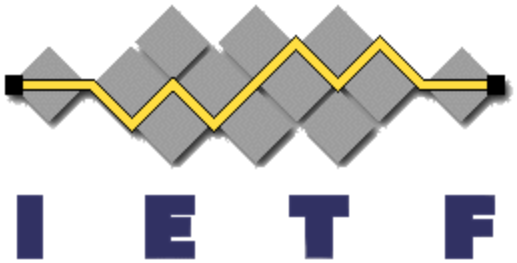


RFC 2196 – Site Security Handbook

a guide to developing computer security policies and procedures for sites that have systems on the Internet

B. Fraser SEI/CMU

INSA
Information Networking Security and Assurance Lab
National Chung Cheng University

Agenda

1. Introduction
2. Security policies
3. Architecture
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

Agenda

1. **Introduction**
2. Security policies
3. Architecture
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

1 Introduction

- This handbook is a guide to setting computer security policies and procedures for sites that have system on the internet.
- Definitions
  - **Site** – any organization that owns computer or network-related resources.
  - **Internet** – RFC 1594

    A collection of thousands of networks linked by a common set of technical protocols which make it possible for users of any one of the networks to communicate with, or use the services located on, any of the other networks
  - **Administrator**
  - **Security administrator**
  - **Decision maker** – refers to those people at a site who set or approve policy.

1.5 Basic Approach

- Steps to develop a security plan for your site

1. Identify what you trying to protect

2. Determine what you are trying to protect it from.

The cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you.

5. … continuously and make improvements each time a weakness is found.

… likely the threats are.

4. Implement measures which will protect your assets in a cost-effective manner

1.6 Risk Assessment

- It is possible to be mislead about where the effort is needed.
- Risk analysis
  - Determining what you need to protect, what you need to protect it from, and how to protect it.

1. Identifying the assets
   - the basic goals of security are availability, confidentiality, and integrity
2. Identifying the threats
   - Each threat should be examined with an eye to how the threat could affect these areas

1.6.2 Identifying the Assets

Hardware	CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drivers, communication lines, terminal server, routers
Software	source programs, object programs, utilities, diagnostic programs, operating systems, communication programs
data	During execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
People	User, administrators, hardware maintainers
Documentation	On programs, hardware, systems, local administrative procedures.
Supplies	Paper, forms, ribbons, magnetic media.

1.6.3 Identifying the Threats

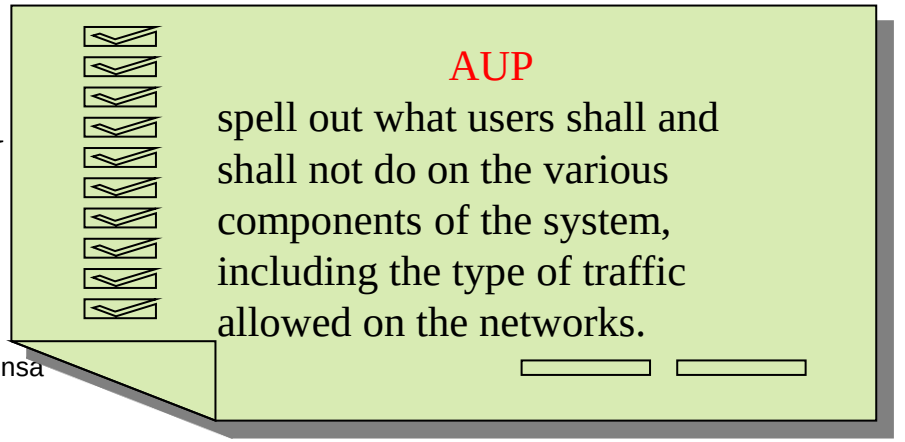
- The following are classic threats that should be considered
  1. Unauthorized access to resources and/or information
  2. Unintented and/or unauthorized disclosure of information
  3. Denial of service

Agenda

1. Introduction
2. **Security policies**
3. Architecture
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

2 Security Policies

- What is a security policy and why have one?
  - A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.
- Purposes of a security policy
  - To inform users, staff and managers of their obligatory requirements for protecting technology and information assets.
  - Appropriate Use Policy



2 Security Policies

- Determined by the following Key tradeoff

Monetary
Performance
Ease of use

1. **Services Offered** versus **Security Provided**
2. **Ease of Use** versus **Security**
3. **Cost of Security** versus **Risk of Loss**

