SECURITY TECHNIQUES HARDWARE pdf

1: News, Tips, and Advice for Technology Professionals - TechRepublic

Follow these tips to keep your computer's security tight. If this is your first visit, use these tips as a security checklist. Patch, Patch, PATCH!

Security in this context can refer to protection against malicious attack or unintended operation brought about by an external influence. It may relate to the reading of some secret data within a device by a non-authorized third party confidentiality or a change in device execution through an unintended input integrity. Whatever the effect, testing for hardware vulnerabilities is complex and error prone. While various mechanisms have been exploited to target software vulnerabilities, hardware security verification is relatively new and requires exhaustive code analysis. Modern semiconductor designs have been found vulnerable from invasive physical access for example, de-packaging or deep probe insertions and logical access for example, extracting information using misconfigured on-chip debug ports, scan paths, electromagnetic radiation or power consumption. With the growing complexity of modern SoCs operating multi-access software platforms, multiple stakeholders with mixed trust levels share often resources on the same SoC. Providing this functionality while also maintaining platform integrity is often the core issue for security systems and their verification. A few examples of common vulnerabilities might include: Unauthorized access of protected assets e. Violation of a protected memory range by non-privileged software or Untrusted Direct Memory Access DMA by a rogue DMA controller Overriding register or cache security by non-privileged software Timing of operations to discern root keys Denial of service to shared hardware resources Extraction of information through analysis of power rails side channel analysis Reading of internal data through the device scan path For many of these situations, the general verification approach is to identify the vulnerable area and its trusted accessibility options and then to ensure, in an exhaustive fashion, that no other access mechanisms exist. An easy example is a protected key within a device that should be read in an encrypted form when addressed through one specific output port. This detail needs to be specified and the design analyzed for sources of vulnerability. Then a full verification of the design, to see if the key may be accessed through any of these vulnerabilities, needs to take place. Formal techniques are particularly good at tracking signals exhaustively through a design, and understanding all the possible paths a signal might take. It is also easy with Formal to simply ask the question of the form: Formal is an ideal technology for this purpose and, not surprisingly, security solutions are emerging that leverage formal platforms. Some of these security solutions make use of data tagging techniques and, indeed, it is possible for a Formal knowledgeable engineer to create a small set of security properties that can tag a security key held in a specific register and then check that there is no unexpected leakage of information of the key to any output. Leakage can occur, for example, through a specialized debug interface, by a memory read for software access, or down a scan path in an unexpected fashion. Of course security experts can create a more refined set of security properties based on methods used to attack a device, and their knowledge is invaluable when looking for new methods in which a chip may be hacked. They have written a white paper that gets into more detail on how to tackle these kinds of issues.

2: 7 Security Measures to Protect Your Servers | DigitalOcean

Technology Security Tips: Hardware Desktop Computers. Screen Saver Password. The first step in protecting your desktop computer is to up a screen saver password.

You are not alone. Data security is the leading concern for IT professionals when it comes to cloud computing. Services like Amazons EC2 are simply not equipped to address the security and privacy needs of data-sensitive organizations. When it comes to security, the importance of control over your environment cannot be overstated, and leads most IT professionals to adopt private cloud hosting over the public cloud. When comparing cloud options, here are 5 security tips to consider: Know where your data lives. Sure, firewalls and intrusion detection and prevention can keep out most intruders, and data encryption keeps the data safer, but how do you know where your data goes when you terminate your service or when the cloud provider goes out of business? Being able to point to a machine and say your data and only your data is on that machine, goes a long way in the security of your data in the cloud. Dedicated hardware is the key that allows for cloud computing services to pass the most stringent security guidelines. Always backup your data. One of the most overlooked aspects of cloud computing and one of the easiest way to increase the control of your data is to make sure that whatever happens, you have a secure backup of that data. This is more about securing your business than your actual data but provides the same type of peace of mind. We have seen big companies like T-Mobile lose its customers data, by not having a backup, leaving them with nothing. Make sure your data center takes security seriously. By knowing which server and data center your data is being stored at, you can probe them for all applicable security measures that are in place. Managed services can also add a great deal of benefit and expertise to making your applications, data, and business more resilient. Services like managed firewalls, antivirus, and intrusion detection are offered by reputable data center or cloud providers, and allow for increased security measures for managed servers. Get references from other clients. When in doubt, ask your cloud provider for client references that require stringent security measures. Financial, healthcare, insurance, or government organizations are a good start. Be sure to contact these references directly when possible to see what these companies are using the cloud services for, and the steps they have taken to secure their data. The only way to make sure something is secure is to test it. It is not uncommon for highly data-sensitive organizations to hire a skilled ethical-hacker to test their security provisions. Vulnerability scanning and assessments are just as important inside the cloud as they are outside the cloud. Chances are that if you can find a way to get unauthorized access to your data, someone else can as well. Conclusion Achieving sufficient security assurances in the cloud is possible but it is not guaranteed. Just like any other IT project, you have to do your homework and in the case of security, it is better to be safe than sorry. The private cloud hosting model can certainly provide a more secure framework than the public clouds.

