Network Security Best Practices

Ed Crowley

Ch 11

Network Security

- Practice of protecting the usability, reliability, integrity, and safety of a network infrastructure and its data traveling in transit.

Assess and Audit the Network

- Network assessment is an objective review of an organization's network infrastructure in terms of:
  - current functionality
  - security capabilities.
- Once documented, stored as a baseline for future audits.
- With technologies that enable administrators to move virtual machines between hosts with no downtime and very little administrative effort, IT environments have become extremely volatile.
  - Side effect of that volatility is that the security posture of a guest on one host may not be retained when it has been migrated to a different host.

Leverage Established Industry Frameworks

- Frameworks have been established both to improve the quality of IT organizations:
  - Information Technology Infrastructure Library (ITIL)
  - Microsoft Operations Framework (MOF),
- and to ensure regulatory compliance, like:
  - payment card industry regulation (PCI/DSS)
  - the Sarbanes-Oxley Act (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA).
- Regulatory compliance is expensive not only do they need to build solutions according to those regulations, they must also demonstrate compliance to auditors.

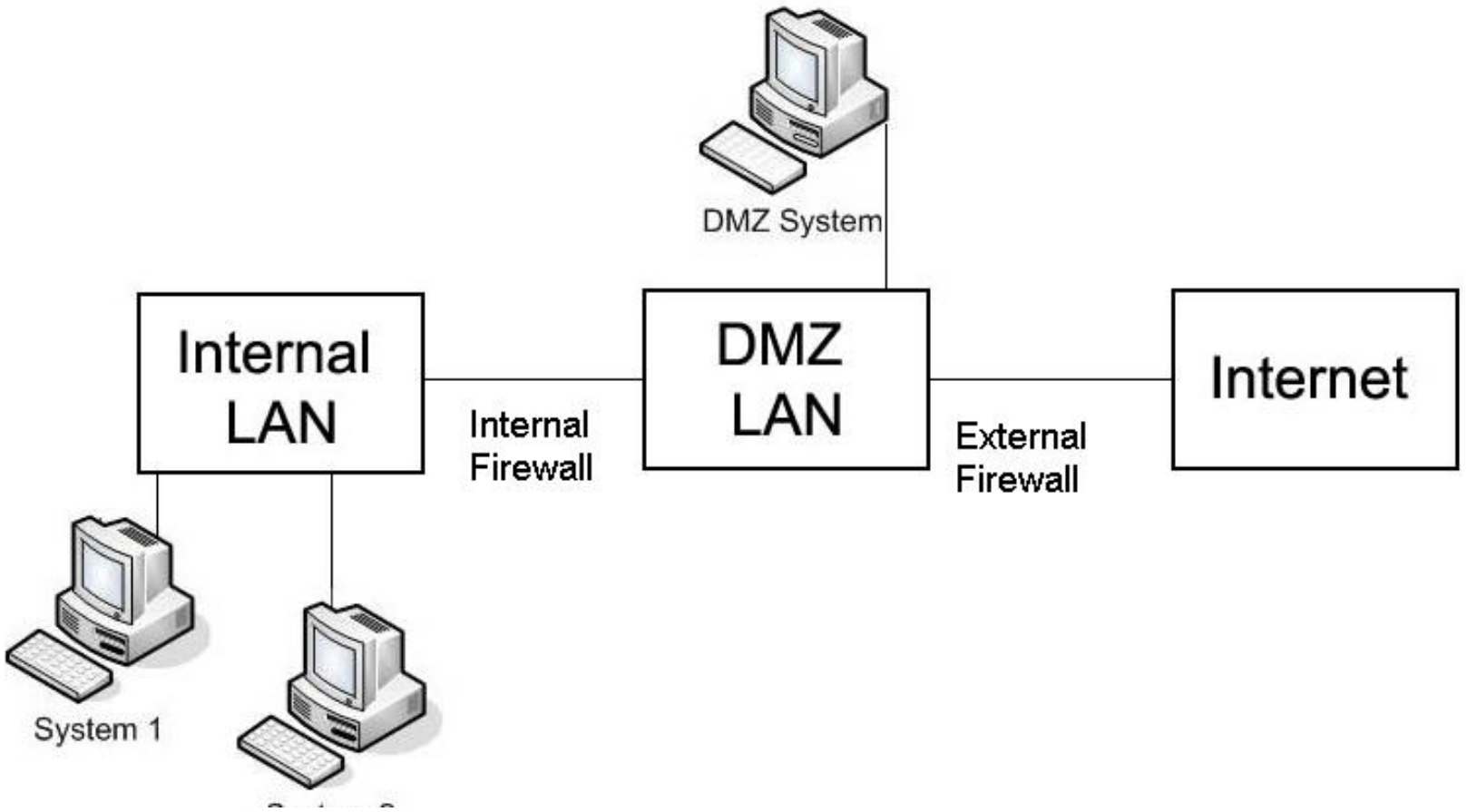
Layered Security

- To protect network resources from external threats, secure network design employs multiple layers.
- The most secure design possible blocks access to all network traffic between the Internet and the local area network (LAN), where protected resources reside.
- This secure design must be altered, however, to allow any services from those protected resources to access the Internet.

DMZ

- A DMZ is a separate network layered in between two separate networks that holds resources that need to be accessed by both.
- A DMZ enhances security through the concept of multiple layers, because if an intruder were to gain access to the DMZ, they would still not have access to the protected resources on the LAN.

DMZ


DMZ System
Internal LAN
Internal Firewall
DMZ LAN
External Firewall
Internet
System 1

DMZ

- Most common architectural design for setting up a DMZ is to place a hardware firewall between the external network and the DMZ, and to both control access and protect against attacks using that device.
- Firewalls use access lists.
- Access lists explicitly allow or deny network traffic to specific network addresses on specific network ports, and allow for very granular access.
- Access lists are a simple way to allow authorized traffic to network resources.

Intrusion Detection and Prevention

- In order to deter or actively prevent unauthorized access of internal network resources, there are several tools that can be implemented in addition to the ACLs.
- Intrusion detection systems can be layered on top of firewalls to detect malicious packets and send alerts to system administrators to take action.
- Intrusion prevention systems take security one step further, actively shutting down the malicious traffic without waiting for manual intervention from an administrator.

