**Glossary**

**A**

**AAA of security**
Authentication, authorization, and accounting. Together, they provide accountability.

**A (host) record**
A DNS record used to resolve host names to IP addresses.

**account lockout**
What results if an Account Lockout Policy exists and a user enters the incorrect password too many times. Users can’t log on utilizing an account that has been locked out.

**Account Lockout Policy**
A policy that sets the rules for account lockouts. It includes the Account Lockout Threshold, Account Lockout Duration, and Reset Account Lockout Counter values.

**Active Directory**
A database of objects (such as users, computers, and groups) for a Microsoft domain. Active Directory is stored on a server configured as a domain controller. Permissions protect objects within Active Directory.

**Active Directory Certificates Services (AD CS)**
A role on Windows Server 2008 used to create a certification authority (CA). The CA can be either an enterprise CA or a standalone CA.

**Advanced Encryption Standard (AES)**
A very strong and efficient symmetric algorithm. It was selected by the U.S. National Institute of Standards and Technology (NIST) as a standard and was adopted by the U.S. government.

**antivirus (AV) software**
Software designed to detect different types of malware. AV software can block, remove, or quarantine a wide variety of malware including viruses, worms, Trojan horses, and more.

**asymmetric encryption**
A protocol that converts plaintext data into ciphered text. Asymmetric encryption uses two keys (a public key and a private key) to encrypt and decrypt data. The public key is shared with others in a certificate. Asymmetric encryption is 1,000 (or more) times slower than symmetric encryption. It’s typically only used to privately share a secret key that is used in symmetric encryption.

**audit logs**
The files that store recorded event activity within a system. The primary log used to store auditable activity in Windows is the Security log.

**auditing**
Tracking activity within a system, and recording the activity in one or more event logs.
**authentication**

Proving your identity by providing credentials. The three factors of authentication are something you know (such as a password), something you have (such as a smart card), and something you are (proven through biometrics such as fingerprints).

**Automatic Updates**

A feature that allows clients to automatically discover, download, and install updates.

**availability**

Ensuring that systems and data are available when needed. Availability is enforced with redundant hardware, software, and infrastructure components. This is part of the security triad of availability, integrity, and confidentiality.

**BitLocker Drive Encryption**

A feature on Windows systems that can encrypt an entire hard drive. BitLocker Drive Encryption can be locked with a TPM v1.2, a USB key, or any combination of a TPM, a USB key, and a PIN.

**BitLocker To Go**

A feature on Windows 7 and Windows Server 2008 R2 systems that can encrypt USB flash drives. BitLocker To Go encrypts data with AES. Files can be read on systems without BitLocker using the BitLocker To Go Reader.

**botnet**

A network of computers taken over by malware and acting as zombies or clones. Clones regularly contact a server acting as a command-and-control center on the Internet that is controlled by an attacker.

**certificate**

A file used for a wide variety of security purposes such as authentication, encryption, and digital signatures. A certificate is also called a public key certificate because it holds the public key.

**certification authority (CA)**

An organization or a service that issues and manages certificates. A public CA is an organization hosting a server running a certificate services application. You can also run a private CA with Microsoft’s Active Directory Certificate Services (AD CS) by adding the AD CS role to a Windows Server 2008 server.

**confidentiality**

Ensuring that data isn’t disclosed to unauthorized parties. Confidentiality is enforced with access controls and encryption. This is part of the security triad of availability, integrity, and confidentiality.

**Default Domain Controllers Policy**

A Group Policy object created by default when a Microsoft domain is created. It’s
linked to the Domain Controllers OU. Only domain controllers should be in the Domain Controllers OU, so this policy only applies to domain controllers.

**Default Domain Policy**
A Group Policy object created by default when a Microsoft domain is created. It’s linked to the domain and applies to all users and computers in the domain.

**defense-in-depth**
A security strategy that employs multiple layers of security. If one layer fails, other layers still provide protection. A defense-in-depth strategy often deters or slows down an attack to provide extra time to detect it and respond to the attack.

