CSC 402 – Internet Technology

Recap

- Security and System Administration Issues, Firewalls and Content Filtering

Benefits and drawbacks of Intranets

- Main benefits
  - Information management & Web publishing.
  - Business operations and management.
  - Enhance internal communication & collaboration.
  - Workforce productivity.
- Drawbacks
  - Information overload may decrease productivity
  - Cost - setting up intranet incurs direct (Hardware and Software) & indirect costs.
  - Security - policy & guidelines to be enacted in place.
  - Training to use the intranet & intranet applications.

Benefits Intranets

- Cost effectiveness
  - Intranets are significantly cheaper to operate (running cost, training, and support) than an alternative, such as a proprietary network, and can contribute to lower overall costs.
- Easy publication and sharing of information
  - Used to develop and post documents to appropriate locations for ease of access.
  - Maintaining the information is also much easier because it resides in a single location or a small set of defined locations.
- Scalable applications
  - Adding users is simple. New users just need an Internet connection, a browser, and permission to access your intranet to start interacting with your network.
  - They start out with a few applications and add functionality as needs and opportunities are discovered.
- Easy monitoring of use
  - Easier to determine what content is being accessed, by whom, and through what pathways. This can be beneficial in learning what information is being shared or not shared through the organization and in enhancing the design of services.

Drawbacks of Intranet

- Content maintenance
  - Content comes from inside organization, not Internet.
  - Maintaining content is costly and requires dedication of resources to ensure the accuracy, reliability, and timeliness of the information.
  - Maintaining content is waning as the novelty of the medium wears off, and new policies to enforce content quality are necessary.
- Security violations
  - Someone with access to the network, it is easier for them to do damage or steal information.
- Connection issues
  - Built-in data replication is not available in an intranet or extranet. As a result, all users must be connected to the intranet in order to access it.
  - Offline support can be important for mobile users who do not always have telecommunications access to connect to the intranet.
- Evolution of standards and technology
  - Programming standards for the web are immature and subject to change.
    - Consider web pages. Several years ago, frames were the latest and greatest in web development. They allowed content to change in one part of a window while remaining constant in another.
    - Now, they are too clumsy and have been replaced by more sophisticated tools, such as embedded menus.

Protocols, Structure and Scope of Networks

- Protocols
  - Intranet as an application of Internet technology to private networks.
  - Use of TCP/IP Protocol suite – HTTP, SMTP, FTP.
  - Remember “Protocols” vs “Standards”.
- Scope of Networks
  - Internet - accessible to all connected to the Internet.
  - Intranet – available within one or several organizations.
  - LAN technology – Ethernet, VLAN, WLAN.
  - WAN technology - Frame relay, PPP, ATM, X.25, xDSL, ISDN, VPN, SONET.

Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources

- Network Resource:
  - Computing, storage, database, files etc.
- Performance
  - Set of levels for capacity, delay, & RMA in a network.
    - RMA: Reliability, Maintainability, and Availability.
    - Improve the overall performance of the network w.r.t. response time, throughput, latency, bandwidth availability etc.
    - Support a particular user groups or applications groups.
    - Control resource allocation for accounting and management purposes.
  - Controlling traffic inputs to the network (admission & rate controls).
  - Adjusting traffic or capacity benchmarking.
  - Prioritizing, scheduling & conditioning traffic flows.
  - Implementing a feedback loop to users, applications, devices & mgmt. to modify controls.
- Performance monitoring
  - Network latency - ping ,trace route utility
- Research on Performance Monitoring Tools:
  - Inbuilt in various programming language package.
  - Also, independent 3rd party tool.

Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources

- Network Monitoring System - monitors a network for slow or failing components & that notifies administrator (via email, SMS or other alarms) in case of outages
- Nagios
  - Open source computer system monitor, network monitoring, & infrastructure monitoring software application.
  - Offers complete monitoring and alerting for servers, switches, applications, and services.
  - Considered the defacto industry standard in IT infrastructure monitoring.
  - Monitor network services – SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, and SSH.
  - Monitor host resources (processor load, disk usage, system logs, etc.) on a majority of network OS.
- Alternatives
  - Icinga
  - Icinga2
  - Pingdom, etc.

Intranet Implementation Guidelines

- Establish an Intranet Business Model and define Intranet ownership.
- Create Publishing Policies.
- Select a Security Model.
  - Against unauthorized access and snooping.
  - Even if login is successful, the user activity should be tracked.
- Select a Content Management System (CMS).
  - Joomla and Drupal.
  - To keep content up to date with the help of custom built front end.
  - To keep track of usage and analysis.
- Select a Database Integration Standard.
  - Open & flexible tool or integration standards that have the capability to connect to legacy systems if needed.
- Select Intranet Traffic Analysis Tools.
- Estimate Server and Bandwidth.

Tunneling Protocols: VPN

- Conventional private networks assist connectivity among various network entities through a set of links.
- These links are leased from public telecommunication carriers as well as privately installed wiring.
- The traffic on these private networks belongs only to the company deploying the network.
- Shortcomings of conventional private networks:
  - Conventional private networks are not cheap to plan and install.
  - The planning periods are long.
  - Dedicated links take time to install.

Tunneling Protocols: VPN

- Virtual Private Networks (VPNs) have emerged as an effective and popular means for providing secure communications between geographically distributed network entities.
- VPN – a private network connecting different sites by using public telecommunication infrastructure (e.g., the Internet) with encryption and tunneling protocol procedures for secured and reliable connectivity.
  - Thus, a VPN can be viewed as an improved WAN, connecting multiple LANs.
- “Using the Internet as a medium” presents concerns for network security.
  - An intruder can intercept the traffic that passes between a remote office and main office over these insecure Internet connections.
- Clearly, efficient security protocols should be used for VPNs.

