Cyber Security Concepts

There is a shift to internet and cloud-based connectivity that has become more prevalent. The proliferation and sophistication of hacker attacks has multiplied as well. That has changed how companies view and develop security strategy from intranet to cloud. The hackers attempt to steal or destroy application data on internal servers. Any effective security strategy should have multiple layers of security.

Exploit - Attack strategy that leverages an existing security vulnerability. The exploit is software designed to attack a specific vulnerability. (malware, root kit etc.) email phishing, MITM, spoofing, DDoS.

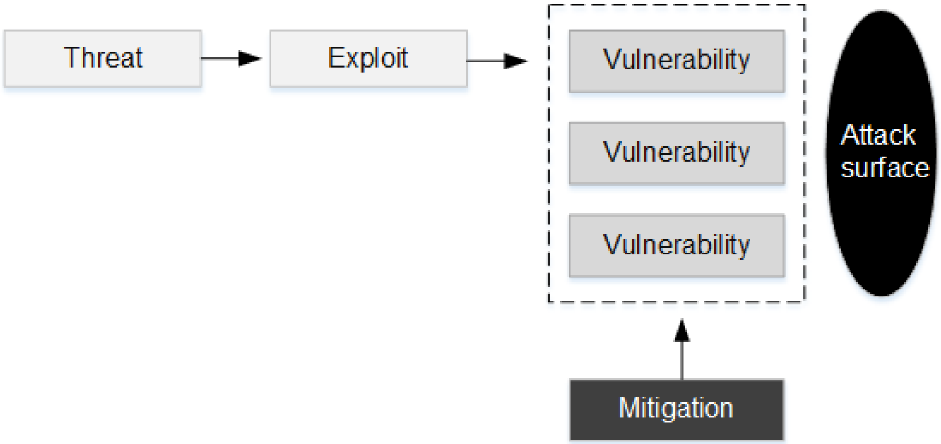
Vulnerability - Existing security flaws such as software bugs, default passwords and misconfigured firewall rules that could be exploited.

Mitigation - Specific techniques employed to decrease or eliminate the security threat level of a vulnerability. Some examples include awareness training, software updates, IPS, firewall inspection, Incident response and vulnerability assessment testing.

Threat – This is a potential danger, or event that results from exploiting a vulnerability. Hackers will often use multiple exploits in a threat. Some examples are spyware, malware, power outage, virus, and software error.

Attack Surface - The number of attack vectors that exist for a hacker to exploit vulnerabilities that enables unauthorized access.

Figure 1 Cyber Attack Chain Flow



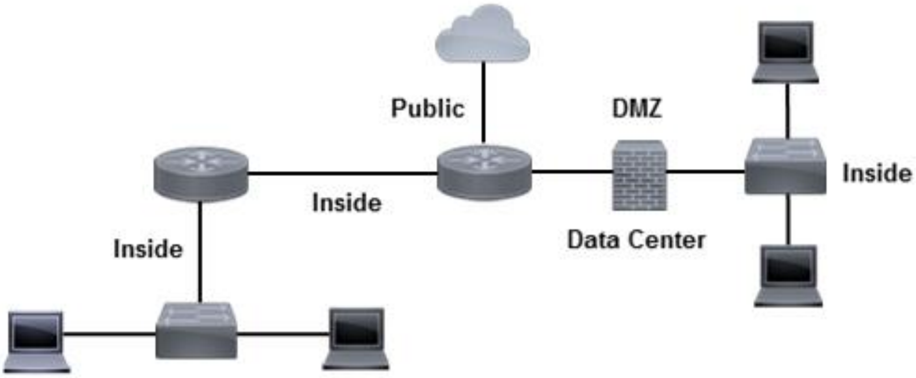
Security Zones

The idea of creating security zones is fundamental to network security. It is common for a company network to extend globally and transit multiple different administrative domains. On-premises security architecture is based on an intranet, guest, DMZ, and internet. As packets move from the inside intranet through each zone to the internet, there is a lower security level. The intranet security zone has the highest security level.

Intranet zone is accessed from employees internally and via VPN tunnel. VPN tunnels traverses the public internet zone with encryption. Guests are granted temporary access from the intranet, that amount to internet zone access only. DMZ is a mixed security zone with private and public interfaces for internal and external access. Finally there is the internet zone where all network interfaces are public only.

The internal network has highest security level where firewalls and monitoring is deployed. Security zones are created primarily with network addressing and access control lists (ACLs). There is application security implemented as well with user authentication and authorization methods.

Figure 2 Security Zones



The following illustrates the transition from lower to higher security level. The user starts outside the building with physical access security controls and transits on the private network to eventually access server data.

Security Program Elements

User awareness and training have become a standard part of any security strategy. One of the most compelling reasons is the proliferation of an exploit called phishing emails. It exploits the tendency to click on an email that is masquerading as something legitimate. It could be a Fedex delivery notice or an alert notification from your bank. The security program is designed to create awareness among the user community for developing proper work habits. In addition there is training on common security attacks and vulnerabilities. The following is a list of topics and recommendations that should be discussed as a part of any awareness and training program.

Clean desk policy

- Notes on desk, passwords, leaving computer on, screen saver sword.

Internet attacks

- Avoiding phishing email, installing software, personal browsing, adware, spyware, viruses, ransomware, root kits, trojans, botnet

Separate work and home

- BYOD, malware, media cross-sharing, mobile app. store.