3: Computer security - Wikipedia

Hardware-based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography by Roger R. Dube Stay ahead with the world's most comprehensive technology and business learning platform.

Desktop Computers Screen Saver Password The first step in protecting your desktop computer is to up a screen saver password. Password protecting the Windows screen saver is "locking" the desktop. When you step away from your desk, the computer is locked or logged off. To set a screen saver password: Right click on the desktop. Make sure to miss any icons. Select the Screen Saver tab. Select a screen saver from the drop-down list. Check On Resume, Password Protect. Make sure the wait time is no more than 10 minutes. An easy way to turn on the screen saver is the Windows Key â€" L. If you have any questions, contact the Technical Support Center. This is useful for malicious pop-ups because it allows you to close the window without clicking on the ad or the link. Deleting Files Deleting files may not be enough to protect data. When you upgrade to a new computer at home, make sure your old hard drive is properly wiped clean of old data. Simply deleting information from a computer hard drive does not necessarily get rid of it. Deleting it only frees up the space so it can be overwritten with new data. Unless the hard drive has been subject to an erasing utility or it has been physically removed from the computer and destroyed, the likelihood is that someone could retrieve information from it. That can lead to data and identity theft. Laptops Never leave your laptop unattended. Utilize a security cable or similar device and attach it to a solid fixture, such as a desk. Never check your laptop as luggage. Consider using a backpack instead of the standard laptop case. If you have confidential data, consider storing the data on the network and access it through WebVPN. Handheld Devices Be careful before you resell or give away your handheld devices such as cellphones and PDAs. The new owner can uncover your data. At a minimum, figure out how to reset it to the factory standard. Refer to your manual or call the manufacturer for more information.

4: Top Ten Safe Computing Tips | Information Systems & Technology

Taking these into consideration, it is best to take control of your company's safety online with these 7 best Internet security tips in 1. Improve Security on the Hardware and Firmware Level.

The software security assurance process begins by identifying and categorizing the information that is to be contained in, or used by, the software. The information should be categorized according to its sensitivity. For example, in the lowest category, the impact of a security violation is minimal i. Once the information is categorized, security requirements can be developed. The security requirements should address access control , including network access and physical access; data management and data access; environmental controls power, air conditioning, etc. What causes software security problems? In most cases, these defects are created by two primary causes: Non-conformance, or a failure to satisfy requirements[edit] A non-conformance may be simpleâ€"the most common is a coding error or defectâ€"or more complex i. The important point about non-conformance is that verification and validation techniques are designed to detect them and security assurance techniques are designed to prevent them. Improvements in these methods, through a software security assurance program, can improve the security of software. Errors or omissions in software requirements[edit] The most serious security problems with software-based systems are those that develop when the software requirements are incorrect, inappropriate, or incomplete for the system situation. Unfortunately, errors or omissions in requirements are more difficult to identify. For example, the software may perform exactly as required under normal use, but the requirements may not correctly deal with some system state. When the system enters this problem state, unexpected and undesirable behavior may result. This type of problem cannot be handled within the software discipline; it results from a failure of the system and software engineering processes which developed and allocated the system requirements to the software. Software security assurance activities[edit] There are two basic types of Software Security Assurance activities. Some focus on ensuring that information processed by an information system is assigned a proper sensitivity category, and that the appropriate protection requirements have been developed and met in the system. Others focus on ensuring the control and protection of the software, as well as that of the software support tools and data. At a minimum, a software security assurance program should ensure that: A security evaluation has been performed for the software. Security requirements have been established for the software. Each software review, or audit, includes an evaluation of the security requirements. A configuration management and corrective action process is in place to provide security for the existing software and to ensure that any proposed changes do not inadvertently create security violations or vulnerabilities. Physical security for the software is adequate. Building in security[edit] Improving the software development process and building better software are ways to improve software security , by producing software with fewer defects and vulnerabilities. A first-order approach is to identify the critical software components that control security-related functions and pay special attention to them throughout the development and testing process. This approach helps to focus scarce security resources on the most critical areas. Tools and techniques[edit] There are many commercial off-the-shelf COTS software packages that are available to support software security assurance activities. However, before they are used, these tools must be carefully evaluated and their effectiveness must be assured. Common weaknesses enumeration[edit] One way to improve software security is to gain a better understanding of the most common weaknesses that can affect software security. With that in mind, there is a current community-based program called the Common Weaknesses Enumeration project, [2] which is sponsored by The Mitre Corporation to identify and describe such weaknesses. The list, which is currently in a very preliminary form, contains descriptions of common software weaknesses, faults, and flaws.