Loss of privacy
Loss of data
Loss of service

- Who should be involved when forming policy
  1. Site security administrator
  2. Information technology technical staff
  3. Administrator of large use groups within the organization
  4. Security incident response team
  5. Representative of the user groups affected by the security policy
  6. Responsible management
  7. Legal counsel

2.2 What Makes a Good Security Policy?

- The characteristics of a good security policy
  1. Be implementable through system administration procedures
  2. Be enforceable with security tools
  3. Cleary define the area of responsibility for the users and management.
- The component of a good security policy
  1. Computer technology purchasing Guidelines which specify required, or preferred, security features
  2. A privacy policy which defines reasonable expectations of privacy regarding.
  3. An access policy which defines access rights and privileges to protect assets for users.

2.2 What Makes a Good Security Policy?

- The component of a good security policy
  4. An accountability policy which defines the responsibilities of users.
  5. An authentication policy which established trust through an effective password policy.
  6. An Availability statement which sets users' expectations for the availability of resources.
  7. An Information Technology System & Network Maintenance Policy which describes how both internal and external maintenance people are allowed to handle and access technology.
  8. A Violations Reporting Policy that indicates which types of violations must be reported and to whom the reports are made.
  9. Supporting Information which provides users, staff, and management with contact information for each type of policy violation

2.3 Keeping the Policy Flexible

- In order for a security policy to be viable for the long term, it requires a lot of flexibility based upon an architectural security concept.
- It is important to recognize that there are exceptions to every rule.
  - the policy should spell out what exceptions to the general policy exist.
- Garbage Truck Syndrome
  - This refers to what would happen to a site if a key person was suddenly unavailable for his/her job function.

Agenda

1. Introduction
2. Security policies
3. **Architecture**
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

3 Architecture

1. Objectives

Individual policies can be consistent with the overall site security

   1. Completely defined security plans
      1. the list of network services that will be provided
      2. which areas of the organization will provide the services
      3. who will have access to those services
      4. how access will be provided
      5. who will administer those services.
   2. Separation of services
      - to distinguish between hosts which operate within different models of trust

host or network level

Deny all/ Allow all

Router level

the theory of a hard "crunchy" shell and a soft "squishy“ middle.

   4. Identify real need for services

security complexity can grow exponentially with the number of services provided.

3.2 Network and Service Configuration

1. Protecting the infrastructure
2. Protecting the network
    1. DoS
        - attacking the routers
        - Flooding the network with extraneous traffic
    2. Spoofing
    3. Solutions
        1. Clear-text password
        2. Cryptographic checksum
        3. Encryption
3. Protecting the services
    - Name servers (DNS and NIS(+))
    - Password/key servers (NIS(+) and KDC)
    - Authentication/proxy servers (SOCKS, FWTK)
    - Electronic Mail
    - World Wide Web (WWW)
    - File Transfer (FTP, TFTP)
    - NFS
4. Protecting the Protection