Tunneling Protocols: VPN

- In general, a VPN can be defined as a network that provides a secure link ("tunnel") between 2 private networks.
- **Virtual** – because data are tunneled through a public network, such as the Internet, emulating a logical point-to-point connection.
- **Private** – because the tunnel provides data privacy (aka confidentiality), integrity, authentication, and access control.
- Benefits of VPNs:
  - Cost savings – the biggest benefit
  - Scalability – VPNs can easily extend the geographic reach of the company's networks since new connections can be added easily.
  - Flexibility – VPNs can be designed to provide varying levels of security and different connection speeds.

Tunneling Protocols: VPN

- The terms used in the context of VPNs:
  - **VPN client** – a device that initiates a VPN tunnel with a VPN server.
  - **VPN server** – a device that accepts a VPN tunnel request from a VPN client.
  - **VPN tunnel** – a secure logical connection between 2 private networks across a public network.
  - **Tunnel endpoints** – the 2 devices that are at the start and culminating points of a VPN tunnel.
    - E.g., routers, firewalls, servers, workstations, or mobile devices.
    - VPN clients and servers can themselves be tunnel endpoints.
  - **Tunneling protocol** – a communications protocol that enables setting up of a VPN tunnel and typically provides secure communication.

Tunneling Protocols: VPN

- **P (Provider) network** – a provider backbone network, typically a public infrastructure network like the Internet.
- **C (Customer) network** – a private network that is owned and managed by a customer.
- **P devices** – devices that switch and forward packets in the P network.
- **C devices** – devices that switch and forward packets in the C network.
- **PE (Provider Edge) devices** – P devices at the edge of the P network that connect to devices in the C network.
- **CE (Customer Edge) devices** – C devices at the edge of the C network that connect to devices in the P network.
- **VPN concentrator** – a device (typically) at the server side to which multiple VPN tunnels are terminated.

Tunneling Protocols: VPN Taxonomy

- Traditionally, VPNs have been classified into:
  - Remote access VPNs
  - Intranet VPNs
  - Extranet VPNs
- Remote access VPNs – connect individual remote users to corporate networks.
  - I.e., enable remote users to work as if they are at their workstations in their offices.
  - Installing remote access VPNs can result in considerable cost savings, eliminating the need for organizations to manage large modem pools, and substituting the need for toll-calls to these modems by calls to local ISPs.
  - By using a high-speed access infrastructure, some of the performance limitations typically associated with remote access can be alleviated.

Tunneling Protocols: VPN Taxonomy

- Intranet VPNs – connect a number of LANs (Intranets) located in multiple geographic areas over the shared network infrastructure.
  - Typically, it is used to connect multiple geographic locations of a single company.
  - Intranet access is limited to these LANs, and connections are authenticated.
  - Because an Intranet VPN is formed by linking 2 or more trusted sites that are certainly protected by firewalls, most security fears are eased.
- Extranet VPNs – limited access of corporate resources is given to business partners, such as customers or suppliers, enabling them to access shared information.
  - These users are allowed to access specific areas of the Intranet that are referred to as the De-Militarized Zone (DMZ).
  - The firewall and access management facilities are responsible for differentiating between the company's employees and other users as well as each group's privileges.
  - The requests for connection by the company's employees must be directed to the company Intranet, while these by a third party must be directed to the DMZ.
- Try to get some information on PE-based and CE-based VPNs.

Tunneling Protocols: VPN

- In order to implement any VPNs, a number of hardware devices is needed:
- Firewalls
  - A firewall is a set of related programs, located at a network gateway server, which protects the resources of a private network from users from other networks.
  - A firewall is often installed away from the remainder of the network in order to avoid incoming requests from getting directly to the private network resources.
- Routers
  - Adding a VPN functionality to existing routers may degrade the performance, specifically at network critical points.
  - Particularly, MPLS VPNs tackle this problem by making only the perimeter routers VPN-aware.
  - Thus, the core routers do not need to maintain the multiple routing tables which introduce a huge overhead on PE routers.

Tunneling Protocols: VPN

- Switches
  - A number of switches provide facilities for improved separation of traffic by permitting a physical network to be divided into a number of Virtual LANs (V-LANs).
- Tunnel servers
  - This can be offered by a VPN router or a firewall.
  - If this additional responsibility is assigned to an already existing network's component, then a performance degrade may result.
- Cryptocards
  - All effective cryptographic algorithms are computationally costly and can limit the effective bandwidth.
  - This dedicated hardware is offered as an extension card for workstations that could be integrated as part of the network interface card or as a separate card.

Tunneling Protocols: VPN Security Protocols

- Confidentiality (aka Privacy) – to prevent eavesdropping of the tunnel data traveling through the Internet.
  - Cryptographic algorithms.
- Integrity – to ensure that the received tunnel data are identical to the sent data.
  - One-way hash functions.
- Authentication – to ensure that any request for tunnel creation comes from a legitimate client and to ensure that the data have originated from an authorized sender and have not been modified in the tunnel.
  - Digital signatures.
- Certification – to establish the identity of the tunnel peer entities before keys are exchanged.
  - Digital certificates issued by a trusted third party.
- Access control – tunnel endpoints must limit access to legitimate users.
  - Firewalls or other filtering mechanisms at the tunnel endpoints
- Key management – to have an efficient mechanism by which the keys are exchanged during a session.

Tunneling Protocols: VPN Security Protocols

- Security Protocols:
  - PPTP
  - L2F
  - L2TP
  - IPSec
  - SSL/TLS
  - SSH
- If interested:
  - Is MIPv6 (Mobile IPv6) doing the same as VPN would have done?
  - Sort of, if the reverse tunneling is enabled then it is exactly the same. If the route optimization is used, then it is more like DNS lookup.