5: Top 5 Tips For Cloud Computing Security

Computer Systems Security is a class about the design and implementation of secure computer systems. Lectures cover threat models, attacks that compromise security, and techniques for achieving security, based on recent research papers.

Share to 7 Best Internet Security Tips In While advancement in technology is something that can be considered as a good thing, it has also breathed life into one of the scariest attacks any person or institution could ever encounter: Since the dawn of the cyber age, people, companies, and even government agencies have become vulnerable to virtual attacks. While these social media platforms have been trying to protect its integrity and reliability by giving their users a way to report these mishaps, it always seemed like things have a way of turning for the worse. Experts explained that there are three major factors that contribute to this kind of situation: Improve Security on the Hardware and Firmware Level The first thing you need to do to improve your Internet security is to secure your hardware and firmware. It is also expected to push these tech firms into prioritizing security more when it comes to their hardware offerings in the future. With that in mind, it may be good to update or replace your hardware altogether to stay safe this Increase Awareness About Cybersecurity Since human error is considered as one of the major factors that contribute to the problem of cyber attacks, limiting its occurrence is the best course of action for companies relying on the Internet for their transactions. This is because these companies tend to invest less in Internet security, making them an easy target. This way, ransomware, which lock digital content from its rightful owners and offer an unlock code in exchange for money, are rendered useless since companies have another copy of the data. Limit Accessibility Through the Least Privilege Mindset Limiting accessibility is also a good way to prevent leakage of important data. While there are many ways to do it, experts in Internet security strongly recommend establishing a culture where the privilege of access to information is granted only when required and after being approved. Under this culture, computers assigned to end-users are configured in a way that they can only make use of a default profile with limited privilege. In the same manner, computers assigned to IT or admin personnel are given super-privilege with full control over end-user PCs. Through this, administrators can prevent malicious applications from being run in the least privileged computers through remote tools and commands. Enhance Management of Identity Access Improving identity access is also advised for companies to improve their Internet security in as it prevents inadvertent leakage through the cloud and mobile technologies. For years, a firewall has been built by companies to protect sensitive information from getting accessed through wired networks. However, the emergence of cloud access has made it difficult for firms to set these parameters, which is why experts recommend strengthening the identification system. Do Constant Monitoring After applying all the tips mentioned above, some people might think they can rest easy. This should not be the case as malicious hackers are constantly working on a way to gain access to valuable information that can be exchanged for money. To do so, you should also establish metrics that determine when it is time to employ your recovery and a backup plan.

6: Protecting Devices | Information Systems & Technology

Overview of Network Security Products and Capabilities Page 3 Shifting from Software to Hardware for Network Security February Altera, now part of Intel.