**delegation**
Passing control of a task from one entity to another. For example, the Delegation of Control Wizard in Active Directory Users and Computers allows an administrator to grant permissions to others to perform specific tasks, such as resetting passwords for accounts.

**Delegation of Control Wizard**
A wizard in Active Directory Users and Computers. It’s used to delegate control for specific tasks (such as resetting a password) to users and groups. Control can be delegated for specific organizational units.

**denial of service (DoS)**
An attack on a system designed to prevent the system from providing a service.

**distributed denial of service (DDoS)**
A DoS attack launched from multiple sources. Many DDoS attacks are launched from botnets.

**DNS (Domain Name System)**
A service that runs on a server to provide name resolution and identify computers. A (host) records resolve host names to IP addresses, and PTR (pointer) records resolve IP addresses to host names. SPF (Sender Policy Framework) records help identify spoofed email to reduce spamming. DNS is required in a Microsoft domain.

**DNS cache poisoning**
Malicious practice of modifying the DNS data. DNS cache poisoning is the process of inserting bogus entries into a system’s DNS cache, redirecting a user to the attacker’s website instead of the intended website. This is one of the methods used for pharming.

**dynamic updates**
A process that allows clients to update DNS records without administrative intervention. Clients receive TCP/IP configuration from DHCP and then update DNS with their host name and IP address.

**Encrypting File System (EFS)**
A security feature built into NTFS that can encrypt folders and files. Folders and files stay encrypted if they’re copied or moved anywhere within an NTFS volume or to other NTFS volumes.
**encryption**

A process of converting plain-text data into ciphered text. The ciphered data can’t be read until it’s decrypted. Encryption normally includes an algorithm (a mathematical formula) that stays the same and one or more keys that are kept secret and changed often.

**enterprise CA**

A CA created with Active Directory Certificate Services (AD CS). An enterprise CA requires Active Directory Domain Services and supports autoenrollment to automatically issue certificates to clients within the domain.

**Event Viewer**

A tool used to view logs in Windows systems. For example, you can view the Security log, which records auditable events.

**F**

**FAT**

File Allocation Table (FAT) is a filesystem used for portable devices such as USB flash drives and digital cameras. It doesn’t support any type of permissions.

**G**

**Group Policy**

A Microsoft technology used to streamline administration of user and computer accounts. Settings are configured once and then deployed to either all the users and computers in a domain, or targeted users and computers. Security Group Policy settings include the Account Lockout Policy and Password Policy settings.

**H**

**hardware-based firewall**

A firewall hosted on a dedicated hardware appliance. Network-based firewalls are typically hardware-based. In comparison, Windows Server 2008 includes a software-based firewall, which is an additional piece of software running on the server.

**I**

**InPrivate Browsing**

A special browsing session that prevents any history of the session from being recorded. It isn’t used by default but is useful when you’re using a public computer.

**InPrivate Filtering**

A security feature that detects when web content is being used on multiple websites. It indicates that a third-party is using this information to track a user. InPrivate Filtering is off by default but can be enabled.

**integrity**

Ensuring that data isn’t modified. Integrity is enforced with security logging and with hashing methods. This is part of the security triad of availability, integrity, and confidentiality.

**Internet Explorer add-ons**

Browser plug-ins that extend the capability of IE. Add-ons can be enabled and disabled
through the Manage Add-ons page. All add-ons can be removed by resetting IE to the default settings.

**Internet Explorer security zones**

Four security zones (Internet, local intranet, trusted sites, and restricted sites) with varying default security settings. The trusted sites and restricted sites zones aren't used unless websites are added to the zones. The local intranet zone is used for UNC paths and websites with single-label names. All other websites use the Internet zone by default.

**K**

**Kerberos**

The primary authentication protocol used in Microsoft domains. It uses port 88 and requires all clients to have the same time (within five minutes of each other).

