

Security+

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.



PrepLogic

Be Prepared. Be Confident. Get Certified.



Justin Korelc - Author

Domain 1 - Systems Security

The full scope of system security concepts are an all-encompassing umbrella category of computer-related exposures, threats, risks and vulnerabilities. Any security issue corresponding to end-user applications and the underlying operating system falls under this categorical heading. Various types of threat, risk, vulnerability and exposure exist at the local level, where physical access is granted and authorization provided to perform computer operator tasks.

System Security Concepts

General system security concepts are governed by a few core standards and principles. These elements compose the foundation for larger system security constructs and establish the groundwork to build frameworks for robust security components.

System Security Standards

A system security standard forms the basis for exercising secure procedures and baseline for executing secure functions within the context of secure computing systems. System security standards are composed into formal security policies that dictate the overall practices and procedures governing an organization's operations.

- **Trusted Computer System Evaluation Criteria (TCSEC):** Also known as the 'orange book.' The TCSEC is an old standard that describes security levels operating systems. Security designations range from A to D, with D being the most secure. The C2 standard level was the goal which discretionary access control based operating systems like Windows, Netware, and Linux tried to attain. TCSEC was replaced by the Common Criteria.
- **Information Technology Security Evaluation Criteria (ITSEC):** A European security criteria based on TCSEC. However, ITSEC rates both functionality (with a rating of F for CIA), and assurance (with a rating of E). ITSEC was replaced by the Common Criteria.
- **Canadian Trusted Computer Product Evaluation Criteria (CTCPEC):** This is a computer security standard comparable to the American TCSEC ("Orange Book"), but somewhat more advanced. CTCPEC was replaced by the Common Criteria.
- **Common Criteria (CC):** The CC is an international standard (ISO 15408) for computer security. Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. It is considered the de facto security evaluation criteria that the international community follows.

System Security Threats

The practice and process of system security requires professionals and practitioners to maintain constant vigil over end-user interactions, application launches, system events and also keep abreast of current security topics. Only truly ambitious individuals will succeed in the dynamically evolving security realm, where one false move or absolute failure can sometimes unfairly overshadow a history of successful outcomes. Your entry into the security field begins with identifying local system threats, which is where most of the firefighting tasks happen.

Privilege Escalation

Multi-user computer systems are designed for interaction among numerous users and user groups, each having separate and incompatible permissions to perform various activities. For a system attacker, the ideal user account has administrative privileges on the system and is permitted to perform virtually any task—particularly those that further intrusion, infiltration or interception of valuable information. A *privilege escalation* attack exploits a configuration error, design flaw or exposed vulnerability in a privileged security application to gain illegitimate access to protected resources.

Virus

A computer *virus* is any form of malicious code that spreads from system to system by attaching itself to data or files. Viruses typically self-replicate on local systems, however they can extend to other computers by targeting network drive shares, removable media and other communal resources. Each virus is specifically designed to attack systems in a particular way and target particular areas. The following list briefly describes the different features and forms a virus may take:

- **Resident virus** – a terminate-and-stay resident virus permanently attaches to the host computer and operates in memory (RAM). It attempts to load before other mechanisms that attempt to analyze, detect and identify its purpose and origin and can bypass, interrupt or manipulate basic operating system functions.
- **Direct action virus** – an aggressive form that replicates and takes direct action when triggered by some condition, date or event. The direct action virus typically resides in system folders or the root directory path where it can be readily accessed and activated and carry out its tasks when the system boots up.
- **Overwrite virus** – a virus can partially or completely delete information contained in the files it infects, even replacing portions of application code with its own payload. Viruses of this kind are generally easy to identify with anti-virus software, as they generally tend to alter end-user and system applications in noticeable and identifiable ways.
- **Macro virus** – certain applications contain embedded scripting or “macro” languages enabling users to automate long series of operations as single shorthand actions. A *macro virus* targets these applications by containing code that replicates and replaces other macros to launch the virus payload when common functions are called.
- **Polymorphic virus** – a virus can avoid detection by through cyclic changes to its original form. Such a virus may encode or encrypt certain code segments that are transformed during runtime as usable code segments, then later encrypted differently than before to evade signature analysis and thwart behavioral analysis engines.
- **File infectors** – the traditional virus is a file infector that targets executables to cause direct or indirect execution of its payload. Most viruses fall under this category and are further classified depending on what is targeted and the actions taken during the infection process.
- **Companion virus** – another typical type of viral infector is the *companion virus*, one that accompanies another ordinary executable file. When the source file executes, control is passed to the companion virus and the end-user remains completely unaware.
- **Boot sector virus** – viruses may also infect the boot sector on a storage volume with its own payload to ensure that the virus always loads before the operating system. Though less common, these viruses still flourish since master boot records (MBR) and other disk allocation methods see continued use.

Worm

A *computer worm* is exploitive malicious code like a virus in that it self-replicates; however, all similarity ends there, as one thing a worm does (that a virus cannot do) is replicate directly across network media. Worms are also generally designed to leverage some software, system or service vulnerability to enable propagation across network connections.

Trojan

The classic Trojan horse is a class of computer threat that apparently perform some desirable function (launch a game, activate an e-card) but instead transparently or invisibly conducts malicious activity to allow unauthorized access and/or usage of the affected machine. A Trojan horse application is often disguised as a legitimate application or portion of some software suite and opens a back door into the system when invoked by the user unless designed to trigger upon some condition, date or event.

Spyware

Computer software installed surreptitiously and without the owner's or operator's consent and then attempts to harvest personal information (e.g., usage trends, software licenses, sites visited), invades privacy or manipulates browser activity is called *spyware*. Such software appears to be legitimate but contains hidden functionality that is otherwise undesirable and unwarranted.

