PRINCIPLES OF INFORMATION SECURITY, FOURTH EDITION

Chapter 6

Security Technology: Firewalls and VPN

Learning Objectives

Upon completion of this material, you should be able to:

1. Recognize the important role of access control in computerized information systems, and identify and discuss widely-used authentication factors
2. Describe firewall technology and the various approaches to firewall implementation
3. Identify the various approaches to control remote and dial-up access by means of the authentication and authorization of users
4. Discuss content filtering technology
5. Describe the technology that enables the use of virtual private networks

Recap

- This chapter uses what may be a familiar meaning **allowing, restricting,** and **denying access to resources**.

Authorization and Access

- Authorization is permission, and access is means.
  - ***Authorization*** *means we allow someone to do something.*
  - ***Access*** *means someone can get at an asset.*

Vocabulary

- **Owner** - A person responsible for the integrity and security of an asset. This may be a management role instead of a technical role.
- **Custodian** - A person who maintains the security of a system, perhaps by adding and removing access by user accounts. (Aka. **Administrator**.)
- **End User** - A person who uses the asset, such as reading a file, opening a web page, or printing some data from a database, but who is not allowed to change access rights to the asset. This concept is also called a subject in some texts.
- **Subjects** (users or processes acting for users) perform operations on objects(assets)
  - ***Supplicant*** - *synonym for "requester"*

Access Controls

- **Mandatory Access Control (MAC)** - The owner defines a security policy, the custodian implements it, and the end users cannot change it;
- Nondiscretionary controls come in two types:
  - ***Role Based Access Control (RBAC)*** *- access is granted to roles (groups) defined on the systems, end users are assigned to roles so they can access assets needed for their jobs.*
  - ***Task Based Access Control (TBAC)*** *- may be the most complex model; rulescan change which role a user is assigned to, based on the task the user is performing, changing the level of access the user has*

Access Controls

- **Discretionary Access Control (DAC)** - least restrictive model; subjects (end users) can own objects, and have total control over them (like a SharePoint web server system);
  - *end users must set and maintain security for their assets, which most people will do badly; processes run by end users inherit their permission levels*

Authentication

- **Authentication** is one of three key elements to security:
  - *Authentication*
    - confirmation of identity
  - *Authorization*
    - granting permissions that are linked to the user's account
  - *Accounting*
    - accountability, auditing - tracking what the user does

Authentication

- Generally, authentication has three factors:
  1. *Something a supplicant knows*
  2. *Something a supplicant has*
  3. *Something a supplicant is*

Something a Supplicant Knows

- Password
  - *23skedoo*
- Passphrase
  - *MTFBWYA*
- PIN
  - *3298*

Something a Supplicant Has

Supplicant Knows

Password
- *23skedoo*

Passphrase
- *MTFBWYA*

PIN
- *3298*

- ID Card
- ATM Card
- Token

Something a Supplicant Is or Can Produce

Supplicant Knows

Password
- *23skedoo*

Passphrase
- *MTFBWYA*

PIN
- *3298*

Supplicant Has

- ID Card
- ATM Card
- Token

Supplicant Is

- Fingerprint
- Hand topography
- Iris Scan

Authentication

Supplicant Knows

Password
- *23skedoo*

Passphrase
- *MTFBWYA*

PIN
- *3298*

Supplicant Has

- ID Card
- ATM Card
- Token

Supplicant Is or Can Produce

- Fingerprint
- Hand topography
- Iris Scan

Firewalls

- Firewalls have been a first line of defense in network security for over 25 years.
  - *A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.*
- A firewall in an information security program that prevents specific types of information from moving between the outside world, known as the untrusted network (example, the Internet), and the inside world, known as the trusted network.

Firewalls

Firewalls fall into five major processing-mode categories:

- **Packet-filtering firewalls:**
  - *E*xamines the header information of data packets that come into a network.
- **Application gateways:**
  - Known also as proxy server since it runs special software that acts as a proxy for a service request.
- **Circuit gateways:**
  - *O*perates at the transport layer. Connections are authorized based on address. Circuit gateways do not usually look at traffic flowing between one network and another, but they do prevent direct connections between one network and another.

Firewalls

Firewalls fall into five major processing-mode categories:

- **MAC layer firewalls:**
  - *This enables these firewalls to consider the specific host computer's identity, as represented by its MAC or network interface card address in its filtering decisions.*
- **Hybrids:**
  - *Combine the elements of other types of firewalls that is the elements of packet filtering and proxy services or packet filtering and circuit gateways.*

Firewalls

Firewalls fall into five major processing-mode categories:

- **Packet-filtering firewalls**
- **Application gateways**
- **Circuit gateways**
- MAC layer firewalls
- Hybrids

Firewalls

To understand further, let's watch this video:

https://www.youtube.com/watch?v=aUPoA3MSajU

Firewalls

Firewall Categorized by Structure

- Commercial-Grade Firewall Appliances
- Commercial-Grade Firewall Systems
- Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.

