

General computer security

Presented by developerWorks, your source for great tutorials

ibm.com/developerWorks

Table of Contents

If you're viewing this document online, you can click any of the topics below to link directly to that section.

1. Tutorial tips	2
2. Security concepts	3
3. Physical security	5
4. Logistical security	6
5. Data security	7
6. Technical security	9
7. Overview and summary	11
8. Feedback	12

Section 1. Tutorial tips

Should I take this tutorial?

The objective of this tutorial is to give an overview of the security process surrounding computer systems. It is aimed at the computer professional who may or may not already have some security background.

This tutorial is general in scope. Many of the issues covered here will be examined in more depth in future tutorials.

Tutorial navigation

Navigating through the tutorial is easy:

- * Use the Next and Previous buttons to move forward and backward through the tutorial.
 - * Use the Main menu button to return to the tutorial menu.
 - * If you'd like to tell us what you think, use the Feedback button.
 - * If you must stop and want to resume on a specific panel, use the Section menu to find your place again.
-

About the author

Larry Loeb has been writing and consulting since the 20th century about computer topics. He has published a book on SET, the protocol developed by Visa and MasterCard for secure electronic transactions. He can usually be contacted at larryloeb@prodigy.net.

Section 2. Security concepts

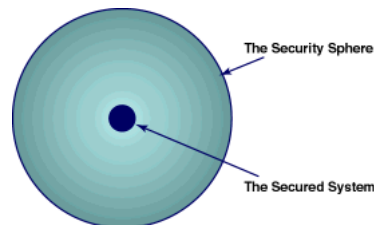
Security is spherical

Computer systems can never have absolute security in real life. They exist to be used; not to be admired in a locked room sealed away from the outside world. Systems can, however, be made more secure than they would be otherwise. Let's see how we can conceptualize this.

Security is spherical, but has markers

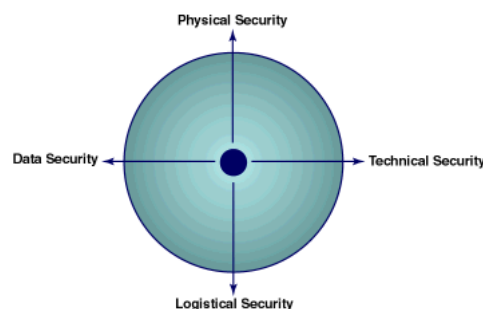
Threats to a system can originate from any source, not just the ones that you have considered or defended against. Think of the threat universe as a sphere around the target, each incoming threat made up of the results of many different vector components. Like a color wheel, it gradiates as the radius increases.

Think of the system at the center of a sphere made up of hostile intentions. Let's cut a circular plane out of the sphere in the middle of it.



Let's then mark four orthogonal vectors like the main points on a compass, except that they point to four security concepts.

These concepts are physical security, logistical security, data security, and technical security.



Security is spherical and made up of components

Each concept by itself is only a part of the overall solution to the risk management problem. Combined in the proportions necessary for the job at hand, they can have a powerfully deflective effect.

We will look at each "point of the compass" individually, so that we can learn to combine them.

Section 3. Physical security

Physical security overview

Physical security includes all that pertains to the physical siting and environment. In many situations, this area is ignored or downplayed. Bad move. What good is encryption of data if someone can waltz into the computer room and read data in plain text?

Physical security elements

The computer itself (and any hardware attached to it) should be covered in this phase. Relevant factors include the physical plant and the siting of the machine, any hardware "dongles" that are needed to run the program (perhaps for copy protection), and environmental factors.

Disaster recovery plans -- surely an integral part of any security operation -- should also be keyed to the physical situation.

Physical security can mean limiting access

One of the simplest and most effective concepts of physical security is to limit the access of non-essential personnel to the computing area by physical means, like walls and locked doors. Protect routers and servers in a secure, maintainable area; don't just shove them into a handy closet because there's space available there.

Scrutinize the cable and wires that go into and out of your site. If it's easy for a motivated attacker to place a listening device on an unprotected cable, then that's likely to happen. Use metal conduit shields routinely on cables to help make it harder for someone to tap the line.

Physical security summary

In summary, physical security deals with those aspects of security that are in the physical plane. If you can touch it, lock it down, or sit on it, it's physical.

Section 4. Logistical security

Logistical security basics

Logistical security is an institution's security policies and procedures. If the computer is in a locked room, the logistical aspect of security determines who gets the key.

In many ways, logistics are the management aspects of the security spectrum. In short, logistical security includes a business' usage of and support for security practices.

Logistical security embraces feedback

Logistics is where we "close the loop" on the security process. For instance, there should always be a way to obtain stakeholder feedback about the practice of security, as well as an oversight process to address any identified security lapses with an eye toward preventing their recurrence.

The results of the oversight/review efforts can and should impact policies and procedures. If they don't, the review process is not a true security review. It's a blame shifter.

Logistical security manages the details of security practice

Security depends on the correct execution of the appropriate policies. Logistical security includes the effective promulgation of those policies.