**keylogger**

A program that can capture all the keystrokes entered on a computer. Attackers sometimes use keyloggers to capture keystrokes, store them in a log file, and then email the file to the attacker periodically.

**L**

**LAND attack**

A local area network denial (LAND) attack spoofs the source address with the destination address. It causes a system to continuously reply to itself.

**least privilege**

A security strategy in which users, resources, and applications are only given the rights and permissions needed to perform required tasks, and no more.

**Local Security Policy**

A small part of the local Group Policy. Group Policy includes thousands of settings. Hundreds of these settings are related to security and are in the Security Settings node. You can access just the Security Settings of the local Group Policy via the Local Security Policy.

**M**

**MAC filter**

A filter on a wireless access point or wireless router that can block or allow access based on the media access control (MAC) address. MAC filters aren't effective as a security measure because it's easy to spoof MAC addresses.

**malware**

Malicious software such as viruses, worms, and Trojan horses. Up-to-date antivirus software detects and blocks malware.

**mantrap**

A physical security entry point that restricts access to a single person at a time. It's used to prevent piggybacking or tailgating.

**Microsoft Update**

A Microsoft service that provides updates for Windows operating systems and for Microsoft software such as Microsoft Office.
**multifactor authentication**

When two or more authentication factors are used. The three factors of authentication are something you know (such as a password), something you have (such as a smart card), and something you are (proven through biometrics, such as fingerprints).

**N**

**Network Access Protection (NAP)**

Part of the Network Policy and Access Services role. NAP can inspect clients based on administrator definitions of health and isolate unhealthy clients in restricted networks.

**Network Address Translation (NAT)**

A protocol that translates public IP addresses to private IP addresses and private back to public. NAT provides a layer of protection for the clients. Firewalls and routers can have NAT installed to translate IP addresses.

**nonrepudiation**

A process that ensures that an entity can’t believably deny taking an action. For example, a log entry indicating that a user took an action provides nonrepudiation. As long as the system has reliable accounting, the user can’t believably deny performing the recorded action.

**NTFS**

New Technology File System (NTFS) is a filesystem used by Microsoft. NTFS provides security benefits because you can assign permissions to files and folders.

**O**

**organizational unit (OU)**

A container within Active Directory Users and Computers. Objects (such as users, computers, and groups) are organized in OUs for easier administration.

**P**

**Patch Tuesday**

The second Tuesday of every month, when Microsoft releases security updates. Security updates that are released on other days are called out-of-band updates.

**Password Policy**

A policy configured with Group Policy to enforce secure password practices. A Password Policy can ensure passwords are strong, of sufficient length, not repeated, and changed often. A Password Policy starts as a written security policy and is then enforced through technology such as Group Policy’s Password Policy.

**password-reset disk**

A disk created in advance to allow a user to reset their password if the user has forgotten their password. It can be created on a floppy drive or a USB flash drive.

**perimeter network**

A network used to host Internet-facing servers while providing a layer of protection for these services. Also called a demilitarized zone (DMZ).
**permission inheritance**

The process of passing permissions from parents to children. In NTFS, permissions are inherited by default for all files and folders within a folder. Inheritance can be disabled.

**pharming**

Malicious practice of modifying name-resolution methods to redirect users from valid websites to bogus websites. DNS poisoning is one method used to redirect the users.

**phishing**

Malicious practice of sending emails to users, trying to entice them into providing personal information or trick them into visiting a malicious website.

**piggybacking**

Piggybacking (or tailgating) is when more than one person accesses a secure area but only one person provides credentials. Other individuals follow close behind but don’t provide credentials. Piggybacking can be prevented with a mantrap.

**private key**

One of two matched keys used with asymmetric encryption. The private key must stay private. If it’s compromised, the key pair shouldn’t be used any more. Anything encrypted with the private key can only be decrypted with the matching public key. Similarly, anything encrypted with the private key can only be decrypted with the private key.

