Network Security

by David G. Messerschmitt

Supplementary section for Understanding Networked Applications: A First Course, Morgan Kaufmann, 1999.

By its very nature, a public network is a security risk, as it opens up access to each connected host to everybody (see Chapter 13). Fortunately, there are measures that can be taken to mitigate these risks. Both the risks, and the measures taken to counter them are dependent on an understanding of the network architecture presented earlier in this chapter.

Secure and Insecure Authentication

One key to protecting a host is access control and associated authentication of users. Unfortunately, some simple authentication approaches commonly used are insecure. A common approach is to ask a user to supply a password, which can be captured in transit unless the entire session is encrypted. Alternatively, the IP address of a host is sometimes used to authenticate it. An intruder who gains physical access to a network (or can surreptitiously install a program in a host connected to a network) can monitor network traffic. This *sniffing attack* can uncover valuable information, such as the IP address of hosts or user passwords. It is possible for an attacker to masquerade as a different host by *spoofing* an IP address, making it appear that packets are originating from another host. Authentication based on a shared secret or certificate as was described in Chapter 13 is much more secure.

Servers sometimes authenticate another host by matching its domain name against its IP address by making a query to the domain name system. Unfortunately, the DNS is itself insecure, and thus should not be trusted. Also, the information sent among DNS zones can be sniffed, uncovering potentially valuable information such as a list of domain names and IP addresses internal to an intranet. These examples illustrate that there many subtle security issues on a public network. On the other hand, a public network actually benefits from many attempts at penetration, which increase the likelihood that subtle security flaws are discovered and repaired.

Security Flaws in Public Servers

Many Internet hosts must offer publicly available servers, for example to send and receive email and provide Web services. Not infrequently these servers have security flaws. Once external access to these servers is allowed, attackers can exploit them. Web servers are especially vulnerable given the capability to extend them—using a *common gateway interchange (CGI)*—allowing the HTTP server to invoke an arbitrary program or script. Sometimes ordinary users add CGI extensions, and they sometimes have security flaws.

Firewalls and Packet Filtering

Applications in an intranet can be publicly available without compromising the security of other applications or hosts by adding firewalls. As described in Chapter 13, firewalls create a *trusted enclave* that is partially isolated from the global Internet (less Draconian than physically isolating the enclave). They enforce security policies such as:

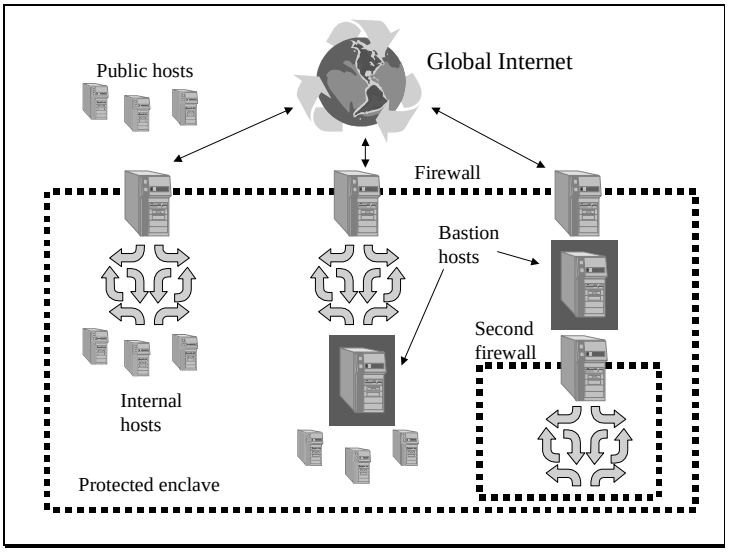

Figure 1. Several typical firewall configurations.

- *Access control*. Limit access from outside the enclave to a specific list of hosts (or whole sub-networks). Alternatively a specific list of hosts can be excluded.
- *Application control*. Restrict services and applications available to users outside the enclave, or access of internal users outside the enclave, by restricting the transport protocols that can pass through the firewall (usually to TCP), the acceptable addresses, and applications.

Firewalls must be continually monitored by system administrators. Suspicious activity can be logged, and system administrators alerted. It is common to put public servers requiring unfettered access to the Internet *outside* the trusted enclave, hoping to isolate any security problems caused by these servers from penetrating the enclave.

Several common configurations for firewalls [Gar96] are shown in Figure 1.. The elements of these configurations include:

- The firewall acts as a *packet filter*, examining all IP packets and passing only those meeting specific criteria, such as destination, or running specific transport protocols (like TCP), or supporting specific applications.

Firewalls Inhibit Innovation

One key source of success in the Internet was keeping the network simple, and allowing additional capabilities (new transport protocols or applications) to be added. It has traditionally been possible for a single programmer to make an innovation and distribute it widely in very short order.