Vulnerability computing A vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures CVE database. An exploitable vulnerability is one for which at least one working attack or " exploit" exists. To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below: Backdoor[edit] A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Denial-of-service attacks[edit] Denial of service attacks DoS are designed to make a machine or network resource unavailable to its intended users. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service DDoS attacks are possible, where the attack comes from a large number of points â€" and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet , but a range of other techniques are possible including reflection and amplification attacks , where innocent systems are fooled into sending traffic to the victim. Direct-access attacks[edit] An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms , keyloggers , covert listening devices or using wireless mice. Disk encryption and Trusted Platform Module are designed to prevent these attacks. Eavesdropping[edit] Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. Even machines that operate as a closed system i. Multivector, polymorphic attacks[edit] Surfacing in , a new class of multi-vector, [7] polymorphic [8] cyber threats surfaced that combined several types of attacks and changed form to avoid cybersecurity controls as they spread. These threats have been classified as fifth generation cyberattacks. Privilege escalation[edit] Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to " become root " and have full unrestricted access to a system. Social engineering security Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. Spoofing attack Spoofing is the act of masquerading as a valid entity through falsification of data such as an IP address or username , in order to gain access to information or resources that one is otherwise unauthorized to obtain. Email spoofing , where an attacker forges the sending From, or source address of an email. IP address spoofing , where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system. Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers [17] are examples. Incident Response Planning and Organization[edit] Incident response is an organized approach to addressing and managing the aftermath of a computer security incident or compromise with the goal of preventing a breach or thwarting a cyberattack. An incident that is not identified and managed at the time of intrusion, typically escalates to a more impactful event such as a data breach or system failure. The intended outcome of a computer security incident response plan is to limit damage and reduce recovery time and costs. Responding to compromises quickly can mitigate exploited vulnerabilities, restore services and processes and minimize impact and losses. Without a documented plan in place, an organization may not successfully detect an intrusion or compromise and stakeholders may not understand their roles, processes and procedures during an escalation, slowing the organizations response and resolution. There are four key components of a computer security incident response plan: Isolating affected systems to prevent escalation and limit impact, pinpointing the genesis of the incident, removing malware, affected systems and bad actors from the environment and restoring systems and data when a threat no longer remains Post Incident Activity: Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation. Clustering[definition needed] people is helpful to achieve it. Commitment of the management Courses for all organizational members Commitment of the employees [22] Systems at risk[edit] The growth in the number of computer systems, and the increasing reliance upon them of individuals, businesses, industries and governments means that there are an increasing number of systems at risk. Financial systems[edit] The computer systems of financial regulators and financial institutions like the U. Securities and Exchange Commission , SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illicit gains. Utilities and industrial equipment[edit] Computers control functions at many utilities, including coordination of telecommunications , the power grid , nuclear power plants , and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable. In , the Computer Emergency Readiness Team , a division of the Department of Homeland Security , investigated 79 hacking incidents at energy companies. The consequences of a successful attack range from loss of confidentiality to loss of system integrity, air traffic control outages, loss of aircraft, and even loss of life. Consumer devices[edit] Desktop computers and laptops are commonly targeted to gather passwords or financial account information, or to construct a botnet to attack another target. Smartphones , tablet computers , smart watches , and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach. Many people believe the Russian government played a major role in the US presidential election of by using Twitter and Facebook to affect the results of the election. Additionally, connected cars may use WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network. All of these systems carry some security risk, and such issues have gained wide attention. Internet of things and physical vulnerabilities[edit] The Internet of things IoT is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics , software , sensors , and network connectivity that enables them to collect and exchange data [67] â€” and concerns have been raised that this is being developed without appropriate consideration of the security challenges involved. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical rather than simply virtual threat. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks.

7: Computer Systems Security | Electrical Engineering and Computer Science | MIT OpenCourseWare

The security of computer hardware and its components is also necessary for the overall protection of data. If a stand-alone system contains some important or classified information, it should be kept under constant surveillance.

Usually, these devices also connect to the Internet. Computers running on the Windows operating system are more at risk of security invasions than Mac computers. Other devices that can comprise a home network include routers , firewalls , cable or DSL modems, printers, video game consoles, smartphones and voice over Internet protocol VoIP phones. Depending upon the protocols you use, you may have even more devices linked to your network. For example, Bluetooth gadgets can sync with each other when they come within range of the network. From a security standpoint, the pieces of hardware that will help provide security are firewalls and routers. Firewalls come in two varieties: You can purchase a physical firewall device or run a firewall application. Many routers have firewall software built into them. Firewalls act like filters. They help you monitor data traffic between your network and the Internet. Most firewalls have several security settings to choose from. The most restrictive settings are generally the safest, but they also limit your options. Most firewalls will allow you to create a list of Web addresses that are off limits. If you use a wireless router, you should make sure you set a password and enable encryption. Unprotected wireless networks are a bad idea. Enabling encryption and choosing a strong router administrator password are two steps that will help keep your network secure. You should pick passwords that are hard to guess. A string of letters, numbers and other characters is best. And resist the temptation to use the same password for all of your hardware and services.

