Computing Systems And Security

In both the Star Army of Yamatai and a variety of other organizations (both military and civilian), computing systems have often been seen as nigh invulnerable systems tasked with not only the operation of critical systems but also tasks that are considered too mundane for trained personnel to bother. However, such a fallacy can lead to downfall as unrealistic expectations are crushed by the overbearing weight of reality.

The Fallacy

Mostly seen in some of the more powerful organizations, “the fallacy” of invulnerable computers revolves around the use of powerful, sapient Artificial or Synthetic Intelligences with near god-like omnipotence that allows entire interstellar networks to remain unhindered by the woes of more primitive networks. Hackers and their ilk remain frustrated by the overwhelming force of security these networks are capable of maintaining. This leaves networks of these Superpowers to be overpowering and flawless beacons of Information Storing Might.

The Reality

The reality is much more mundane than expected. Networks such as PANTHEON are indeed powerful, but not invulnerable. The more accurate term for it all would be *resistant* than invulnerable.

The Resistance of "Super" Systems

The artificial/synthetic intelligences involved in these “Super” Systems are what gives such networks their resistance. The main factor of their success are the speeds at which they process information accurately and efficiently. This allows faster reactions to intrusions as well as the capability of maintaining a more proactive stance on network security when compared to standard networks.

This doesn't make Information Specialists obsolete though as not even the AI / SI monitors of such a network can be completely safe. Sometimes intrusions or cyber-war implements can target these monitors, making the Information Specialist the 'hero' that rescues the 'victim'.

On Networks without AI / SI Monitors

With networks that do not have the advantage of Artificial / Synthetic Intelligences to monitor them, the Information Specialist's importance is almost tripled. Without the constant vigilance of the Monitor, the Information Specialist must set up alarms and constantly maintain security on networks to insure confidentiality and authentication.

The Weaknesses of Information and Computing Systems

Computing Systems and their Networks have many weaknesses both artificial and natural. While some of these weaknesses can be compensated for and / or protected, it is impossible to completely protect from all of them.

Artificial weaknesses are exploits and design flaws that have either been purposefully added through sabotage in the design phase, through negligence of design standards/philosophies, or through just the standard deviation of manufacturing that may cause errors. These can be compensated for via updates and maintenance, but they can also be exploited by sapient threats.

Natural weaknesses are dangers that occur in the natural environment. These dangers can interfere with signals or even damage the hardware computing / information systems use for operation. While computing systems can be protected from these natural weaknesses, sometimes protection measures fail.

The Enemy and their Tools

Threats to networks and the tools used by them.

Potential Threats to Computing Systems

Threat	Description
Cyber Warfare Specialists	Information Specialists from other Factions that purposefully infiltrate systems to steal or sabotage system information.
Disgruntled/Disgraced Employees	Individuals that work for the organization that use their current systems access to steal or sabotage system information.
Disgruntled/Disgraced IT Specialists	Information Specialists that work for the organization and use their specialized training and knowledge to steal or sabotage system information. They may even try to take down the entire system themselves.
Disgruntled/Disgraced IT Security Specialists	The greatest danger to any system, these individuals use their knowledge and training to bypass security protocols to devastate entire information systems.
Environmental Concerns	While not an active enemy, the environment is also a threat to computing systems. Electromagnetic storms and a variety of natural disasters can physical wreck hardware and eliminate computing systems that are needed for everyday life.
Equipment Failure	An issue with any type of system (whether information or not) equipment eventually fails.
Hackers	Civilians that infiltrate systems in order to commit criminal acts either for pleasure or for *making a statement*.

Tools and Techniques of the Enemy

Artificially created methods / tools used by sapient attackers to damage computing systems.