Attacks

- Routine attacks include:
- Distributed Denial of Service (DDoS) attack
  - Target a single system simultaneously from multiple compromised systems.
- Ping of Death (PoD) attacks
  - Send malformed ICMP packets with the intent of crashing systems.
- Ping Flood attacks
  - Similar to DDoS attacks in that they attempt to overwhelm a system with more traffic than it can handle.

Third Party Network Audit

- When assessing or auditing a network, it is best practice to utilize a third-party product or service provider.
  - Preferable to using internal resources, as they often have both preconceived biases and preexisting knowledge about the network and security configuration.
- A set of eyes from an outside source allows for a different (and in many cases, greater) set of skills to be utilized in the evaluation.
- May be a regulatory requirement.

Harden Computers

- The hardening of computer systems and networks involves reduces risk of attack from either internal or external sources.
- While the specific configuration steps for hardening vary from one system to another, the basic concepts involved are largely similar regardless of the technologies that are being hardened.

Harden Computers

Hardening concepts:

- Remove software and services not needed.
- Maintain firmware and patch levels.
- Control account access.
- Disable unnecessary network ports.
- Deploy antivirus/antimalware.
- Configure log files.
- Limit physical access.
- Scan for vulnerabilities.
- Deploy host-based firewall.

Penetration Testing

- Process of evaluating network security with a simulated attack on the network from both external and internal attackers.
- An active analysis by a testing firm identifying potential vulnerabilities.
- Tester acts like a potential attacker.
  - May involves exploitation of specific vulnerabilities.
- Testing firm might take the results from the test and combine them with an assessment that states the potential impacts to the organization and makes suggestions on how to reduce security risks.

Vulnerability Assessments

- A vulnerability assessment is the process used to identify and quantify any vulnerabilities in a network environment.
- Detailed evaluation of the network, indicating any weaknesses and providing appropriate mitigation procedures to help eliminate or reduce the level of the security risk.

Secure Storage Resources

- Data is the most valuable component of any cloud system.
- Because it is such a critical resource to the users of our cloud models, special care must be taken with its security to make sure it is always available and accurate for only the resources that have been authorized to access it.
- In addition to the network system's hardening steps listed previously, some additional steps need to be taken for storage security.

Data Classification

- Data classification is the practice of sorting data into discrete categories that help define the access levels and type of protection required for that set of data.
- These categories are then used to determine the disaster recovery mechanisms, cloud technologies required to store the data, and the placement of that data onto physically or logically separated storage resources.