8: 7 Best Internet Security Tips In | www.enganchecubano.com

Installing professional alarm hardware is easy, but programming the system can be a challenge. A battery-powered wireless DIY alarm system requires no wiring. Just plug the control box into your Internet router, mount the sensors and arming station, and program the unit with your computer.

Justin Ellingwood Introduction When setting up infrastructure, getting your applications up and running will often be your primary concern. However, making your applications to function correctly without addressing the security needs of your infrastructure could have devastating consequences down the line. In this guide, we will talk about some basic security practices that are best to configure before or as you set up your applications. A private and public key pair are created prior to authentication. The private key is kept secret and secure by the user, while the public key can be shared with anyone. When the user connects to the server, the server will ask for proof that the client has the associated private key. The SSH client will use the private key to respond in a way that proves ownership of the private key. The server will then let the client connect without a password. To learn more about how SSH keys work, check out our article here. How Do They Enhance Security? With SSH, any kind of authentication, including password authentication, is completely encrypted. However, when password-based logins are allowed, malicious users can repeatedly attempt to access the server. With modern computing power, it is possible to gain entry to a server by automating these attempts and trying combination after combination until the right password is found. Setting up SSH key authentication allows you to disable password-based authentication. SSH keys generally have many more bits of data than a password, meaning that there are significantly more possible combinations that an attacker would have to run through. Many SSH key algorithms are considered uncrackable by modern computing hardware simply because they would require too much time to run through possible matches. How Difficult Is This to Implement? SSH keys are very easy to set up and are the recommended way to log into any Linux or Unix server environment remotely. A pair of SSH keys can be generated on your machine and you can transfer the public key to your servers within a few minutes. To learn about how to set up keys, follow this guide. If you still feel that you need password authentication, consider implementing a solution like fail2ban on your servers to limit password guesses. Firewalls A firewall is a piece of software or hardware that controls what services are exposed to the network. This means blocking or restricting access to every port except for those that should be publicly available. On a typical server, a number services may be running by default. These can be categorized into the following groups: Public services that can be accessed by anyone on the internet, often anonymously. A good example of this is a web server that might allow access to your site. Private services that should only be accessed by a select group of authorized accounts or from certain locations. An example of this may be a database control panel. Internal services that should be accessible only from within the server itself, without exposing the service to the outside world. For example, this may be a database that only accepts local connections. Firewalls can ensure that access to your software is restricted according to the categories above. Public services can be left open and available to everyone and private services can be restricted based on different criteria. Internal services can be made completely inaccessible to the outside world. For ports that are not being used, access is blocked entirely in most configurations. Firewalls are an essential part of any server configuration. A properly configured firewall will restrict access to everything except the specific services you need to remain open. Exposing only a few pieces of software reduces the attack surface of your server, limiting the components that are vulnerable to exploitation. There are many firewalls available for Linux systems, some of which have a steeper learning curve than others. A simple choice is the UFW firewall. Other options are to use iptables or the CSF firewall. VPNs and Private Networking Private networks are networks that are only available to certain servers or users. For example, DigitalOcean private networks enable isolated communication between servers in the same account or team within the same region. A VPN, or virtual private network, is a way to create secure connections between remote computers and present the connection as if it were a local private network. This provides a way to configure your services as if they were on a private network and connect remote servers over secure connections. Utilizing private instead of public networking for internal communication is almost always preferable given the choice between the two. However, since other users within the data center are able to access the same network, you still must implement additional measures to secure communication between your servers. Using a VPN is, effectively, a way to map out a private network that only your servers can see. Communication will be fully private and secure. Other applications can be configured to pass their traffic over the virtual interface that the VPN software exposes. This