Lecture 28
NETWORK MANAGEMENT -II

Topics Covered

- Proxy Servers
- Potential purposes
- Firewalls
- Protection Methods
- Packet Filters
- Network Address Translation
- Effective Border Security
- Network Management Tasks/Applications
- Performance Management
- Security Management

Proxy Servers

- Proxy server is a server (a computer system or an application program) that acts as an intermediary between for requests from clients seeking resources from the other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server.
- The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol.

Proxy Servers

- If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.
- A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server.
- In this case, it 'caches'(i.e. stores) responses from the remote server, and returns subsequent requests for the same content directly.

Potential purposes

- To keep machines behind it anonymous (mainly for security)
- To speed up access to resources (using caching). Web proxies are commonly used to cache or reserve web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To bypass security/ parental controls.
- To scan transmitted content for malware before delivery.
- To scan outbound content, e.g., for data leak protection.
- To circumvent regional restrictions.

Firewalls

- Sits between two networks
  - Used to protect one from the other
  - Places a bottleneck between the networks
    - All communications must pass through the bottleneck – this gives us a single point of control

Protection Methods

- **Packet Filtering**
  - Rejects TCP/IP packets from unauthorized hosts and/or connection attempts between unauthorized hosts
- **Network Address Translation (NAT)**
  - Translates the addresses of internal hosts so as to hide them from the outside world
  - Also known as IP masquerading
- **Proxy Services**
  - Makes high level application level connections to external hosts on behalf of internal hosts to completely break the network connection between internal and external hosts

Additional services sometimes provided

- **Virus Scanning**
  - Searches incoming data streams for virus signatures so they may be blocked
  - Done by subscription to stay current
    - McAfee / Norton
- **Content Filtering**
  - Allows the blocking of internal users from certain types of content.
    - Usually an add-on to a proxy server
    - Usually a separate subscription service as it is too hard and time consuming to keep current

Packet Filters

- Compare network and transport protocols to a database of rules and then forward only the packets that meet the criteria of the rules
- Implemented in routers and sometimes in the TCP/IP stacks of workstation machines
  - in a router a filter prevents suspicious packets from reaching your network
  - in a TCP/IP stack it prevents that specific machine from responding to suspicious traffic
    - should only be used in addition to a filtered router not instead of a filtered router

Limitations of Packet Filters

- IP addresses of hosts on the protected side of the filter can be readily determined by observing the packet traffic on the unprotected side of the filter
- filters cannot check all of the fragments of higher level protocols (like TCP) as the TCP header information is only available in the first fragment.
  - Modern firewalls reconstruct fragments then checks them
- filters are not sophisticated enough to check the validity of the application level protocols imbedded in the TCP packets

Network Address Translation

- Single host makes requests on behalf of all internal users
  - hides the internal users behind the NAT’s IP address
  - internal users can have any IP address
    - should use the reserved ranges of 192.168.n.m or 10.n.m.p to avoid possible conflicts with duplicate external addresses
- Only works at the TCP/IP level
  - doesn’t do anything for addresses in the payloads of the packets

Effective Border Security

- For an absolute minimum level of Internet security a Firewall must provide all three basic functions
  - Packet filtering
  - Network Address translation
  - High-level application proxying
- Use the Firewall machine just for the firewall
  - Won't have to worry about problems with vulnerabilities of the application software
    - If possible use one machine per application level server
      - Just because a machine has a lot of capacity don't just pile things on it.
        - Isolate applications, a side benefit of this is if a server goes down you don't lose everything
  - If possible make the Firewall as anonymous as possible
    - Hide the product name and version details, esp, from the Internet

Problems Firewalls can't fix

- Many e-mail hacks
  - Remember in CS-328 how easy it is to spoof e-mail
- Vulnerabilities in application protocols you allow
  - Ex. Incoming HTTP requests to an IIS server
- Modems
  - Don't allow users on the internal network to use a modem in their machine to connect to and external ISP (AOL) to connect to the Internet, this exposes everything that user is connected to the external network
  - Many users don't like the restrictions that firewalls place on them and will try to subvert those restrictions

Firewalls Aren’t Perfect?

- Useless against attacks from the inside
  - Evildoer exists on inside
  - Malicious code is executed on an internal machine
- Organizations with greater insider threat
  - Banks and Military
- Protection must exist at each layer
  - Assess risks of threats at every layer
- Cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

Network Management Tasks/Applications

- fault management
- configuration management
- performance management
- security management
- inventory management
- accounting management

Performance Management

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?
- Indicators: availability, response time, accuracy throughput, utilization
- Service efficiency..
- **network throughput** is the average rate of successful message delivery over a communication channel.

Security Management

- Security services: generating, distributing, storing of encryption keys for services
- Exception alarm generation, detection of problems
- Uniform access control to resources
- Backups, data security
- Security logging

Scope of Research

- Network Management softwares