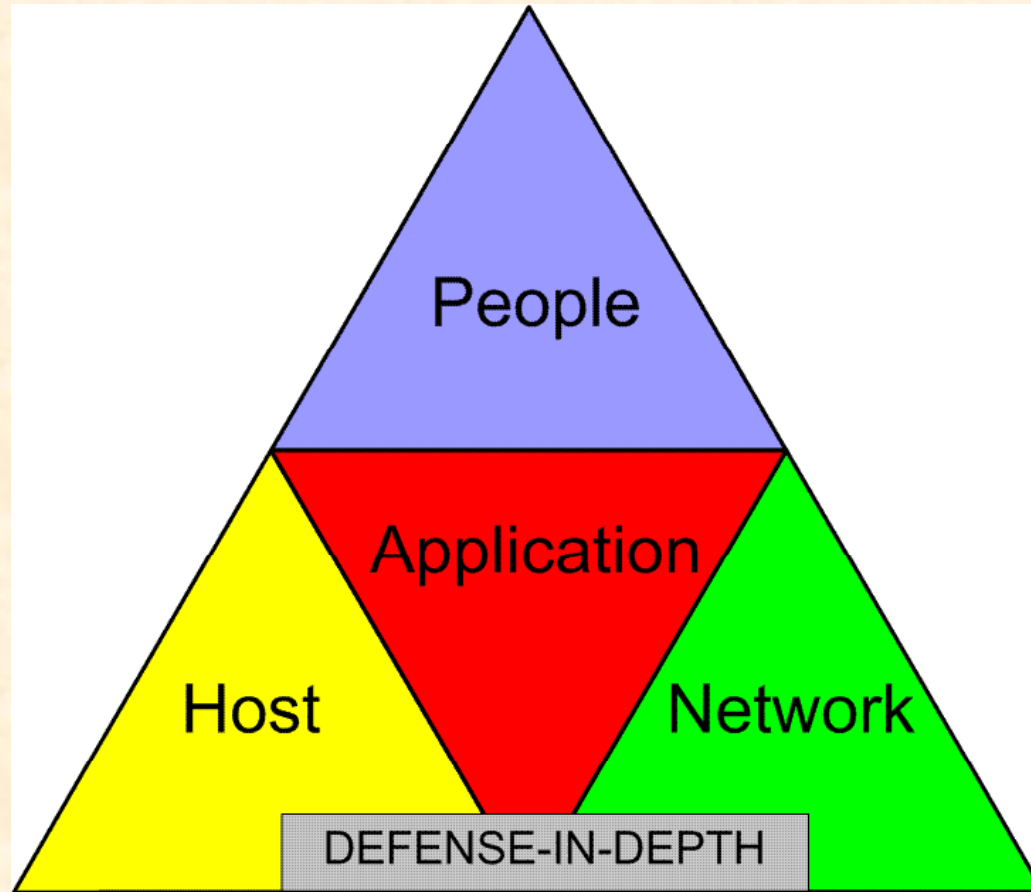
Intrusion: Tools employed

- **ftp or website for downloads**
- **Suckit rootkit (linux kernel rootkit)**
- **Trojan ssh client**
 - **Email to Ip@host**
 - **Port 53/55 data to a DNS entry**
 - **Dynamic DNS for stolen user credentials path**
- **ssh meow backdoor**
- **Ettercap sniffing**
- **nfsshell**
- **.php scripts**
- **Identify system administrators (root group)**
- **Hacker read user and administrator email**

Other Tales of Cybercrime

- Recommend the following reading
 - *Cuckoo's Egg* by Clifford Stoll
 - *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, Richard Powers
 - *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, Shimomura and Markoff
 - *The Fugitive Game ...*, Jonathan Littman

Defense In Depth Strategy



Defense In Depth



Roles and Responsibilities

- **Define information systems roles**
- **Establish management support**
- **Formalize communications**
- **Formalize policy, process and procedures**