**Protected Mode**

A built-in feature in Internet Explorer. Protected Mode runs IE with restricted privileges so that a malicious website can’t write, alter, or destroy data on a user’s system. It also helps prevent a malicious website from installing any type of malware on the system through the browsing session.

**PTR (pointer) record**

A DNS record used to resolve IP addresses to host names.

**public key**

One of two matched keys used with asymmetric encryption. The public key is freely shared in a certificate available to others. If the matching private key is compromised, the key pair shouldn’t be used any more. Anything encrypted with the public key can only be decrypted with the matching private key. Similarly, anything encrypted with the private key can only be decrypted with the public key.

**R**

**RADIUS**

Remote Authentication Dial-in User Service. An authentication service used with remote-access servers for dial-in or VPNs. It can also be used as an 802.1x server to authenticate wireless and wired connections.

**read-only domain controller (RODC)**

A special domain controller that doesn’t store Active Directory secrets. RODCs are deployed to branch offices with limited physical security.

**reducing attack surface**

A security principle that says to remove or disable all unnecessary services and protocols. Removed and disabled services
and protocols can’t be attacked. This reduces the number of possible attacks on a system.

**risk**
The possibility that a threat can exploit a vulnerability.

**risk mitigation**
The reduction of risk by reducing vulnerabilities. Vulnerabilities are reduced by implementing controls. For example, strong authentication and access controls reduce the possibility that unauthorized personnel can access data.

**rogueware**
A Trojan-horse type of malware. It looks like it’s antivirus software or something similar, and it tricks users into installing it. After it’s installed, users are enticed to pay to remove non-existent threats from their computer.

**Run as Administrator**
A Windows Server 2008 feature that allows a user to launch an application as an administrator. Run as Administrator is also available on Windows 7.

**S**

**secret key**
The single key used in symmetric encryption to encrypt and decrypt data. Data encrypted with a specific secret key can be decrypted with the same secret key.

**secure content management (SCM) firewall**
A firewall appliance that filters email and other web-based content. Some SCM appliances can also work as proxy servers.

**secure dynamic updates**
An extension of dynamic updates. Secure dynamic updates prevent unauthorized computers (non-domain computers) from updating DNS records. Only authorized clients (members of the domain) can update DNS records. DNS must be installed on a domain controller, and the zone must be an Active Directory–Integrated zone to support secure dynamic updates.

**Security log**
The log in Windows systems that records auditable activity. You can view the Security log in the Event Viewer.

**smart card**
A card about the size of a credit card used for authentication (something you have). Smart cards have certificates embedded within them and are read by smart-card readers. It’s common to require a PIN or a username and password with a smart card as part of a multifactor authentication implementation.

**SmartScreen Filter**
A built-in feature within Internet Explorer that helps protect against phishing attacks. It helps detect malicious websites and warns users if they try to go to a known malicious website.
social engineering
The practice of tricking users into giving up sensitive information or performing actions on the part of the attacker. The attacker is the social engineer and often succeeds without using technical skills.

something you are
One of the three factors of authentication. It includes distinguishing characteristics about a person that are verified with biometrics such as fingerprints. Other factors of authentication are something you know and something you have.

something you have
One of the three factors of authentication. It includes items you can carry, such as a smart card or a token. Other factors of authentication are something you know and something you are.

something you know
One of the three factors of authentication. It includes knowledge such as knowing a password or a PIN. Other factors of authentication are something you have and something you are.

spam
Unwanted or unsolicited email. Spam often includes malware as an attachment, embedded as a script, or as links to malicious websites.

SSID (service set identifier)
The network name for a wireless network. It’s recommended that you change the default SSID for a wireless network and leave SSID broadcast enabled.

standalone CA
A CA created with Active Directory Certificate Services (AD CS). It’s used to issue certificates within an organization or publicly. It can use Active Directory Domain Services, but doing so isn’t required.

strong password
A password that is sufficiently long and complex so that it’s difficult for an attacker to crack. Microsoft recommends passwords of at least 14 characters made up of a mixture of uppercase and lowercase letters, numbers, and symbols.