way, only services that are meant to be consumable by clients on the public internet need to be exposed on the public network. Keep in mind that data center-wide private networks share space with other servers that use the same network. As for VPN, the initial setup is a bit more involved, but the increased security is worth it for most use-cases. Each server on a VPN must have the shared security and configuration data needed to establish the secure connection installed and configured. After authentication, they can also be used to established encrypted communication. Establishing a certificate authority and managing certificates for your servers allows each entity within your infrastructure to validate the other members identity and encrypt their traffic. This can prevent man-in-the-middle attacks where an attacker imitates a server in your infrastructure to intercept traffic. Each server can be configured to trust a centralized certificate authority. Afterwards, any certificate that the authority signs can be implicitly trusted. Configuring a certificate authority and setting up the rest of the public key infrastructure can involve quite a bit of initial effort. Furthermore, managing certificates can create an additional administration burden when new certificates need to be created, signed, or revoked. For many users, implementing a full-fledged public key infrastructure will make more sense as their infrastructure needs grow. Securing communications between components using VPN may be a good stop gap measure until you reach a point where PKI is worth the extra administration costs. Service Auditing Up until now, we have discussed some technology that you can implement to improve your security. However, a big portion of security is analyzing your systems, understanding the available attack surfaces, and locking down the components as best as you can. Service auditing is a process of discovering what services are running on the servers in your infrastructure. Often, the default operating system is configured to run certain services at boot. Installing additional software can sometimes pull in dependencies that are also auto-started. Service auditing is a way of knowing what services are running on your system, which ports they are using for communication, and what protocols are accepted. This information can help you configure your firewall settings. How Does It Enhance Security? Servers start many processes for internal purposes and to handle external clients. Each of these represents an expanded attack surface for malicious users. The more services that you have running, the greater chance there is of a vulnerability existing in your accessible software. Once you have a good idea of what network services are running on your machine, you can begin to analyze these services. Some questions that you will want to ask yourself for each one are: Should this service be running? Should it be bound to a single IP? Are your firewall rules structured to allow legitimate traffic pass to this service? Are your firewall rules blocking traffic that is not legitimate? Do you have a method of receiving security alerts about vulnerabilities for each of these services? This type of service audit should be standard practice when configuring any new server in your infrastructure. Doing a basic service audit is incredibly simple. You can find out which services are listening to ports on each interface by using the netstat command. If the address is 0. File Auditing and Intrusion Detection Systems File auditing is the process of comparing the current system against a record of the files and file characteristics of your system when it is a known-good state. This is used to detect changes to the system that may have been authorized. An intrusion detection system, or IDS, is a piece of software that monitors a system or network for unauthorized activity. Many host-based IDS implementations use file auditing as a method of checking whether the system has changed. Similar to the above service-level auditing, if you are serious about ensuring a secure system, it is very useful to be able to perform file-level audits of your system. This can be done periodically by the administrator or as part of an automated processes in an IDS. These strategies are some of the only ways to be absolutely sure that your filesystem has not been altered by some user or process. For many reasons, intruders often wish to remain hidden so that they can continue to exploit the server for an extended period of time. They might replace binaries with compromised versions. Doing an audit of the filesystem will tell you if any of the files have been altered, allowing you to be confident in the integrity of your server environment. Implementing an IDS or conducting file audits can be quite an intensive process. It also makes day-to-day operations more involved. It complicates updating procedures as you will need to re-check the system prior to running updates and then recreate the baseline after running the update to catch changes to the software versions. You will also need to offload the reports to another location so that an intruder cannot alter the audit to cover their tracks.

9: Software security assurance - Wikipedia

Hardware-Based Computer Security Techniques to DefeatHackers includes a chapter devoted entirely to showing readershow they can implement the strategies and technologies www.enganchecubano.comy, it concludes with two examples of security systems putinto practice.