For example, a large organization might have well thought out policies in place, but fail to inform new hires about them. Good logistical security enlists human resources to disseminate security information, and continually monitors how well the information is disseminated.

Logistical security summary

Logistical security manages the implementation of security practices. It also incorporates a functional overview of the entire process. This is where the rubber of the paper meets the road of the data, so to speak.

Section 5. Data security

Data security is all about the data

Most people think that data security is the whole of system security, because this is where the whizz-bang stuff lives -- and because most users equate security with resistance to attack. Fancy encryption products (along with their ad budgets) and consultants galore inhabit this part of the security sphere.

But data security should mean that data is not corrupted or altered by some means. This includes data that's sent to or received from a network.

Data security uses differing technologies

Encryption/decryption technologies are only part of the mix used for data security. Simple technologies, like the use of test data sets of known values, can be as important to the data security effort as any other technology.

Sometimes, a technology aspect may combine our "compass points." The physical effect of networks on data (for example, any corruption due to data transmission alone) is usually both a hardware (physical security) and an application-level software (data security) issue. To resolve this, you should address it from both viewpoints.

Data security and software

The software that directly touches the data affects data security, as we've said. It is incumbent upon the analyst to verify each software component's function by itself and within the overall system. Components may function correctly when used independently, but fail in the aggregate system.

Databases, for example, may cause non-obvious failures in systems. If a database provides incorrect numbers, then clearly any downstream software will also produce corrupt results.

But say two database queries try to access the same data at the same time. The database software must be able to serve as a real-time traffic cop, or fall prey to the "fatal embrace" scenario where the data requests lock each other out from access in an ongoing manner. Failure to obtain data is as important a data security problem as any other.

Data security summary

The goal of data security is to preserve the true value of data as it passes through, and is changed by, the system.

Data security usually deals with differing technologies that span the system end-to-end, but from a process-specific viewpoint (a viewpoint that aggregates only the information affecting the process under review). You want the server to pass your data along the network, but you don't need to know what specific program the server is using as long as it functions transparently with your data. Data security focuses on the data and just the data.

Section 6. Technical security

Technical security

Somewhat of a catch-all, technical security comprises the technical details of a secured system. To use the previous section's example, technical security evaluates the operating system of a system's server for its resistance to attacks and its functionality.

As noted before, most users mean "resistance to attack" when they say "security". Technical security deals with the specific details involved in the resisting of attacks. When a virus invades, technical security acts as the immune system of the data ecology, ridding it of any infection.

Technical security means defense

Let's say a threat, such as a virus, has penetrated a secured system.

The technical security response team then:

- * Analyzes the vectoring of the threat -- which direction (combination of vulnerabilities) it arose from;
 - * Determines any negative effect ("damage") the threat will have on the system;
 - * Evolves defense and repair strategies;
 - * Disseminates user information on defense strategies (and monitors compliance) in its role as a user-trusted authority;
 - * Refers implementation of a necessary change in operations to the control structure responsible for the appropriate security "compass point";
 - * Implements any necessary software after-the-fact upgrading, again as part of its responsibilities as user-trusted authority;
-

Technical security organizes and interprets a collection of individual details

To fulfill its responsibilities, technical security has to manage, as well as keep current with, a mountain of details. Most will probably deal with manufacturer-recommended maintenance patches of installed software.

Technical security is responsible for the proactive, routine dissemination to users of this maintenance information, such as updates to virus detection software. This can be seen as locking the barn door *before* the cows get out.

Technical security summary

The specifics of ensuring (and maintaining) attack-resistant systems are the domain of technical security. This is considered "technical" because of the specificity (and technical nature) of the information that it includes.

Technical security should be considered the constantly changing filter that keeps impurities out of the system and catches them before they can escape the secured system.

Technical security responds to change as a situation requires; it is the first line of response to a threat. Like a cop on the beat -- it preserves and protects.

Section 7. Overview and summary

Overview and summary

Security is a lot like playing dodgeball. Stuff comes at you from all directions, and staying in the game depends on not letting it hit you.

The classifications we assign the different facets of security are only worthwhile if we can use them to better plan for and respond to problems. Whether efforts are focused on the physical, logistical, data, or technical facets of the security gem matters not if the end result fails to increase the system's ability to function and defend itself.

Security is never static, and must be able to change as circumstances dictate -- just like the dodgeball player.

Section 8. Feedback

Feedback

Please let us know whether this tutorial was helpful to you, and how we could make it better. We'd also like to hear about other tutorial topics you'd like to see covered.

Thanks!

Colophon

This tutorial was written entirely in XML, using the developerWorks Toot-O-Matic tutorial generator. The Toot-O-Matic tool is a short Java program that uses XSLT stylesheets to convert the XML source into a number of HTML pages, a zip file, JPEG heading graphics, and PDF files. Our ability to generate multiple text and binary formats from a single source file illustrates the power and flexibility of XML.