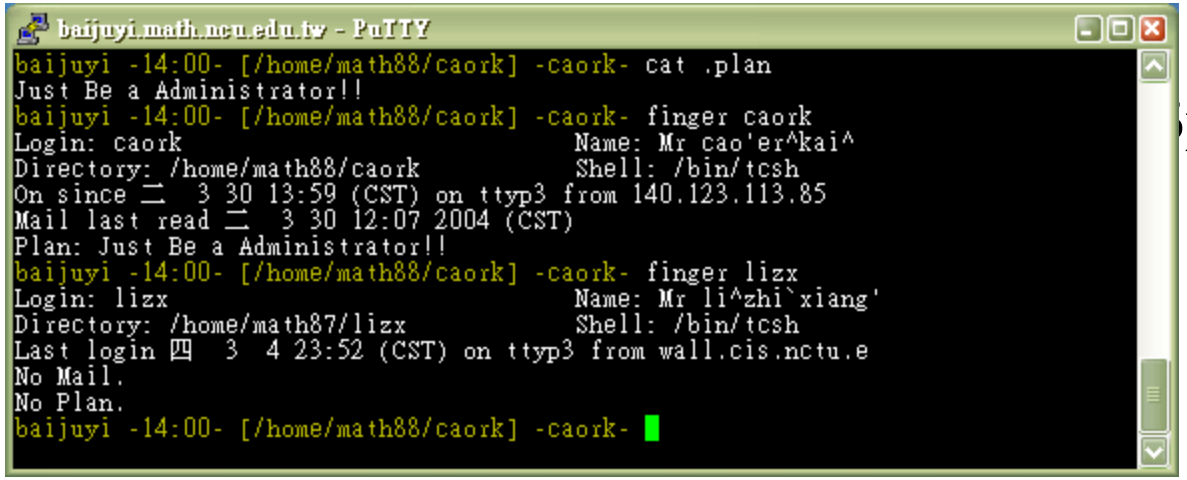
3.3 firewalls

- Filtering routers
  - Filtering policy: source and destination IP address, source and destination TCP port numbers, state of the TCP "ack" bit, UDP source and destination port numbers, and direction of packet flow
- Proxy servers
  - Application Layer Gateway
- Combine with VPN
- Logging function in Firewall

Agenda

1. Introduction
2. Security policies
3. Architecture
4. **Security service and procedures**
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

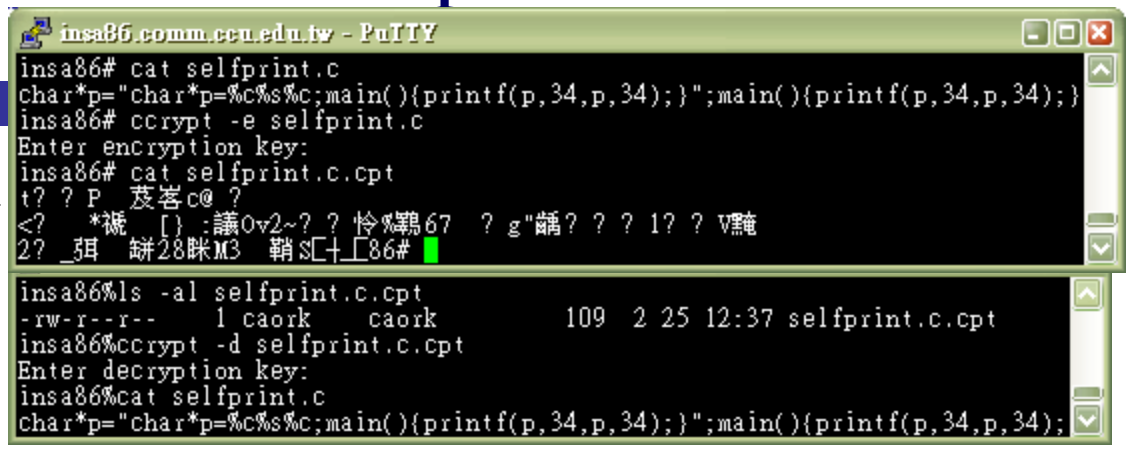
4 Security services and procedures

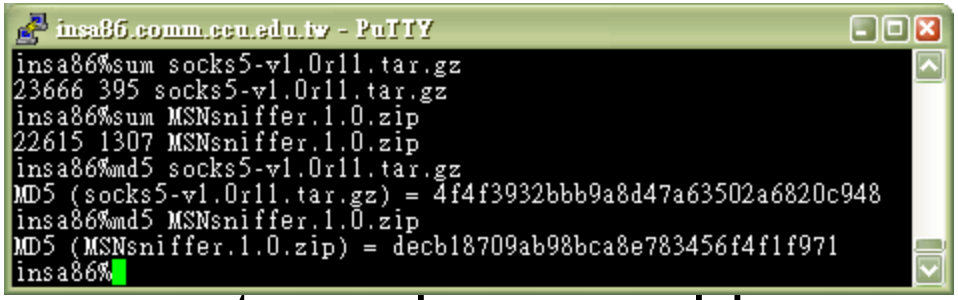
1. Authentication
   - One-time password
   - Kerberos: V4 and V5
   - Choosing and protecting Secret tokens and PINs
   - 

