SE 4C03 Winter 2008

10 Defense Mechanisms

William M. Farmer

Department of Computing and Software
McMaster University

1 April 2008

Defensive Services

- Authentication (subject, source).
- Access control (network, host, file).
- Data protection (confidentiality, integrity, availability).
- Auditing.
- Monitoring.

Defensive Mechanisms

- Authentication mechanisms.
- Host-based mechanisms and procedures.
- Network firewalls.
- Virtual private networks (VPNs).
- Encryption.

Host-based Mechanisms and Procedures

- User account security.
- File protection.
- Access control of network services.
- Auditing and monitoring.

User Account Security

- Secure root account.
  - Choose a strong password for the root account.
  - Change the root password periodically.
  - Use different root passwords for different machines.
  - Use the root account only for administrative purposes.
  - Do not remotely telnet or FTP into a root account.
  - Do not su to root during a remote telnet session.
- Secure other user accounts.
  - Never create a user account without a password.
  - Require all users to have strong passwords.
- Protect the password file.
  - Use shadow passwords.

File Protection

- Protect the file system.
  - Use groups and read, write, and execute permissions.
  - Perform regular backups of the file system.
- Be careful with SUID and SGID programs.
- Encrypt files that need extra protection.

Access Control of Network Services

- Turn off all unnecessary and dangerous network services (e.g., `finger` and `tftp`).
  - Uninstall the software needed for such a service.
  - For a service running under the `inetd` server, comment out the relevant line in the `/etc/inetd.conf` file (which maps services to servers).
- Restrict access to network servers using wrappers.
  - For example, the `tcpd` server ("TCP Wrapper") which controls access via the `hosts.allow` and `hosts.deny` files.
- Restrict access to network servers using packet filters.
- Carefully configure dangerous services such as anonymous FTP and Web services.
- Provide Secure Shell (`ssh`) instead of `rlogin`, `rsh`, and `rcp`.

Network Firewalls: Definitions

- A firewall is a collection of hosts, routers, and other hardware that controls traffic between two parts of a network.
- A bastion host is a firewall computer that is heavily protected because it is exposed to attack.
- A packet filter is a device that accepts (forwards) or rejects (drops) packets usually on the basis of just the information in the packet's header.
- A stateful packet filter is a packet filter that accepts or rejects packets on the basis of what previous packets have been seen as well as on the basis of the information in the packet's header and data.
- A proxy is a middleman server that relays client requests and external server replies across a firewall.

Benefits and Uses of a Firewall

1. Enables network security to be implemented and administered in highly centralized manner.
2. Can enforce a network security policy.
3. Can reduce a network's external exposure to a just small number of hosts.
4. Can monitor network traffic efficiently.
5. Can implement network address translation.
6. Can divide an organization's domain into smaller, more manageable units.

What a Firewall Cannot Protect Against

1. Activities behind the firewall initiated by insiders.
2. Traffic that does not go through the firewall.
3. Illegitimate communication that is "tunneled" through legitimate communication.
4. Dangerous code (e.g., a virus) that is legitimately allowed to go through the firewall.
5. New unforeseen threats.

Firewall Architectures

- Screening router.
  - External packet filtering router.
- Dual-homed gateway.
  - External bastion host.
- Screened gateway.
  - External packet filtering router.
  - Internal bastion host.
- Screened subnet.
  - External packet filtering router.
  - Perimeter network.
  - Internal (choke) filtering router.

Packet Filters

- Inexpensive to build since most routers have filtering capabilities.
- Most routers can have two packet filters at each of its network interfaces, one filter for incoming packets and one for outgoing packets.
  - A packet flowing through a router can be filtered at both the interface where it enters and the interface where it exits.
- Packet filters are especially useful for catching source spoofing packets:
  - Packets coming from the outside which have inside source addresses.
  - Packets coming into a host which have the loopback address (127.0.0.1) as their source address.

Implementing a Packet Filtering Policy

- Designing a packet filtering policy is not very hard.
- Implementing a packet filtering policy with a router can be difficult.
  - Configuring packet filters is often akin to assembly language programming.
  - The syntax of a filter programming language is often inflexible.
  - An implementation involving more than one vendor can be very confusing because different vendors can use different approaches.
  - Documentation is often incomplete or incorrect, and the filter devices themselves may not work as documented.

Packet Filtering Policies

- The Foundational Packet Filtering Policy:
  1. No non-TCP packets are allowed through the firewall.
  2. TCP connections across the firewall may not be initiated from outside the firewall.
  3. No spoofing addresses inside the firewall.
- Many packet filtering policies are modifications of the foundational packet filtering policy.
- Some services initiated by internal users require packets that violate the Foundational Packet Filtering Policy:
  - UDP-based services.
  - ICMP-based services.
  - FTP in normal mode.
  - X11 clients operating outside the firewall.
  - DNS.

Proxy Servers

- Benefits:
  - Can create virtual UDP and TCP connections and manage them using state information.
  - Reduces exposure of internal clients and servers.
  - Reduces logins required on firewall hosts.
  - Can cache requested information.
  - Can translate network addresses.
  - Can be transparent to users.
- Kinds of proxy servers:
  - Application-level (usually dedicated to a protocol).
  - Circuit-level (usually generic).

Steps for Building a Firewall (1)

1. Formulate a network security policy.
2. Choose a firewall architecture.
3. Configure the firewall hosts (routers and bastion hosts).
   - Pump up hardware: Have plenty of memory, disk space, computing capacity.
   - Slim down software: Install only software which is absolutely necessary.
   - Configure disks with multiple, large partitions.
   - No unnecessary user accounts.
   - Set up minimal routing tables, turn off ARP, and do not use any dynamic routing mechanisms.
   - Turn off all network services initially.
   - Close all packet filters initially.

Steps for Building a Firewall (2)

5. Develop administrative procedures and mechanisms for:
   - Logging.
   - File backup.
   - Hardware and software upgrading.
   - Performance monitoring.
   - Intrusion monitoring and response.
6. Install the firewall.
   - Connect the firewall to the internal and external networks.
   - Possibly have a direct connection for emergencies.
7. Install network services one at a time.
   - Do plenty of testing.
   - Use IP addresses instead of domain names.