Tool / Technique	Description
Malware	A generic term for any program that perpetrates an illegal or harmful action upon a system.
Virus	Programs that attach themselves to legitimate programs. Normally spread via electronic messages and file transfers.
Worm	Stand-alone programs that do not attach themselves to other programs, worms spread throughout networks. Worms may propagate without user interaction.
Direct-Propagation Worms	Worms that target systems with specific vulnerabilities.
Blended Attack	An attack upon a network that uses multiple tools and techniques.
Mimic [1)]	A program that hides itself in a system by deleting a system file and replacing it. It is difficult to detect due to appearing to be a legitimate file.
Remote Mimic[2)]	A program that gives attackers remote access to a system.
Downloaders / Droppers	A Mimic that is small and even more difficult to detect with the sole purpose is to download a larger Mimic in order to cause more havoc.
Spyware	Refers to a broad spectrum of Mimics that gather information.
Spyware - Keystroke Loggers	Records a system user's inputs and transmits them to an attacker.
Spyware - Password Thief	Informs a system user that they need to log off a network site and retype their username and password. The program then sends the information to the attacker.
Spyware - Data Miner	searches through a system's storage drive for the same times of information sought after by keystroke loggers. The program then sends the information to the attacker.
Rootkit	A program that takes control of a system's Administrator account and gives the attacker remote access to all administrator privileges for that system.
Social Engineering	A technique attackers use to take advantage of flawed judgement by convincing the victim to take actions counter to security policies.
Social Engineering - Unsolicited Commercial Messages[3)]	While most of these messages are just annoyingly legal advertisements, some may be fraudulent or advertise dangerous products. They are also a common vector in dispensing malware onto the systems of users accessing any attachments on these messages.
Social Engineering - Harvesting[4)]	Electronic Messages that appear to be from banks or firms the victim engages in business. However, they are mostly used to fool the victim into giving out specific, sensitive information.
Social Engineering - Pin-Point Harvest[5)]	Harvesting that is aimed at a specific individual or small group of individuals.
Social Engineering - Hoaxes	Fraudulent messages that attempt to get a victim to either embarrass themselves by repeating stories they've heard or damage their own systems by deleting critical system files.
Social Engineering - Tailgating	The act of entering a secure area by following behind someone and letting the individual's sense of propriety keep them from closing the door on the tailgater.

Tool / Technique	Description
Hacking	The act of infiltrating a system or network of systems in order to accomplish some set objective whether for theft, destruction, or prank.
Address Spoofing	A method used by attackers to either conceal the origin of the attack or framing another system for said attack.
Chain Attack	An attack technique that involves attacking through multiple victim systems before assaulting the actual target system.
Denial of Service Attack	An attack that attempts to make a network or service inaccessible by flooding it with 'packets'.
Distributed Denial of Service Attack	A Denial of Service attack that makes use of a collection of enslaved systems to assault a network with more 'packets'.
Bot	A system that has been enslaved to an attacker for the purpose of attacking other systems / networks.
Man-in-the Middle Attacks	A form of attack where an attacker intercepts messages being sent between two parties and forwards them on.
ARP Poisoning	A network attack used to reroute traffic for man-in-the-middle attacks or even for DoS attacks.
Packet Sniffers	A tool that reads packets and allows intruders to intercept and read traffic.
Evil Twin Access Point	A system that masquerades as a wireless access point.
Code Injection	If raw data is not examined for possible attacks when parsed by users on any level of the system (which is resource intense and often inefficient), the code to signify the end of raw data can be given and the system will anticipate executable code to follow. Code can then be injected on the end of the data into the interpreter
Buffer Overflow	Similar to code injection, the same principle is instead applied to memory.

Security and their Countermeasures

In both military and civilian organizations, the importance of information security is paramount. Raw Data as well as the Information gleaned from said data is a currency unto itself and much therefore be protected just as much, if not more, as any other asset.

In this regard, Information Specialists and their AI / SI Assistants are necessary in order to be both proactive and reactive against any possible threat. They would be responsible for the protection of any and all data in their respective jurisdictions as well as the hardware that stores and processes such data.