Data Encryption

- Data encryption is an algorithmic scheme that secures data by scrambling into a code that is not readable by unauthorized resources.
- The authorized recipient of encrypted data uses a key that triggers the algorithm mechanism to decrypt the coded message, transforming back into its original readable version.
- Without that key, even if an unauthorized resource were to secure a copy of the data, they could not use it.

Granular Storage Resource Controls

- When using a storage area network (SAN), resources can be limited to which storage logical unit numbers (LUNs) are accessible by the utilization of a LUN mask either at the host bus adapter or at the switch level.
- SANs can also utilize zoning, which is a practice of limiting access to LUNs that are attached to the storage controller.
- Storage security is best implemented in layers, with data having to pass multiple checks before arriving at its intended target.

Protected Backups

- Backups are copies of live data that are maintained in case something happens that makes the live dataset inaccessible.
- Because it is a copy of valuable data, it needs to have the same protections afforded it that the live data employs.
- It should be encrypted, password protected, and kept physically locked away from unauthorized access.

Keep Employees and Tools Up to Date

- Rapid deployment is the ability to provision and release solutions with minimal management effort or service provider interaction.
- Has been enabled by new and better virtualization technologies that allow IT organizations to roll out systems faster than ever before.
  - One hazard of rapid deployment is the propensity to either ignore security or proceed with the idea that the organization will enable functionality for the system immediately, then circle back and improve the security once it is in place.
- Typically, however, the requests for new functionality continue to take precedence and security is rarely or inadequately revisited.

Monitoring and Managing

- Many networks were originally designed to utilize traditional network security devices that monitor traffic and devices on a physical network.
- If the intra-virtual-machine traffic that those tools are watching for never routes through a physical network, it cannot be monitored by that traditional tool set.
- The problem with limiting network traffic to guests within the host is that if the tools are not virtualization or cloud aware, they will not provide the proper information to make a diagnosis or even to suggest changes to the infrastructure.
- Therefore, it is critical that monitoring and management tool sets are updated as frequently as the technology that they are designed to control.

Data Security

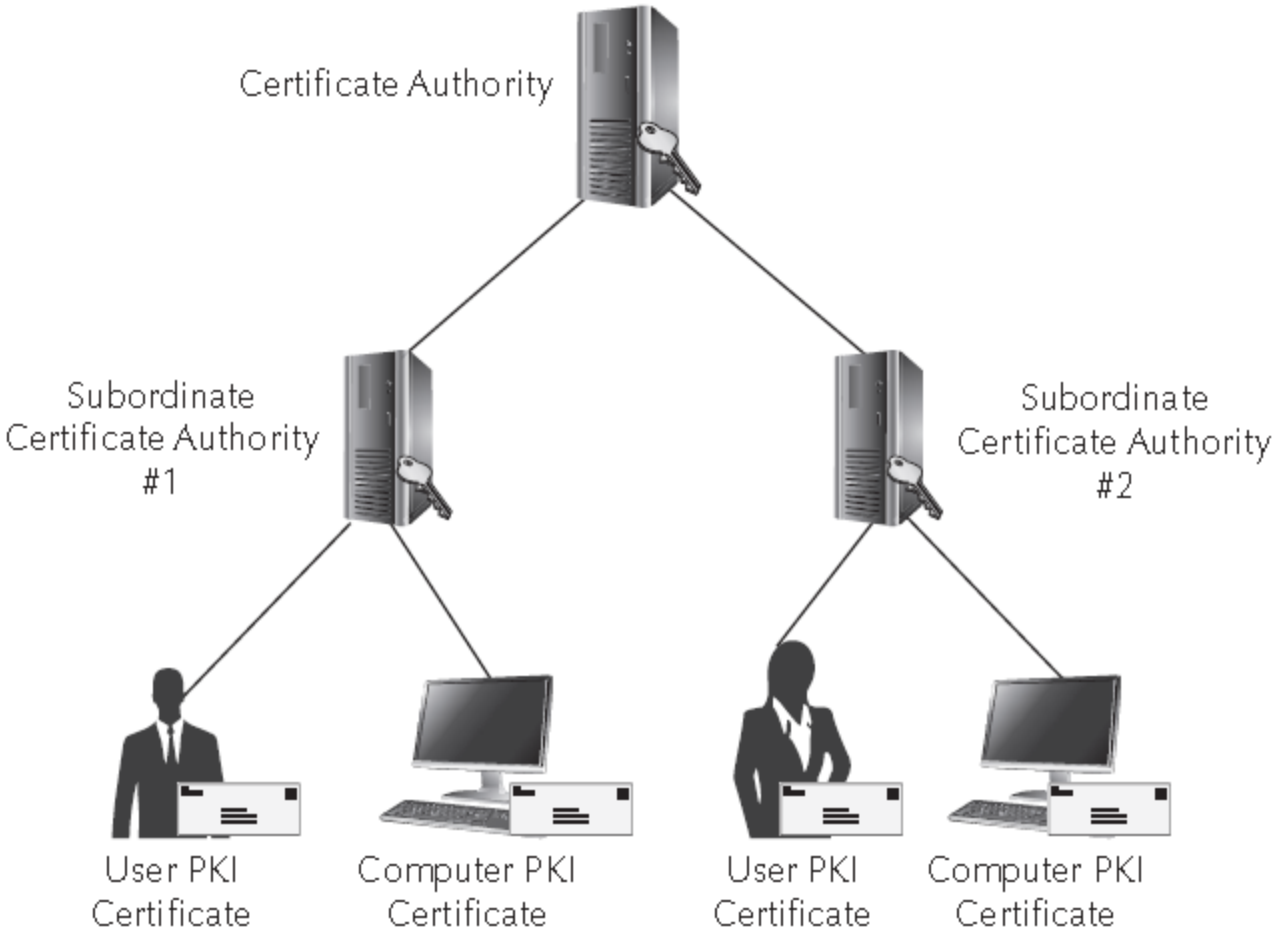
- In its simplest form, data security is accomplished by authenticating and authorizing both users and hosts.
- Authentication means that an entity can prove that it is what it claims to be…
- Authorization means that an entity has access to all of the resources it is supposed to have access to, and no access to the resources it is not supposed to have access to.