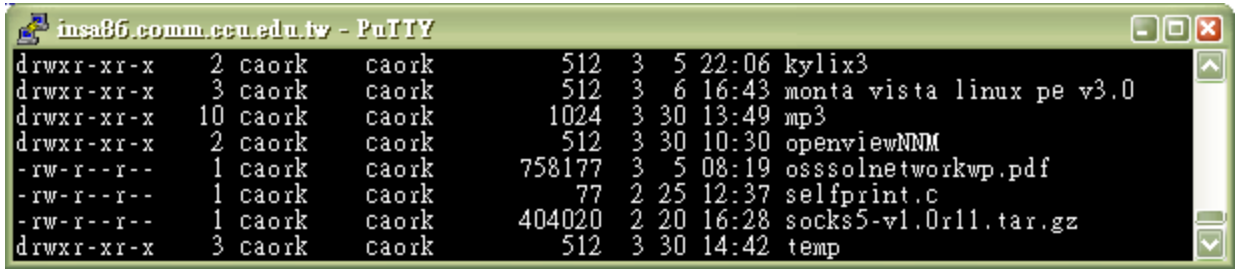
     - A word about the finger daemon

4 Security services and procedures

2. Confidentiality
   - Encryption
3. Integrity
   - Checksum: MD5
4. Authorization
   - The privileges, rights, property, and permissible actions
   - ACL







4.5 Access

- Physical Access
- Walk-up Network Connections
- Other network technologies
- Modems
  - Modem lines must be managed
  - Dial-in user must be authentication
  - Call-back capability
  - All logins should be logged
  - Choose your opening banner carefully
  - Dial-out authentication
  - Make your modem programming as “Bullet-proof” as Possible

4.6 Auditing

- What to collect — Do not gather passwords
  - Login and logout, super user access, ticket generation, and any other change of access or status.
- Collection process
  1. Read/write file
  2. Write-once/read-many
  3. Write-only
- Collection load
  - Data compressed or batch capture
- Handling and preserving audit data
- Legal considerations

4.7 securing backups

1. Make sure your site is creating backups
2. Make sure your site is using offsite storage for backups
3. Consider encrypting your backups to provide additional protection of the information once it is off-site.
4. Don’t always assume that your backups are good.
5. Periodically verify the correctness and completeness of your backups

Agenda

1. Introduction
2. Security policies
3. Architecture
4. Security service and procedures
5. **Security incident handling**
6. Ongoing activities
7. Tools and locations
8. Mailing list and other resources

5 Security incident handling

1. Preparing and planning
2. Notification
3. Identifying an incident
4. Handling
5. Aftermath
6. Administrative response to incident

5.1 preparing and planning for incident handling

- Why learning to respond efficiently to an incident?
  1. Protecting the asset which could be compromised
  2. Protecting resources which could be utilized more profitably if an incident did not require their services
  3. Complying with (government or other) regulations
  4. Preventing the use of your systems in attacks against other systems
  5. Minimizing the potential for negative exposure.

5.1 preparing and planning for incident handling

- A set of objective can be identified for dealing with incidents
  1. Figure out how it happened
  2. Find out how to avoid further exploitation of the same vulnerability.
  3. Avoid escalation and further incidents
  4. Assess the impact and damage of the incident
  5. Recover from the incident
  6. Update policies and procedures as needed
  7. Find out who did it

5.1 preparing and planning for incident handling

- Suggested priorities may serve as a starting point for defining your organization's response
  1. Priority one – protect human life people's safety
  2. Priority two – protect classified and sensitive data. Prevent exploitation of classified and sensitive systems.
  3. Priority three – protect other data, including proprietary, scientific, managerial and other data.
  4. Priority four – prevent damage to systems.
  5. Priority five – minimize disruption of computing resources.

5.2 Notification and points of contact

1. Local managers and personnel
2. Law enforcement and investigative agencies
   - legal and practical issues
     1. Whether your site or organization is willing to risk negative publicity or exposure to cooperate with legal prosecution efforts.
     2. Downstream liability
     3. Distribution of information
     4. Liabilities due to monitoring

5.2 Notification and points of contact

3. Computer security incident handling (response) teams
4. Affected and involved sites
5. Internal communications
6. Public relations – press releases
   - Guidelines to provide to the press
     1. Keep the technical level of detail low.
     2. Keep the speculation out of press statements.
     3. Work with law enforcement professionals to assure that evidence is protected.
     4. Try not to be forced into a press interview before you are prepared.
     5. Do not allow the press attention to detract from the handling of the event.