Access Control

A preventative measure used to protect information systems, Access Control revolves around the physical and electronic restriction of information based upon certain criteria. Over all, Access Control has three functions: Authentication, Authorization, and Auditing. **Authentication** means assessing the identity of each individual claiming to use system resources. **Authorizations** are the specific permissions an authorized individual can access. **Auditing** is the collecting of information about an individuals activities while logged onto the system.

For Authentication, a simple password is never enough. At this point, two-factor or multifactor authentication are necessary for a strong authentication set-up (though Mimics and man-in-the-middle attacks may negate such endeavors).

Methods of Authentication	
Method	**Description**
Reusable Passwords	An outdated model of authentication using a series of characters/numbers to identify a user. Easy to crack and easy to obtain. Usage of reusable passwords requires strict policies.
One-Time Password Tokens	Small devices that generate one-time usage passwords from either connection to a server or synced seed generation. Works by creating an expected answer with the other machine then has to solve from a sensitive question which is not transmitted. Solves a few issues of reusable passwords.
Obfuscation	The act of hiding meaningful information as meaningless information - either as background static noise or as gibberish. Unlike encryption, cannot be solved mathematically and relies on both parties knowing the complete 'language'.
Media Tokens	Small devices that plug into systems to authenticate a user[6].
Proximity Access Tokens	Small devices that transmit authentication data to readers[7].
Magnetic Strip Cards	Primitive identification cards that store authentication data on a magnetic strip.
SMART Cards	Cards with built-in microprocessors and memory, which allow more sophisticated authentication methods.
Biometrics	Systems that read biometric data to authenticate users. Some examples range from primitive finger print scans to retinal pattern scans to even genetic scans.

Part of Authorization is the appropriate permissions individuals have when they finally log onto the system. To assign these permissions, there are two methods of assigning these permissions. **Individual Access Control** is the procedure in which individuals are assigned these permissions, which is a time consuming operation. Because of this, many users are assigned roles where permissions are then applied to those roles. This is known as **role-based access control**. This ability to access the system can be further broken down into whether departments or sub-divisions can assign roles or not. In **Mandatory Access Control**, a central authority is responsible for assigning roles and permissions. **Discretionary Access Control** is more flexible and allows departments and sub-divisions to assign roles to their members.

In Auditing a System, all access and activities to a system must be recorded and logged in secured servers / sections of the system. This allows IT Security personnel to periodically examine these logs for signs of suspicious activity. With the advent of Artificial / Synthetic Intelligences comes the ability to have these logs monitored constantly and quickly in order to speed up the process of identifying and neutralizing intruders into systems.

Physical Access

While a part of Access Control, Physical Access to terminals and core components of Information / Computing Systems must be strictly monitored and controlled. This means that core components of a system are not centralized and distributed in a manner where damage to one location will not destroy

the system as a whole. These facilities must also be secure with access to them restricted to necessary personnel only and all terminals / equipment must be physically secured to their locations.

Securing these areas also means denying unauthorized equipment as well. Recording equipment and storage media should be limited to those authorized by the organization or banned altogether. These facilities need to be monitored as well, which means recording activity both at the entryway and inside the facility as well.

Encryption for Confidentiality

The basic method of communicating confidentially is via a cryptographic system. Communication between two systems begins with three **handshaking stages** before actual communication can start. **Initial Negotiation** involves the selection of a cipher suite by both parties. **Initial Authentication** involves testing the identity of each communication partner, creating a baseline reading. **Keying** involves sending cipher keys securely for authentication purposes. These handshaking stages are done automatically and leads to the actual communication between the two partners. This requires message-by-message authentication and includes an electronic signature in every message so the systems may identify each other. Digital signatures may also be used to authenticate single messages with keys.

Some primitive methods of ciphers involve public-private key encryption and hashing. **Public keys** are keys used by individuals to identify themselves and are openly available to everyone. **Private keys** correspond to public keys but are kept secret from everyone but the communication partners, who use the private key to decrypt messages sent by their public keys. **Hashing** is applied to binary messages and produces and irreversible cipher-text that cannot be decrypted like encryption.