Confidentiality

- Confidentiality (encryption) ensures that only authorized parties can access data, whereas data integrity (digital signatures) ensures that data is tamper-free and comes from a trusted party.
- These control mechanisms can be used separately or together for the utmost in security, and this section will explore them in detail.

Public Key Infrastructure

- A hierarchy of trusted security certificates.



Certificates

- Certificates (akaX.509 certificates) are issued to users or computing devices.
- PKI certificates can be used to encrypt and decrypt data, as well as to digitally sign and verify the integrity of data.
  - Each certificate contains a unique public key.
- When the certificate is issued, it has an expiration date; certificates must be renewed before the expiration date.
- The certificate authority (CA) exists at the top of the PKI hierarchy, and it can issue, revoke, and renew all security certificates.
- Under it reside either user and device certificates or subordinate certificate authorities.

Subordinate CAs

- Can also issue, revoke, and renew certificates.
- A large enterprise, for example, Acme, might have a CA named Acme-CA. For the western region,
  - Acme might create a subordinate CA named West and the same for East and Central.
  - Allows IT security personnel in each of the three regions to control their own user and device PKI certificates.
- Instead of an organization creating their own PKI, they may want to consider acquiring PKI certificates from a trusted third party such as VeriSign or Entrust.
- Modern operating systems have a list of trusted certificate authorities, and if an organization uses their own PKI, they have to ensure that all of their devices trust their CA.

Terms

Plaintext

- Before data is encrypted, it is called plaintext. When an unencrypted e-mail message (i.e., an e-mail in plaintext form) is transmitted across a network, it is possible for a third party to intercept that message in its entirety.

Obfuscation

- Obfuscation is a practice of using some defined pattern to mask sensitive data.
- Obfuscation is more secure than plaintext, but can be reverse engineered if a malicious entity were willing to spend the time to decode it.

Cipher Text

- Ciphers are mathematical algorithms used to encrypt data. Applying an encryption algorithm (cipher) against plaintext results in what is called cipher text; it is the encrypted version of the originating plaintext.

Symmetric Encryption

- Encrypting data requires a passphrase or key.
- Symmetric encryption, also called private key encryption, uses a single key that encrypts and decrypts data.
  - Think of it as locking and unlocking a door using the same key.
- The key must be kept safe since anybody with it in their possession can unlock the door.
- Symmetric encryption is used to encrypt files, to secure some VPN solutions, and to encrypt Wi-Fi networks, just to name a few examples.