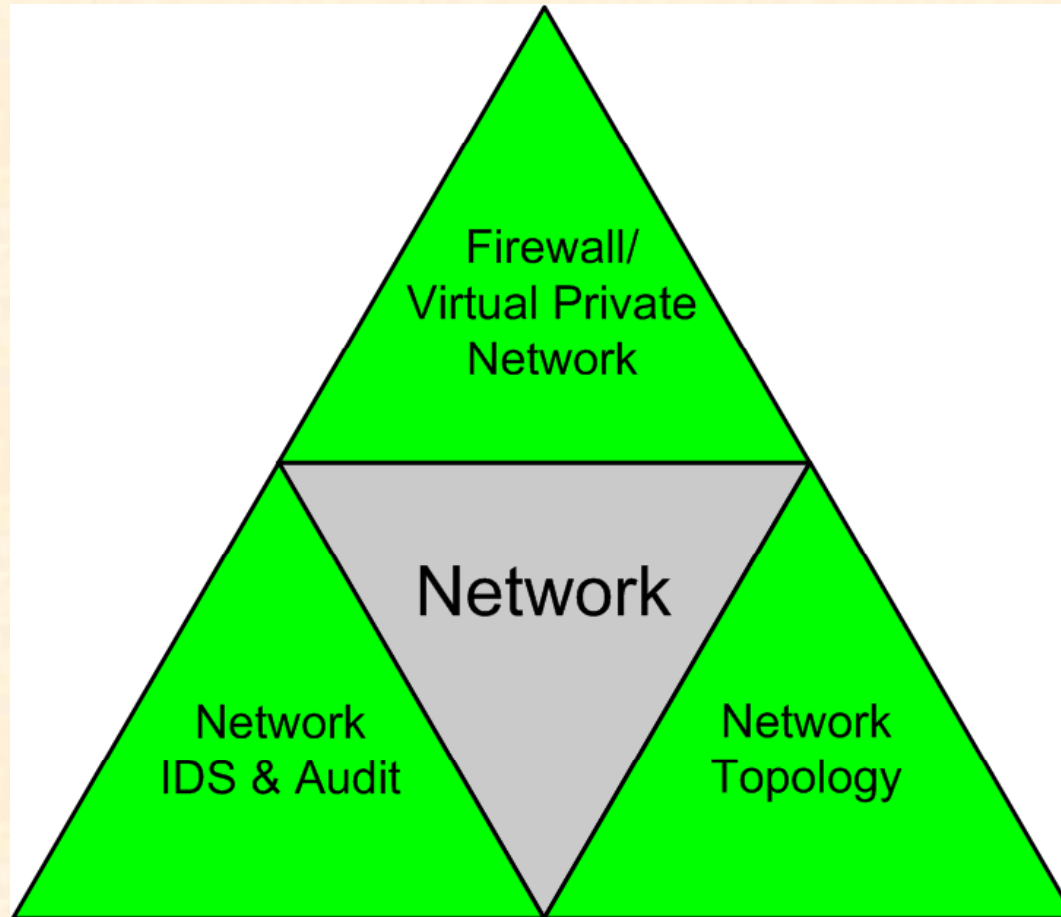
Roles

- **Chief Information Security Officer**
- **Chief Privacy Officer**
- **Systems Administrator**
- **Security Administrator**
- **Database Administrator**
- **Webmaster**
- **Postmaster**
- **Operator**
- **Help Desk Associate**

Other People Issues

- **Skills and Training**
- **Incident Response**
- **Security Awareness Training**

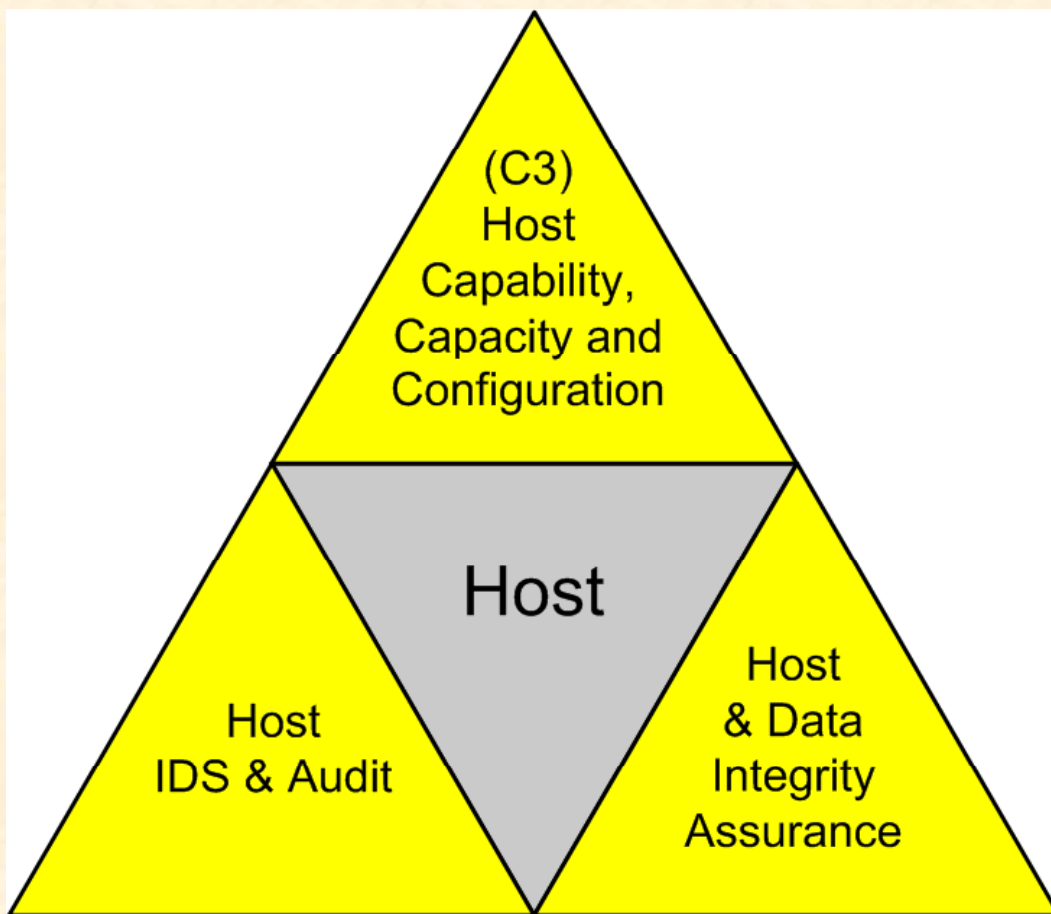
Defense In Depth



Network Issues

- **Firewalls and VPNs**
- **Network topology**
- **Network Intrusion Detection System**