Spam

Unsolicited bulk email messages (particularly those sent indiscriminately to tens, hundreds or thousands of subscribers) is called *spam*. Spam is the electronic form of postal "junk mail", filling inboxes with useless and unrequested material typically used for marketing purposes. Spam can be malicious, but mostly it takes the form of dubious advertisements or money schemes.

Adware

Advertising-supported software or *adware* is any program that automatically displays or downloads advertisements during application usage. Adware may accompany or integrate into a larger software package and install usage monitoring components, but mostly its purpose is to custom tailor advertisements for targeted users.

Certain types of adware are also spyware if they perform the same information gathering and snooping functions. However, adware is mostly harmless in that it only produces advertisements for goods and services or extended features not included as part of some free or limited software package.

Rootkits

Malware consisting of a program or collection of programs designed to hide one's presence and activity on a compromised system is called a *rootkit*. An attacker must first gain access for the rootkit to be truly effective and various layers of the operating system are manipulated to disguise activities, applications and connectivity from watchful administrators.

Botnets

A collection of compromised computers operating in a collected, cohesive fashion (coordinated by a controller computer) is called a *botnet*. Individual computers are captured and controlled by a *bot* or malicious application that leverages remote control for an attacker, the *bot herder*. Command and control channels are often basic IRC channels containing other bots within the botnet.

Logic Bomb

Any malicious code that lies dormant until triggered by some condition, date or event is called a logic bomb. A trusted insider could emplace a logic bomb to cause damage in the event of their firing or as part of industrial espionage for a competitor. Generally, logic bombs appear as part of some other unsuspecting software package and are invoked without the end-user's knowledge.

Hardware and Peripheral Security Risks

Computer security threats, risks and vulnerabilities are not restricted to software; even hardware can cause significant security violations. Several key aspects of the system require adequate protection against tampering and manipulation by unauthorized parties. Sensitive applications, services and processes can be disrupted and security mechanisms bypassed by employing or modifying various hardware configurations.

Basic Input/Output System (BIOS)

Every PC has a BIOS, which is specialized boot firmware designed to identify and initialize system devices prior to turning over control to the operating system. A computer's BIOS prepares the machine in a process called *bootstrapping* or just *booting*. Most computers provide basic access to BIOS settings through configuration menus invoked prior to boot-up. When users can perform unauthorized changes to BIOS settings they can bypass local security settings and violate company security policy.

The most common approach to securing the BIOS includes setting an administrative password so that users cannot change boot device priorities, enable or disable features or utilize unauthorized devices. If an attacker can boot from external media, none of the system's local security settings are effective and the internal storage volumes themselves are completely open to attack (installing backdoors, Trojans or rootkits) and manipulation (data theft, tampering or trashing).

USB Devices

Any removable storage media can present a series of issues in the protected workplace. Sensitive information can be passed beyond security controls and taken outside of the security perimeter. An individual can also knowingly or unknowingly introduce malware to the local system or attached network or use bootable USB media to bypass local security restrictions. Specialized USB devices can also harvest information, interrupt operation or copy data on-the-fly and in some cases transparently to the end-user.

USB devices access should be selectively enabled and tightly controlled to prevent users from bypassing restrictions, overcoming security or subverting control. Malware infections make little distinction about their storage media, just so long as it holds (and in some cases transports) its code for future use. Sensitive data cannot determine what storage devices are authorized or unauthorized, and will gladly store wherever accepted.

Mobile Phones

The emergence of the mobile phone marked a trend that would soon find itself merging with other portable technologies (e.g., image capturers, video recorders, music players, digital organizers) and converging on the corporate workspace. Because mobile phones are no longer mobile phones, they pose a considerable security threat for a number of reasons.

Bluetooth and 802.11 wireless have become a popular item among recent cell phone designs, which means that attacks can originate from or be destined for equipped phones. Newer phones are also capable of executing a range of compiled and scripted code, leaving many forms of computer-related attack feasible on these platforms. Phones equipped with cameras are capable of photographing sensitive equipment and information that is otherwise restricted to authorized parties.

Removable Storage

All removable storage does is create a temporary attachment point for users to access and copy data or execute files. Like USB (and Firewire) devices, removable storage media often helps end-users bypass local security restrictions that affect other portions of the system. Users may bypass safe storage requirements when operating in highly sensitive areas, relocate and expose sensitive data beyond the security perimeter, and introduce unsafe code or executable data into protected environments.

Network Attached Storage (NAS)

A common arrangement for larger networks is to place storage volumes in full view of the entire network scope so that all users may centrally access them. NAS devices create an attachment point between storage volume and network media thereby giving access to devices that are typically enslaved to a single computer.

Without proper permissions, unauthorized users may deliberately access confidential files and sensitive data. Left unchecked, malware can also easily propagate to end-user workstations and back-room servers via NAS drives. NAS security centers around administratively-configured group and individual Access Control Lists (ACLs) with restrictive access virtually segregated (VLAN and router rules) and physically separated.

System Hardening Practices

The practice of hardening a computer system follows a series of protocols, procedures and policies that define and describe system security. Blocking unused ports, removing unnecessary services, deleting unused applications and plugging all known holes are just some activities involved in the system hardening process.

Hotfixes, Patches and Updates

The term *hotfix* originally described remedying code fragments (called *patches* or *updates*) to currently-running applications but has now become to mean a single, cumulative package that includes files that resolve an identified problem in some software product. In some instances, a hotfix may resolve only a customer-specific issue and not reach widespread distribution channels.

Microsoft Windows uses the term *service pack* to describe collections of fixes, enhancements and updates for various related products. They can also be incremental in that a later service pack contains files not present in earlier service packs or cumulative in that it contains all previous files.