Single Key Crypto

- Consider a situation where a user, Stacey, encrypts a file on a hard disk:

1. Stacey flags the file to be encrypted.
2. The file encryption software uses a configured symmetric key (or passphrase) to encrypt the file contents.
3. The key might be stored in a file or on a smart-card, or the user might simply be prompted for the passphrase at the time.

Key Management Problem

- This same symmetric key (or passphrase) is used when the file is decrypted.
- Encrypting files on a single computer is easy with symmetric encryption, but when other parties that need the symmetric key are involved (e.g., when connecting to a VPN using symmetric encryption), it becomes problematic: How do we securely get the symmetric key to all parties?
- We could transmit the key to the other parties via e-mail or text message, but we would already have to have a way to encrypt this transmission in the first place.

Asymmetric Encryption

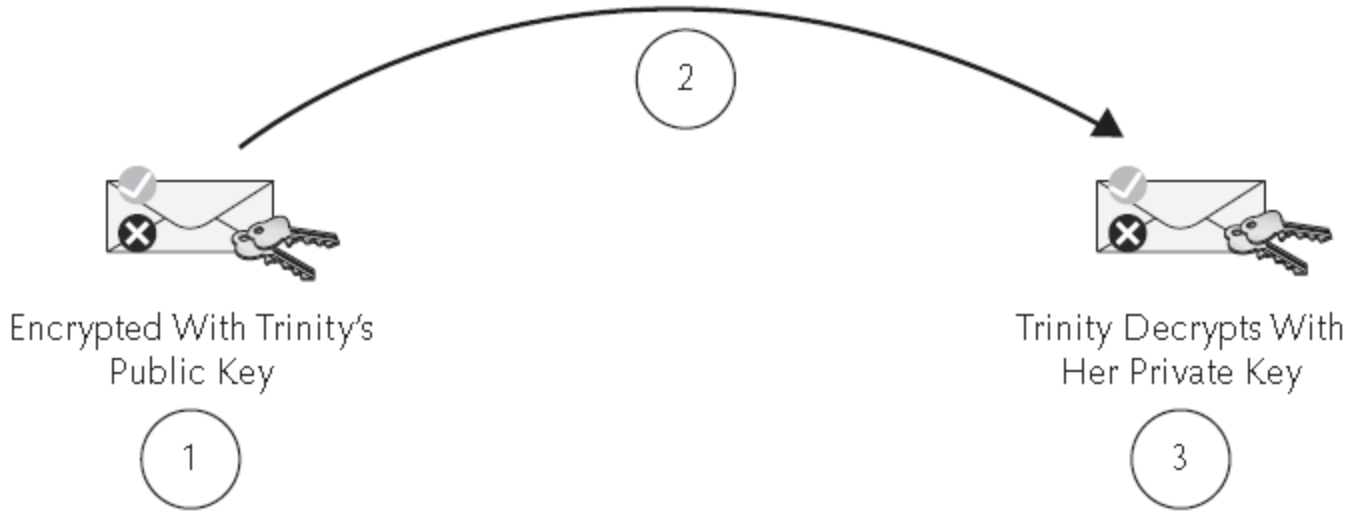
- Asymmetric encryption uses two different, but related, keys to secure data: a public key and a private key.
- Public key stored in a PKI certificate (which itself can be stored as a file), in a user account database, or on a smartcard.
- Using two mathematically related keys is what PKI is all about:
- a hierarchy of trusted certificates each with their own unique public and private key pairs.

Key Pair

- The public key can be freely shared, but the private key must be accessible only by the certificate owner. Both the public and private keys can be exported to a certificate file or just the public key by itself.
- Keys are exported to exchange with others for secure communications or to use as a backup. If the private key is stored in a certificate file, the file must be password protected.

Key Pair

- The recipient's public key is required to encrypt transmissions to them.
- Bear in mind that the recipient could be a user or a computer. The recipient then uses their mathematically related private key to decrypt the message.



Process

- Consider an example, shown in Figure 11-2, where user Roman sends user Trinity an encrypted e-mail message using a PKI, or asymmetric encryption:

1. Roman flags an e-mail message for encryption. His mail software needs Trinity's public key. PKI encryption uses the recipient's public key to encrypt. If Roman cannot get Trinity's public key, he cannot encrypt a message to her.
2. Roman's mail software encrypts and sends the message. Anybody intercepting the mail message will be unable to decipher the message content.
3. Trinity opens the mail message using her mail program. Because the message is encrypted with her public key, only her mathematically related private key can decrypt the message.