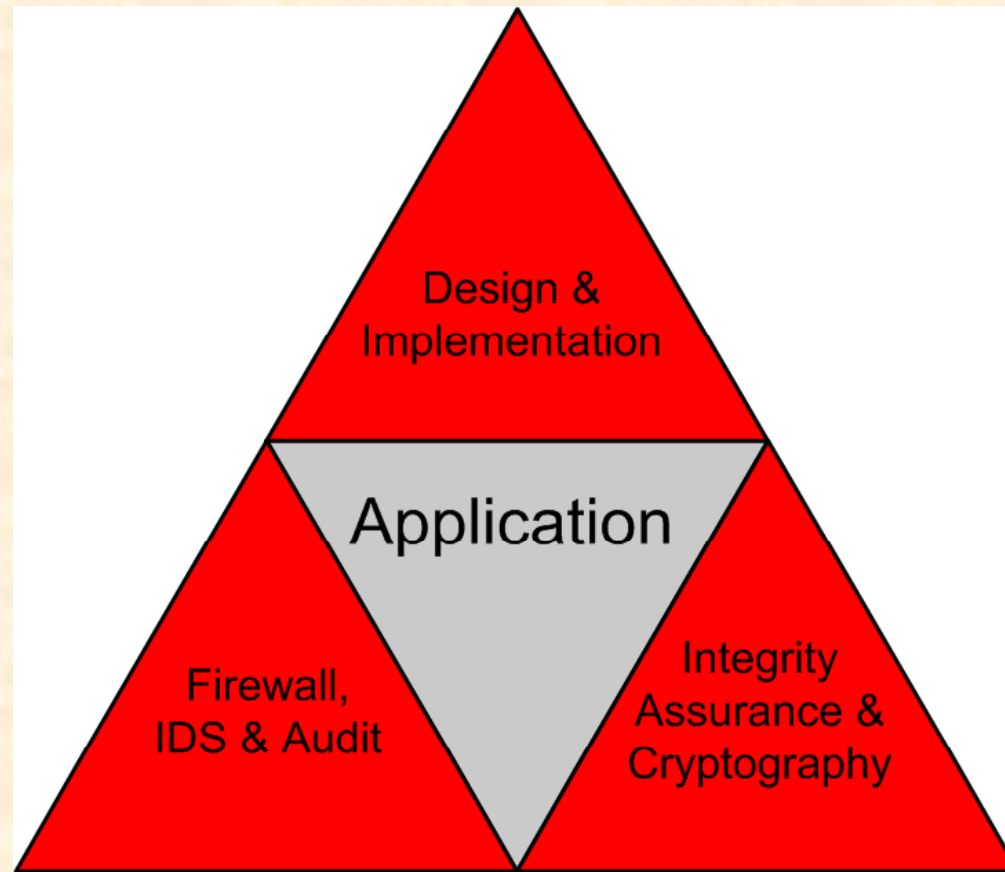
Defense In Depth



Host Issues

- **Host Intrusion Detection System**
 - Unix/cisco syslog
 - Windows event logs
 - Centralized log server concept
- **Configuration**
 - Patch Management
 - Configuration management with cfengine or SMS
 - backups
- **Host Integrity Assurance (Tripwire)**
- **Vulnerability scanning**

Defense In Depth



Application Security

- **Security of applications is today's weak link. Many application developers are not trained or skilled in designing and implementing secure applications**
- **Application firewall usually by content inspection**
- **Application audit trails**
- **Using cryptography and ensuring application integrity**

The Protection Gap*

- **Information system protection measures have not kept pace with rapidly advancing technologies**
- **Information security programs have not kept pace with the aggressive deployment of information technologies within enterprises**
- **Two-tiered approach to security (i.e., national security community vs. everyone else) has left significant parts of the critical infrastructure vulnerable**
- *** source Ron Ross of NIST**

References

- **Regulations**
 - **HIPPA**
 - **Sarbanes-Oxley**
 - **California SB1386**
 - **FISMA**
 - **Others...**
- **Standards**
 - **ISO 17799**

NIST Security Publications

- **FIPS Publication 199** (Security Categorization)
- **FIPS Publication 200** (Minimum Security Requirements)
- **NIST Special Publication 800-18, Rev 1** (Security Planning)
- **NIST Special Publication 800-26, Rev 1** (Reporting Formats)
- **NIST Special Publication 800-30** (Risk Management)
- **NIST Special Publication 800-37** (Certification & Accreditation)
- **NIST Special Publication 800-53** (Recommended Security Controls)
- **NIST Special Publication 800-53A** (Security Control Assessment)
- **NIST Special Publication 800-59** (National Security Systems)
- **NIST Special Publication 800-60** (Security Category Mapping)

Questions or Comments?