Additionally, none of the words in a dictionary of any language should be included in the password.

symmetric encryption
A protocol that converts plain-text data into ciphered text. Symmetric encryption uses a single key (called a secret key) to encrypt and decrypt data. A popular symmetric algorithm is AES.

SYN flood attack
A specific type of DoS attack. A SYN flood attack (also called an IP half-scan attack) withholds the third packet in the TCP handshake process. When this is done repeatedly, it can consume system resources.
**System Center Configuration Manager (SCCM)**

An add-on server application that can be used to deploy updates. It includes more capabilities than WSUS, such as the ability to schedule when updates are deployed. It can also deploy applications and operating system images.

**Tailgating**

Tailgating (or piggybacking) is when more than one person accesses a secure area but only one person provides credentials. Other individuals follow close behind but don’t provide credentials. Tailgating can be prevented with a mantrap.

**Threat**

A manmade, natural, or environmental event that can negatively impact confidentiality, integrity, or availability. Threats can be intentional or unintentional.

**Token**

A physical device that can be carried around and even attached to a key chain as a key fob and used for authentication (something you have). It displays a number, which changes regularly, such as every 60 seconds, and is synchronized with a server. When users want to log on, they enter the number shown in their token and additional information such as their username and password, or a PIN. As long as all the information is accurate (and entered before the number in the token changes), the user is able to authenticate.

**Trojan horse**

A type of malware that looks like one thing but is actually something else. It could be a screen saver that looks useful but includes a malicious component such as a keylogger.

**Trusted Root Certification Authority store**

A location on a system that holds certificates from root certification authorities that are trusted. Many certificates are automatically located in the Trusted Root Certification Authority store as part of the Windows operating systems.

**Unified Threat Management (UTM) Firewall**

A firewall appliance that provides multiple protection mechanisms in addition to a basic firewall or an SCM firewall. A UTM can include routing, firewall, VPN access, and network-performance features.

**User Account Control (UAC)**

A security feature that prompts users before allowing some changes to the system. When a user logs on with an administrative account, two tokens are assigned: one for regular use and one for administrative use. UAC prompts the user when the administrative token is needed.

**Virus**

A type of malware that requires human interaction to spread. It’s an executable
program that replicates itself and can spread from computer to computer after the user launches it.

**vulnerability**
A weakness. Examples include weaknesses in software, hardware, procedures, configurations, and physical security. Threats can exploit vulnerabilities, resulting in realization of risk.

**W**

**Wi-Fi Protected Access (WPA)**
WPA was introduced as an interim replacement for WEP until WPA2 could be finalized. WPA offers significantly improved security over WEP without requiring additional hardware.

**Wi-Fi Protected Access version 2 (WPA2)**
WPA2 provides a permanent fix for the security problems of WEP and is standardized as IEEE 802.11i. WPA2 often requires different hardware than that used by WEP and uses the Advanced Encrypted Standard (AES) encryption method.

**Windows Server Update Services (WSUS)**
A free server application used to deploy updates. An administrator synchronizes the server with the Microsoft Update site and approves updates, and WSUS deploys approved updates.

**Windows Update**
A Microsoft service that provides updates for the Windows operating systems.

**Wired Equivalent Privacy (WEP)**
An early security protocol used for wireless networks. WEP has several security flaws and isn’t recommended for use.

**worm**
A type of malware that doesn’t require human interaction to spread. It’s a software program that copies itself onto other computers by connecting over the network and exploiting open ports.

**WPA-Personal/WPA2-Personal**
A form of Wi-Fi Protected access that uses a preshared key (PSK) for authentication of clients. All clients use the same PSK.

**WPA-Enterprise/WPA2-Enterprise**
A form of Wi-Fi Protected access that uses an 802.1X authentication server for authentication. The 802.1X authentication server passes out encryption keys used by the clients.