Scales Well

- PKI scales well.
- There is no need to find a safe way to distribute secret keys because only the public keys need be accessible by others, and public keys do not have to be kept secret.

Digital Signatures

- A PKI allows us to trust the integrity of data by way of digital signatures.
- When data is digitally signed, a mathematical hashing function is applied against the data in the message, which results in what is called a message digest, or hash.
- The PKI private key of the signer is then used to encrypt the hash: this is the digital signature.
- Notice that the message content has not been secured; for that encryption is required.
- Other parties needing to trust the digitally signed data use the mathematically related public key of the signer to validate the hash.
- Remember that public keys can be freely distributed to anyone without compromising security.

Digital Signatures

- As an example of the digital signature at work, consider user Ana, who is sending user Zoey a high-priority e-mail message that Zoey must trust really did come from Ana:

1. Ana creates the mail message and flags it to be digitally signed.
2. Ana's mail program uses her PKI private key to encrypt the generated message hash.
3. The mail message is sent to Zoey, but it is not encrypted in this example, only signed.
4. Zoey's mail program verifies Ana's digital signature by using Ana's mathemat-ically related public key; if Zoey does not have Ana's public key, she cannot verify Ana's digital signatures.

Digital Message

- Using a public key to verify a digital signature is valid because only the related private key could have created that unique signature, so the message had to have come from that party.
- This is referred to as nonrepudiation.
- If the message is tampered with along the way, the signature is invalidated.
- Again, unlike symmetric encryption, there is no need to safely transmit secret keys; public keys are designed to be publicly available.
- For the utmost in security, data can be encrypted and digitally signed, whether it is transmitted data or data at rest (stored).

Ciphers

- Recall that plaintext fed to an encryption algorithm results in cipher text. "Cipher" is synonymous with "encryption algorithm," whether the algorithm is symmetric (same key) or asymmetric (different keys).
- There are two categories of symmetric ciphers: block ciphers and stream ciphers.
- Table 11-1 lists some of the more common ones.

Common Ciphers

TABLE 11-1 Common Block and Stream Ciphers

Cipher Name	Cipher Type	Cipher Strength (in bits)	Usage
Advanced Encryption Standard (AES)	Symmetric, block	Up to 256	Replaced DES in 2001 as the U.S. federal standard
Digital Encryption Standard (DES, 3DES)	Symmetric, block	56 for DES, 168 for 3DES	U.S. federal standard until 2001
Digital Signature Algorithm (DSA)	Asymmetric, block	Up to 2048	U.S. federal standard for digital signatures
Rivest Cipher (RC4)	Symmetric, stream	128	Byte-oriented stream operation
Rivest Cipher (RC5)	Symmetric, block	Up to 2040	A simple and fast algorithm
Rivest, Shamir, Adleman (RSA)	Asymmetric, stream	Up to 4096	Some hardware and software may not support up to 4096 bits

Block Ciphers

- Designed to encrypt chunks or blocks of data, block ciphers convert plaintext to cipher text in bulk as opposed to one data bit at a time, either using a fixed secret key or by generating keys from each encrypted block.
  - A 128-bit block cipher produces a 128-bit block of cipher text.
- This type of cipher is best applied to fixed-length segments of data, such as fixed-length network packets or files stored on a disk.

Stream Ciphers

- Unlike block ciphers, stream ciphers convert plaintext bits into cipher text and are considered much faster than block ciphers.
- Stream ciphers are best suited where there is an unknown variable amount of data to be encrypted, such as variable-length network transmissions.

Encryption Protocols

- There are many methods that can be used to secure and verify the authenticity of data.
- These methods are called encryption protocols, and each is designed for specific purposes, such as encryption for confidentiality and digital signatures for data authenticity and verification (also known as nonrepudiation).

IPSec

- Internet protocol security (IPSec) secures IP traffic using encryption and/or digital signatures. PKI certificates or symmetric keys can be used to implement this type of security.
- What makes IPSec interesting is that it is not application specific; so if IPSec secures the communication between hosts, it can encrypt and/or sign network traffic regardless of the application generating the traffic.

SSL/TLS

- Unlike IPSec, secure sockets layer (SSL) and transport layer security (TLS) are used to secure the communication of specifically configured applications.
- Like IPSec, encryption and authentication (signatures) are used to accomplish this level of security. TLS is SSL's successor, although the improvements are minor.
- Most computer people associate SSL with secured web servers, but SSL can be applied to any network software that supports it, such as simple mail transfer protocol (SMTP) mail servers and lightweight directory access protocol (LDAP) directory servers.
- SSL and TLS rely on PKI certificates to obtain the keys required for encryption, decryption, and authentication.