5.3 Identifying an incident

1. Is it real?
   - Certain indications or symptoms of an incident that deserve special attention
   1. System crashes
   2. New user accounts
   3. New files, or strange file names
   4. Accounting discrepancies
   5. Changes in file lengths or dates.
   6. Attempts to write to system
   7. Data modification or deletion
   8. Denial of service
   9. Unexplained, poor system performance
   10. Anomalies
   11. Suspicious probes
   12. Suspicious browsing
   13. Inability of a use to log in due to modifications of his account.

5.3 Identifying an incident

2. Types and scope of incidents
    1. Is this a multi-site incident?
    2. Are many computer at your site affected by this incident?
    3. Is sensitive information involved?
    4. What is the entry point of the incident?
    5. Is the press involved?
    6. What is the potential damage of the incident?
    7. What is the estimated time to close out the incident
    8. What resource could be required to handle the incident?
    9. Is law enforcement involved?
3. Assessing the damage and extent

5.4 Handling an incident

1. Types of notification and exchange of information
   - The following minimum information should be provided
   1. Timezone of logs, … in GMT or local time
   2. Information about the remote system
   3. All log entries relevant for the remote site
   4. Type of incident
2. Protecting evidence and activity logs
   - Gathering evidence
   1. All system event
   2. All actions you take
   3. All external conversations

5.4 handling an incident

3. Containment
4. Eradication
5. Recovery
6. Follow-up
   - to write a report describing the exact sequence of events:
     1. the method of discovery
     2. Correction procedure
     3. monitoring procedure
     4. a summary of lesson learned

5.5 Aftermath of an incident

- In the wake of an incident, several actions should take place.

1. An inventory should be taken of the systems' assets
2. The lessons learned as a result of the incident should be included in revised security plan to prevent the incident from re-occurring
3. A new risk analysis should be developed in light of the incident.
4. An investigation and prosecution of the individuals who caused the incident should commence, if it is deemed desirable

5.6 Responsibilities

1. Not crossing the line
2. Good internet citizenship
3. Administrative response to incidents

Agenda

1. Introduction
2. Security policies
3. Architecture
4. Security service and procedures
5. Security incident handling
6. **Ongoing activities**
7. Tools and locations
8. Mailing list and other resources

6 Ongoing activities

1. Subscribe to advisories that are issued by various security incident response teams.
2. Monitor security patches that are produced by the vendors of your equipment, and obtain and install all that apply.
3. Actively watch the configurations of your systems to identify any changes.
4. Review all security policies and procedures annually
5. Read relevant mailing lists and USENET newsgroups to keep up the date with the latest information being shared by fellow administrators
6. Regularly check for compliance with policies and procedures.

Agenda

1. Introduction
2. Security policies
3. Architecture
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. **Tools and locations**
8. Mailing list and other resources

7 Tools and locations

- COPS, DES, Drawbridge, identd, ISS, Kerberos, logdaemon, lsof, MD5, PEM, PGP, rpcbind/portmapper replacement, SATAN, sfingerd, S/KEY, smarsh, ssh, Swatch, TCP-Wrapper, tiger, Tripwire, TROJAN.PL

1. CERT Coordination Center
   - ftp://info.cert.org:/pub/tools
2. DFN-CERT
   - ftp://ftp.cert.dfn.de/pub/tools
3. Computer operations, audit, and security tools (COAST)
   - soast.cs.purdue.edu:/pub/tools

Agenda

1. Introduction
2. Security policies
3. Architecture
4. Security service and procedures
5. Security incident handling
6. Ongoing activities
7. Tools and locations
8. **Mailing list and other resources**

8 Mailing lists and other resources

- Mailing lists
  1. CERT advisory
     - mailto: cert-advisory-request@cert.org
     - Body: subscribe cert <FIRST NAME> <LAST NAME>
  2. VIRUS-L List
     - mailto: listserv%lehiibm1.bitnet@mitvma.mit.edu
     - Body: subscribe virus-L FIRSTNAME LASTNAME
  3. Internet Firewalls
     - mailto: majordomo@greatcircle.com
     - Body: subscribe firewalls user@host
- USENET newsgroups
  1. comp.security.announce
  2. comp.security.misc
  3. alt.security
  4. comp.virus
  5. comp.risks
- World-Wide Web Pages
  1. http://www.first.org
  2. http://www.alw.nih.gov/Security/security.html
  3. http://csrc.ncsl.nist.gov