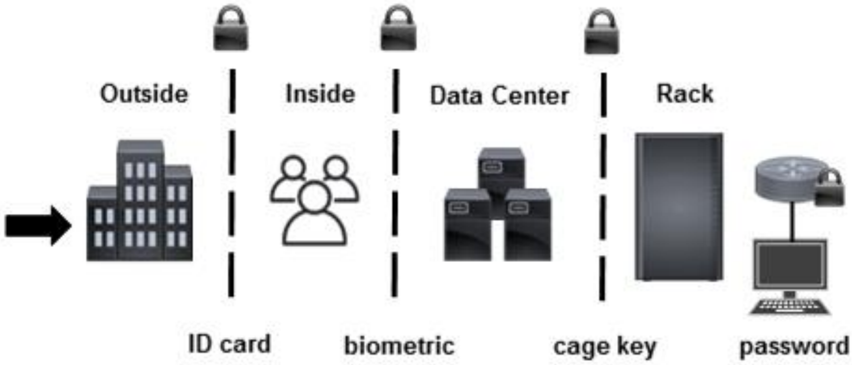
Physical access

- Password surfers, unauthorized visitors. tailgating behavior

Social media

- Using same work login and password, phishing links, sharing information

Figure 3 Physical Security Zones

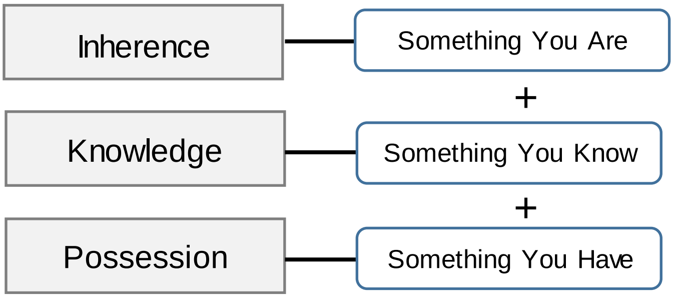


Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is part of a multilayered security architecture. In fact, layered security exists as well from the internet router (perimeter) to server data. Network access is often available globally from a variety of public and private locations. MFA is a solution to the increasing fraud and problem of stolen credentials.

Any strategy must verify user identity based on at least two or more independent security credentials. Consider that multiple security layers exist from when you swipe an ID card, enter a building and then access data. Having multiple authentication also eliminates any single point of failure when security credentials are stolen or compromised. It blends static and dynamic credentials to optimize security posture.

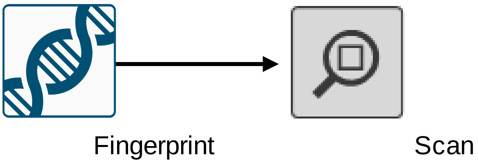
Figure 4 Multi-Factor Authentication Elements



Inherence Factor

This is something you are that is uniquely you. It is a biometric security credential that cannot be shared as with a password or smartphone. Some of the most common biometrics include fingerprint, facial scan and voice recognition. Biometrics are astoundingly effective as an identity credential that is difficult to steal. The scan is dynamic however biometric records are stored for comparison purposes and have been hacked recently. This is where multi-factor authentication really pays off.

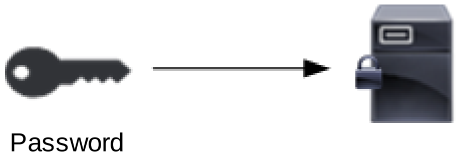
Figure 5 Multi-Factor Inherence Elements



Knowledge Factor

This is something you know that is uniquely assigned to you. The most common example is a username/password credential for authentication of user identity. Most software will verify that at least the username or user ID is uniquely assigned. There is email account name as well that is often assigned as an alternative to username. Any username/password assigned for user authentication is inherently static in nature particularly when the password is never changed. Some new security policies are starting to include random security question challenge for user requests.

Figure 6 Multi-Factor Knowledge Elements

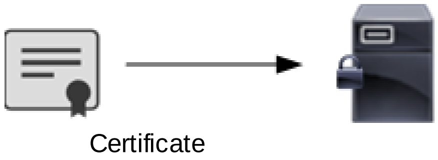


Possession Factor

This is something you have that is uniquely assigned to you. It is either hardware-based or temporary software-based credential. Some examples include digital certificate, hardware token, OTP software token and smartcard. There are a variety of applications for digital certificates such as wireless authentication, VPN and SSL for web-based applications.

Digital certificates are a common identity credential to confirm device and user authentication. They provide mutual authentication between client and server that enhanced identity beyond standard username/password credentials. Tokens are dynamically generated One-time password (OTP) or pin code. The purpose is user authentication for a particular session only. Any new login would require you to enter a new token generated from a keyfob or text message.

Figure 7 Multi-Factor Possession Elements



Location Factor

This is somewhere you are, and referred to as location factor. It is not part of standard MFA model, however it is sometimes used for authentication. For example, security software would verify your login is from a country where you are permitted to originate a network login request. Most employees do not travel outside of the country or even region when working. This factor prevents rogue connections from all international locations or a subset of known hacker sources. There is a time factor as well that could verify any user requests that are made outside normally permitted hours of operations. It is quite easy to enable GPS on a network endpoint device or track source location of ISP where user request originated.

Examples

- ATM = Debit card + Pin code
- Physical Access = Swipe card + Fingerprint
- Online Banking = User ID/password + OTP text message
- Remote VPN = Certificate + Hardware token + username/password

Table 1 MFA Security Attributes

Inherence	Knowledge	Possession
fingerprint	username	certificate
facial scan	password	one-time password
voice recognition	security question	hardware token

Table 2 Layered Security Solutions

Authentication	Authorization	Accounting
• Swipe card • OTP • Certificates • Pre-shared keys • Port security	• RADIUS • TACACS+ • 802.1x EAP • Local	• Syslog • RADIUS • TACACS+