Access Control Methods

- After successful authentication occurs, authorizing the use of network resources is achieved using various access control methods.

TABLE 11-2 Comparison of Access Control Methods

Role-Based Access Control (RBAC)	Mandatory Access Control (MAC)	Discretionary Access Control (DAC)
Permissions are granted to groups or roles	Operating system or application determines who has access to a resource	Permissions are granted to users
Suited for larger organizations	Resources are labeled for granular control	Suited for smaller organizations
Users are added to groups or roles to gain access to resources	User attributes can determine resource access	

Role-Based Access Controls

- Easier to manage permissions to resources by using groups, or roles.
  - Premise of role-based access control (RBAC).
- A group or role has one or more members, and that group or role is assigned permissions to a resource.
- Any user placed into that group or role inherits its permissions; this is known as implicit inheritance.
- Sometimes the groups or roles in RBAC are defined at the operating system level, as in the case of a Microsoft Windows Active Directory group, and other times the group or role is defined within an application, as in the case of Microsoft SharePoint Server roles.

Mandatory Access Controls

- The word mandatory is used to describe this access control model because permissions to resources are controlled, or mandated, by the operating system (OS) or application, which looks at the requesting party and their attributes to determine whether or not access should be granted.
- These decisions are based on configured policies that are enforced by the OS or app.
- With mandatory access control (MAC), data is labeled, or classified, in such a way that only those parties with certain attributes can access it.
- For example, perhaps only full-time employees can access a specific portion of an Intranet web portal. Or perhaps only human resources employees can access files classified as confidential.

Discretionary Access Controls

- With the discretionary access control (DAC) model, the power to grant or deny user permissions to resources lies not with the OS or an app but rather with the data owner.
- Protected resources might be files on a file server or items in a specific web application.
- There are no security labels or classifications with DAC; instead, each protected resource has an access control list (ACL) that determines access.
- For example, we might add user RayLee with read and write permissions to the ACL of a specific folder on a file server so that she can access that data.

Multifactor Authentication

- Authentication means proving who (or what) you are.
- Done with the standard username and password combination or with a variety of other methods.

Three authentication categories:

1. Something you know
   - Knowing your username and password is by far the most common.
2. Something you have
   - Most of us have used a debit or credit card to make a purchase. We must physically have the card in our possession. For VPN authentication, posses-sion of a hardware token with a changing numeric code synced with the VPN server is common.
3. Something you are.
   1. Biometric

