CMPSCI 677 Operating Systems **Spring 2014**

Lecture 24: April 25

Lecturer: Prashant Shenoy *Scribe: Dong Chen*

24.1 Security Design

24.1.1 Focus of control

Three approaches for protection against security threats: protection against invalid operations, protection against unauthorized invocations and protection against unauthorized users.

24.1.2 Authentication protocol

This is a process where the user can prove the system its identity and obtain access to the system. Various authentication protocols are as follows Ap 1.0 Send message directly. Problem: intruder Trudy can also send such a message. Ap 2.0 Authenticate source IP address is from Alices machine. Problem: IP Spoofing (send IP packets with a false address) Ap 3.0 Use encryption: a secret password. Alice to Bob: I am Alice, here is my password. The problem: Trudy can intercept Alices password by sniffing packets. Ap 3.1: Use a symmetric key known to Alice and Bob. Problem: Trudy can intercept Alices message and masquerade as Alice at a later time. The same password is used for all sessions. Ap 4.0 Uses nonces: once-in-a-lifetime-only number for each session. Ap 5.0 Use public keys for authentication. Bob needs Alices public key for authentication. Problem: Trudy can impersonate as Alice to Bob.

24.1.3 Authentication using key distribution center

One of the problems with using a shared secret key for authentication is scalability. If a distributed system contains N hosts, and each host is required to share a secret key with each of the other N - 1 hosts, the system as a whole needs to manage N (N - 1) /2 keys. An alternative is to use a centralized approach by means of a Key Distribution Center (KDC). This KDC shares a secret key with each of the hosts, but no pair of hosts is required to have a shared secret key as well. In other words, using a KDC requires that we manage N keys. If Alice wants to set up a secure channel with Bob, she can do so with the help of a (trusted) KDC. The KDC hands out a key to both Alice and Bob that they can use for communication. Alice first sends a message to the KDC, telling it that she wants to talk to Bob. The KDC returns a message containing a shared secret key KA,B that she can use. The message is encrypted with the secret key KA,KDC that Alice shares with the KDC. In addition, the KDC sends KA,B also to Bob, but now encrypted with the secret key KB ,KDC it shares with Bob.

Digital signatures using Public Keys Its a way of signing the message sent; they are supposed to be equivalent to physical signatures made to a document. Its a digital form of a signature. Sender cannot repudiate message never sent and same way the receiver can never fake a received message. Eg: suppose if A wants B to Sign a message M. B sends DB(M) to A , A computes if EB (DB(M)) == M , Then B has signed M.

Message digests They are essentially hash functions; it takes an arbitrary length of strings but outputs a fixed length hash and this hash function is signed using methods specified earlier. Since the hash is significantly smaller in size and hence not computationally intensive to make Digital Signatures on this, this seems to be more efficient and better approach than hashing the entire message to authenticate. When the receiver, receives the (message + signed hash), the received messaged can be hashed and verify the signed hash.

Properties of hash function (a) Given a digest x, it is infeasible to find a message y such that H(y) = x, (b) It is infeasible to find any two messages x and y such that H(x) = H(y)

MD5: Takes arbitrary message and converts into 128 bits constant length key. But MD5 is not secure anymore. SHA hash functions (secure hash algorithm): SHA-1 : 160-bit function that resembles MD5, SHA-2: family of two hash functions (SHA-256 and SHA-512), Developed by NIST and NSA

24.2 Access Control

Access control gives us the capacity to restrict access to the system. Access control list - where for every resource there is list of which user can read, write, and exit. Capabilities- Every user is basically given a list of capability, when it does an operation the user presents the list of capabilities and gains access.

24.2.1 Security in enterprises

Multi-layered approach to security in modern enterprises, Security functionality spread across multiple entities. Firewall guards what network packet enters or leaves the network, Deep packet inspectionC In this the process looks inside the packet, not only source and destination address like the Firewall. They scan the packet for virus, malware etc. VLAN- virtual network, where the machines are on virtual Ethernet each machine can be restricted access to other machines on network. Network radius servers, Securing Wi-Fi, VPNs, Securing services using SSL, certificates, Kerberos etc.

24.2.2 Security in Internet services

Website has to run over SSL + authentication (to ensure user actually log into the system before usage) by means of password, username + captchas are used to limit access to humans and deny access to computer programs trying to bring down the website. Challenge-response authentication more secured than password authentication. Two factor authentication Gmail uses password and mobile to authenticate the user. One time passwords are used by Microsoft, where once in a lifetime challenge message is sent to a mobile device, increases the security. E.g.: Hotmail.

24.2.3 Firewall

A firewall disconnects any part of a distributed system from the outside world. All outgoing, but especially all incoming packets are routed through a special computer and inspected before they are passed. Firewalls essentially come in two different flavors that are often combined. Packet-filtering gateway operates as a router and makes decisions as to whether or not to pass a network packet based on the source and destination address as contained in the packet's header. The other type of firewall is an application-level gateway, which inspects only the header of network packets, this type of firewall actually inspects the content of an incoming or outgoing message.

24.2.4 Secure Email

Requirements of a secure email service are as follows. Secrecy - only sender and receiver can see the mail and contents. Sender authentication C it has to be authenticated, it has to be proven that the sender is valid and authentic. Message integrity C has to make sure that, message does not get altered in transit. All this can be done using public key encryption, as follows.

Authentication and Integrity (with no secrecy) - Alice applies hash function H to M (H can be MD5) - Creates a digital signature DA(H(M)) - Send M, DA(H(M)) to Bob

Putting it all together - Compute H(M), DA(H(M)) - M= M, DA(H(M)) - Generate symmetric key K, compute K(M) - Encrypt K as EB(K) - Send K(M), EB(K)

24.2.5 Secure socket layer

Provides data encryption and authentication between web server and client. SSL lies above the transport layer. Useful for Internet Commerce, secure mail access (IMAP)

There are several features of SSL they are as follows SSL server authentication, Encrypted SSL session, SSL client authentication.

Following are the events that take place before setting up of an SSL connection.

Browser -¿ Server: Bs SSL version and preferences S-¿B: Ss SSL version, preferences, and certificate- Certificate: servers RSA public key encrypted by CAs private key B: uses its list of CAs and public keys to decrypt Ss public key B-¿S: generate K, encrypt K with ES B-¿S: future messages will be encrypted, and K(m) S-¿B: future messages will be encrypted, and K(m) SSL session begins