Sadly, this capability is lost where firewalls are added. Since firewalls specifically limit protocols and applications, new innovations are available to users within a trusted enclave only when the firewall is upgraded. Since firewalls generally incorporate only standardized protocols and applications, the practical impact of this is to greatly increase the importance of standardization activities like the IETF (see "Internet Engineering Task Force (IETF)" on page 190). Strong security is invasive to users and organizations in many ways.

- *Bastion hosts* are special hosts *within* the enclave. If there are bastion hosts, the firewall only allows IP packets to pass to and from the bastion hosts (other packets are blocked).
- *Public hosts* are special hosts *outside* the enclave. This is where, for example, a public HTTP server might run.

With a single firewall, incoming traffic may be restricted to specific hosts, and some services may be blocked, but internal hosts are given unfettered access to the outside. It may be feasible for intruders to set up *tunneling* of one application (supposedly prohibited) within another (that is allowed). For example, a TCP connection may appear to the firewall to be implementing telnet (which is allowed) but the telnet packets have some other forbidden application encapsulated within them.

When bastion hosts are added, then the firewall passes only packets destined for or originating from the bastions. Bastion hosts provide external services, such as email, and can execute *proxies* for the benefit of applications running on non-bastion hosts. (A proxy is a program that acts on behalf of another.) This limits the damage due to insecure servers and tunneling.

Finally, in the double-firewall architecture, a second firewall interior to the bastion hosts provides an additional layer of protection. For example, an intruder gaining access to the bastion host can't penetrate to hosts within the interior enclave. This architecture is especially common with extranets, where the bastions provide extranet functions and the interior firewall provides additional protection for sensitive internal activity.

Firewalls are also used to compartmentalize an organization. For example, access policies may reasonably prohibit the engineering department from accessing human resources servers, and firewalls can enforce such policies. Recall, however, that firewalls are effective only as part of a security *system*, which should include confidentiality, authentication, and operational vigilance.

Where to Use Encryption and Authentication

The encryption techniques described in Chapter 13 assure confidentiality, but the question arises "where to use encryption?". Chapter 13 incorporated encryption into applications (such as SET, PGP, and SHTTP). This is the most secure approach, but places additional burdens on application developers and is relatively invasive to users (who must deal with passwords, secrets, etc.). Armed with an understanding of the network, there are other possibilities that trade a bit lower security for less intrusiveness. They differ as to the protocol layer where authentication and encryption is implemented, and also position in the network topology:

- *Firewall-to-firewall*. An organization frequently has two or more geographically separated locations, each with a protected enclave. Confidential internal communication among locations can be achieved using leased dedicated facilities (a *private* network). An extranet—a private network embedded within the public Internet—is less expensive. This can be achieved using encrypted semi-permanent IP connectivity among firewalls, which do the encryption and decryption and authenticate one another to avoid spoofing attacks.
- *Host-to-host*. Authentication of hosts and encryption of IP packet payloads can be performed at the IP layer. The IETF is standardizing these capabilities (called *IPsec*).
- *Process-to-process*. One could argue that authentication and encryption should be provided as a normal part of a process-to-process communication service. *Secure sockets layer (SSL)* was originally proposed by Netscape to provide authentication and confidentiality in Web browser-to-server connections, but is available for any TCP process-to-process communica-

tion.

- *Link-by-link*. The previous approaches encrypt only (IP or TCP) packet *payloads*. When IP packet headers aren't encrypted (because network routers must examine them to do packet forwarding) an attacker can do *traffic analysis*; that is, see who is communicating with whom and the amount of traffic. This privacy concern can be redressed by encryption and decryption on communication links between packet switches (including packet headers). Internal to the switch, packet headers must not be encrypted so packets can be forwarded, but an intruder monitoring the communication link would gain no information about packet content, source, or destination. Link encryption is particularly attractive on wireless communication links (which are relatively easy to monitor).

These possibilities are not exhaustive, but serve to illustrate a range of possibilities.

Discussion

D1 Discuss the increasing importance of security in the Internet, in light of its history as a research network (see "The Origins of the Internet" on page 311).

D2 The firewall presumes that users internal to a protected enclave don't present a threat. Discuss situations where this assumption may be violated.

D3 Discuss the role of operational vigilance on security. What should network operations be on the lookout for? How should they respond to security problems they encounter?

Review

Network security is a major issue, especially in the Internet which arose in a relatively benign and trusted environment. Thus, many legacy applications use low-security techniques, such as basing authentication on source address. Firewalls provide a focus point (at the boundary of a trusted enclave) to enforce security policies, such as control of access, protocols, and applications. Using firewall-to-firewall encryption and authentication, virtual private networks can be embedded within the global public Internet.

Concepts

Security:

- Firewalls
- Encryption

Exercises

E1. Discuss the access control mechanisms that you have observed in:

a. A local bank branch

b. A military base

c. A scheduled airline

E2. Give two real-world analogies to each of the following;

a. A firewall

b. A bastion host

c. A public host outside a firewall

E3. Give three example applications where a traffic analysis might be helpful to an intruder in gleaning information that should be private. Describe how the information obtained might be helpful to the intruder.