Biometrics

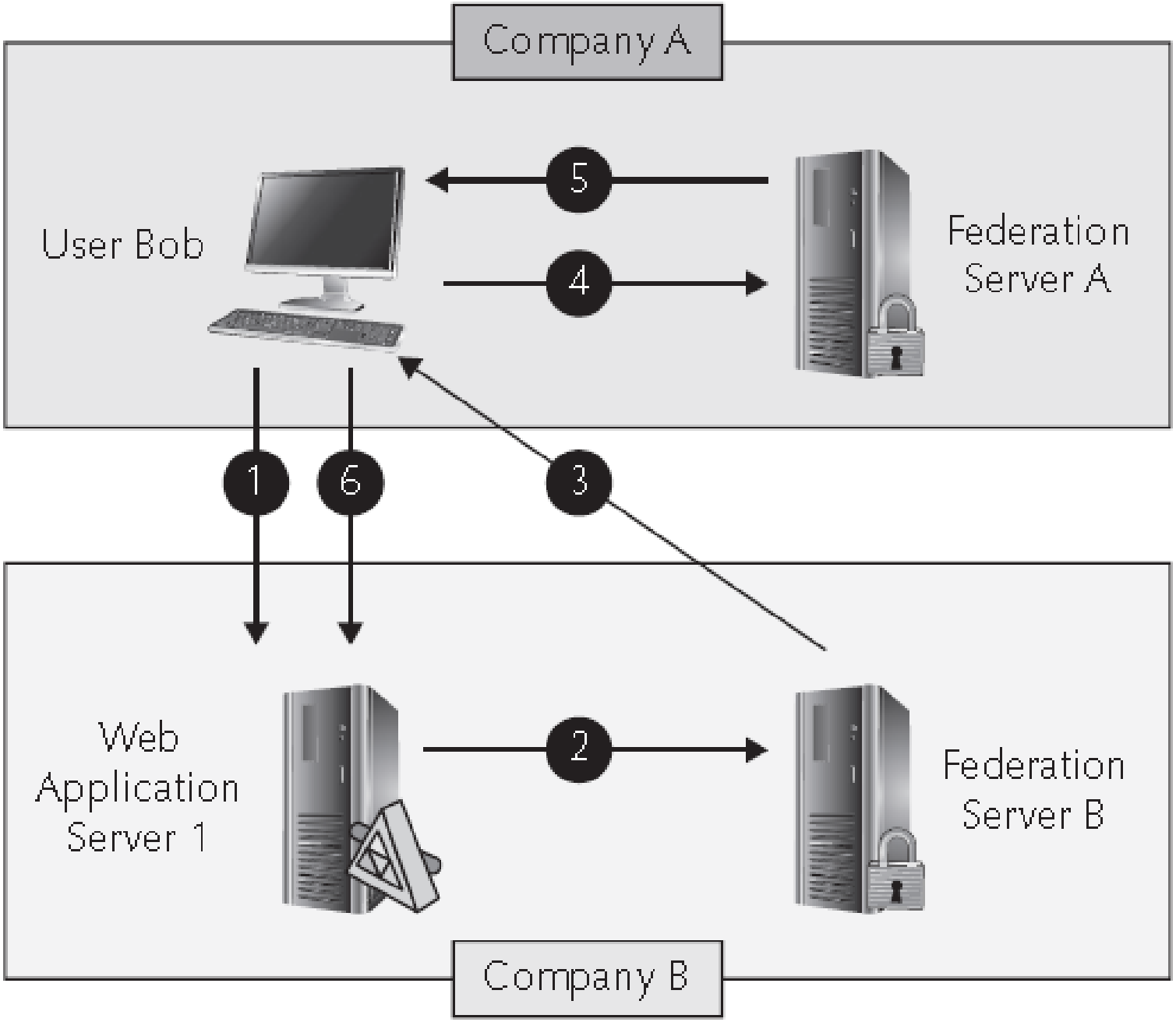
- Fingerprints, voice, facial structure, the capillary pattern in your retinas—these are unique to you.
  - Some methods are more secure than others.
- Some environments use a combination of the three authentication mechanisms; known as multifactor authentication.
- Possessing a debit card, along with knowledge of the PIN, comprises multifactor authentication.
- Combining these authentication methods is considered much more secure than single-factor authentication.

Single Sign-On

- SSO can take operating system, VPN, or web browser authentication credentials and present them to the relying party transparently so the user doesn't even know it is happening.
- Modern Windows operating systems use the credential vault to store varying types of credentials to facilitate SSO.
- Enterprise SSO solutions such as the open-source Shibboleth tool or Microsoft Active Directory Federation Services (ADFS) let IT personnel implement SSO on a large scale.
- The problem with SSO is that different software and websites may use different authentication mechanisms.
- Makes implementing SSO in a large environment difficult.

Federation

- Federation uses SSO to authorize users or devices to potentially many very different protected network resources, such as file servers, websites, and database applications.
  - Protected resources could exist within a single organization or between multiple organizations.
- For business-to-business (B2B) relationships, such as between a cloud customer and a cloud provider, federation allows the cloud customer to retain their own on-premises user accounts and passwords that can be used to access cloud services from the provider.
  - This way the user does not have to remember a username and password for the cloud services as well as for the local network.
- Federation also allows cloud providers to rent, on demand, computing resources from other cloud providers to service their clients' needs.


Company A
User Bob
5
4
Federation
Server A
1
6
3
Web
Application
Server 1
2
Federation
Server B
Company B

Federation

Typical B2B federation scenario (previous slide):

1. User Bob in company A attempts to access an application on web application server 1 in company B.
2. If Bob is not already authenticated, the web application server in company B redirects Bob to the federation server in company B for authentication.
3. Since Bob's user account does not exist in company B, the federation server in company B sends an authentication redirect to Bob.
4. Bob is redirected to the company A federation server and gets authenticated (this is where his user account exists).
5. The company A federation server returns a digitally signed authentication token to Bob.
6. Bob presents the authentication token to the application on web application server 1 and is authorized to use the application.

Questions???