Firewall Categorized by Structure

- **Commercial-Grade Firewall Appliances**
  - Are stand-alone, self-contained combinations of computing hardware and software.
  - These appliances can be manufactured from stripped-down general purpose computer systems, and/or designed to run a customized version of a general-purpose operating system.
- Commercial-Grade Firewall Systems
- Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.

Firewall Categorized by Structure

- Commercial-Grade Firewall Appliances
- **Commercial-Grade Firewall Systems**
  - Consists of application software that is configured for the firewall application and run on a general-purpose computer.
  - These systems exploit the fact that firewalls are essentially application software packages that use common general purpose network connections to move data from one network to another.
- Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.

Firewall Categorized by Structure

- Commercial-Grade Firewall Appliances
- Commercial-Grade Firewall Systems
- **Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.**
  - Dedicated hardware/software solutions designed for small company or home networks, typically less than 25 computers. Many of the firewall appliances also act as routers, and offer other services such as VPN, content scanning, and virus scanning.

Firewall Categorized by Structure

- **Commercial-Grade Firewall Appliances**
- **Commercial-Grade Firewall Systems**
- **Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.**

Firewall Categorized by Structure

- **Commercial-Grade Firewall Appliances**
  - runs on a custom operating system, on a dedicated device
- **Commercial-Grade Firewall Systems**
  - a software solution that runs on a computer that may or may not be dedicated
- **Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.**
  - device may actually be a cable modem, or DSL modem, may also include router and WAP services, may include intrusion protection

Firewall Categorized by Structure

- **Commercial-Grade Firewall Appliances**
  - runs on a custom operating system, on a dedicated device
- **Commercial-Grade Firewall Systems**
  - a software solution that runs on a computer that may or may not be dedicated
- **Small Office/Home Office (SOHO) Firewall Appliances or Residential-grade firewall.**
  - device may actually be a cable modem, or DSL modem, may also include router and WAP services, may include intrusion protection

Firewall Categorized by Structure

- **Residential (consumer) software**
  - typically a combination of anti-virus, firewall, intrusion detection software; should be run on all devices that connect to a home network

- none of the firewall solutions discussed will protect a network from user error.

Firewall: Software VS. Hardware

- **Software Firewall:** The software option allows the hacker inside your computer to battle a piece of software (free software, in many cases) that may not be correctly installed, configured, patched, upgraded, or designed.
- **Hardware Firewall:** Use of non-routable addresses further extends the protection, making it virtually impossible for the attacker to reach your information. Is a firewall installed between network elements and connected devices, and is tasked with filtering traffic for cyber threat to the network or devices.

When Configuring Firewalls

- All traffic from the trusted network (our network) is allowed out.
- Firewalls are not configurable from the public facing part of the network.
- Mail traffic sent by SMTP is sent to a mail gateway.
  - *Some may be allowed, some denied, but all should be examined by a dedicated device.*
- All ICMP (ping) packets from outside our network should be denied.
  - *This is not always done in practice.*

When Configuring Firewalls

- Telnet requests from the outside should be blocked.
  - *This technology is not often used any more, but it is a potential hack that could be used to control our servers.*
- Public facing web servers should be in a DMZ, should use the secure form of HTTP (HTTPS), and should block requests made on them to contact our trusted network assets.
- Deny traffic that has not been authenticated.

When Configuring Firewalls

- You have just set up firewall rules.
- Firewall rules operate on the principle of "that which is not permitted is prohibited," also known as **expressly permitted rules**.
- An alternative is to write rules for everything you want to deny, then allow everything else.

Content Filtering

- A software filter which most likely restrict a certain web address or the access or certain website:
  - *Have malicious contents*
  - *Banned websites for an specific reason such as prohibited contents*
  - *Or, to restrict internal access to external material.*

Virtual Private Networks (VPNs)

- implementations of cryptographic technology
- is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network.
- The VPN Consortium (VPNC) defines VPN as "a private network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Virtual Private Networks (VPNs)

The book describes three VPN types:

- **Trusted VPN** - uses leased data lines from a data vendor that are guaranteed to be separate from the rest of their network.
- **Secure VPN** - uses security technology and encryption to make your traffic meaningless to eavesdroppers.
- **Hybrid VPN** - uses both of the methods above, typically over several hops to the target network.

LAB TIME