However, with the advent of quantum computing, **quantum encryption** has come to be the norm. This is done via **quantum key distribution**, which can deliver enormously long one-time keys to communication partners as long as the entire message. While not susceptible to normal cryptanalysis and attempts to eavesdrop can be immediately apparent, **quantum key cracking** by AI/SI assisted cyber warfare specialists may be done. **Quantum key cracking** is essentially a brute force method of cracking by trying thousands of possible keys at once. This doesn't even count the usage of **quantum networking** either, since the interception of quantum transmissions requires specific equipment that is precisely tuned. If not tuned properly, the transmitted message could come out garbled and unreadable.

This makes intercepting and decrypting transmissions from quantum computers a time-consuming and frustrating affair for everyone, including the more technologically advanced nations. It means that data theft is often easier via the social engineering methods or even by placing imposters into organizations than by intercepting transmissions.

Countermeasures to Enemy Tools / Techniques

The following are countermeasures to tools and techniques of hackers.

Countermeasure	Threat	Description
Black Holing	Denial-of-Service	Dropping all IP packets from an attacker. Short-term strategy since attackers can change source IP addresses.
Validating Handshake	Denial-of-Service	Creates false openings to distracted attackers.
Rate Limiting	Denial-of-Service	Reduces certain types of traffic to a reasonable amount and is a proactive measure against DoS attacks.
Static Host Tables	ARP Poisoning	Manually sets network important tables rather than allow dynamic updating. Makes IT specialist have to change tables with the organization.
Limiting Local Access	ARP Poisoning	Literally limits the access of the local network from foreign hosts.
Firewalls	Provable Attack Packets	Examines packets that pass through it for provable attack packets. Those that test positive are denied entry while others are allowed through.
Border Firewall	—	A firewall that sits between external networks and an organizations network.
Internal Firewall	—	A firewall that filters traffic passing between parts of an internal network.
Application Proxy Firewall	—	A firewall that examines application messages for attack packets.
Intrusion Detection Systems	—	Tools that examine streams of packets for suspicious activities that can signal possible attacks. Does not automatically drop packets though so it must be monitored.
Intrusion Prevention Systems	—	Acts similar to IDSs, but has the ability to automatically stop possible attacks.
Anti-Malware Programs	Malware	A set of programs used for identifying, quarantining, and repairing/purging malware from a system. Some examples of these are Anti-virus, Anti-Spyware, and Anti-rootkit.
Honey Pot	—	A false target (often emulated) machine or database isolated and monitored from mission critical systems which exists to fool an attacker into thinking they have attacked successfully. The machine has a false or fake version of whatever the attacker is looking for, fooling them into thinking they have succeeded and relies on the attacker not being able to verify their find through hash or functionality.

Host Hardening

Host Hardening is a set of policies and procedures that involves securing any device with an IP address against intrusion. In order to do this, several tasks must be implemented:

- Keeping Operating Systems up-to-date and patched
- Keeping Applications up-to-date and patched
- Instituting a schedule of system maintenance and testing
- Managing Accounts and Roles to ensure permissions are up-to-date.

- Ensuring proper Access Control is maintained.
- Maintaining a set schedule and procedure on the back-up of all data on a system.

Penetration Testing

Penetration testing is a procedure in which a security consultant or organisation are hired to perform an agreed attack on the system without malicious intent to test for holes or gaps in security using the same methods real attackers would be.

OOC Notes

This page was originally created on 2013/11/05 08:12 by Abwehran Commander.

Approved:
https://stararmy.com/roleplay-forum/threads/computing-systems-and-the-lack-of-invulnerability.14852/

1)

Trojan Horse
2)

Remote Access Trojan
3)

Spam
4)

Phishing
5)

Spear Phishing
6)

ie. USB
7)

ie RFID