Check new design of our homepage! Types of Computer Security: Threats and Protection Techniques Computer security is one of the most important issues in organizations which cannot afford any kind of data loss. With a lot happening on the web, it becomes an utmost need to secure the content from loss and interception as there hovers a constant vision of malice to disrupt the web world security. Techspirited Staff Last Updated: Mar 19, Computer security is that branch of information technology which deals with the protection of data on a network or a stand-alone desktop. As every organization is dependent on computers, the technology of its security requires constant development. Here are the different types of computer security. Hardware Security Threat Even if the computer is not plugged into a network, a person can open its cabinet and gain access to the hard drives, steal them and misuse or destroy the data saved on them or, damage the device altogether. It is also necessary to remember that in case one dissembles his computer hardware, the risk of losing coverage of warranty becomes very high. Protection The security of computer hardware and its components is also necessary for the overall protection of data. If a stand-alone system contains some important or classified information, it should be kept under constant surveillance. Locking system for a desktop and a security chain for a laptop are basic security devices for your machine. Certain disk locks are available in various sizes, which control the removal of the CPU cover protecting internal components of the system. A disk lock guards all the internal access points located on the CPU and protects them. Software Security Network Security Computer networks are an integral part of any organization these days, as they facilitate the free flow of data and services to the authorized users. However, such networks also pose a security threat in case the data is classified and confidential, thus making network security a vital necessity. Threats As the data is available only for authorized users, it is possible for hackers to pretend to be one, by providing the correct user name and password. Computer network security can be disrupted or encroached in the following ways: Denial of Service Denial-of-service is meant to disable a computer or a network and can be executed with limited resources. It is one of the most common forms of attacks by hackers and can effectively disable the whole network of an organization. Denial of service attack makes a computer resource unavailable to its intended user. To carry out this kind of attack, hackers generally flood a network or the access routers with bogus traffic. They also make attempts to disrupt connections between two machines and prevent individuals from accessing a service. Trojan Horse Trojan horse is common and one of the most potential threats to computer security. They are malicious and security-breaking programs, disguised as something which is considered as non-malicious by the security software. They are a useful tool for hackers who try to break into private networks. Hackers generally attach Trojan horse to a file, which triggers a virus or remotely controlled software, giving the hacker complete control over the computer. Viruses and Worms Viruses and worms are well-known for their destructive nature and the property of replicating themselves. They are basically pieces of computer program codes, which are written by hackers and other computer geniuses. The interception generally takes place through simple eavesdropping done by a hacker. Firewall is a filter that prevents fraud websites from accessing your computer and damaging the data. However, a firewall is not a great option for securing the servers on the Internet because the main objective of a server is granting access to unknown users to connect to various web pages. Security Software Along with firewall, try installing a good anti-virus and security software to enhance the security level of your computer system. Data Security Threat Although uncommon, hardware malfunction can prove to be a major threat to your data in the computer. The life span of hard disks is always limited because of surrounding factors and this can amount to a severe loss of all your files saved on the disk, if there is no proper backup of those files made on any other system. Protection Keep Backup It is important to avoid data and information loss in case of hard disk crashes. The only solution is to regularly keep backups of all the data on other media such as magnetic tapes, CD-ROM, etc. It is a good practice to store the media off-site and in case of a disk crash, restore the information from the backup media onto the new disk. In case a backup media is not affordable, one should try to store the files on at least two different media devices. These media devices should be systematically kept at a place which is safe and secured, as the information contained may be confidential. People usually have backup for database files, spreadsheet files and large documents. As the technical constraints are always there, it is better to take regular backups, in order to avoid any loss of information. Clean-up Software Install a software program on your computer that will clear all the old, unused files and registry keys. It will also help to detect malware and save your computer from a severe damage caused by it. Keep your system in the loop of latest updates and security alerts or else, it will become vulnerable to security threats. It is important to keep a record of technical support consultants and software documentations, like manuals and guides to make them accessible to the staff members of the company.

SECURITY TECHNIQUES HARDWARE pdf

New Deal and its legacy Intermediate Russian grammar Nicholas pileggi wiseguy Around Worthington (OH) Ministry of Musicians The balancing imperative : human rights in conflict 1980 Standard Postage Stamp Catalogue United States (Scott, Volume 1) Elementary Duets, Op. 86 Ezelel saw de wheel way up in de middle o de air (1:1-28) Passages from the American Notebooks, Volume 2 Geometry with an introduction to cosmic topology Marvelous Country Neo-scholasticism and the misunderstanding of grace Forms for Field Use CD-ROM to accompany A Guide to Observation, Participation, and Reflection in the Clas Playbook for progressives Neatness Dont Count Henry Manney Frankfurt Am Main Graduate programs in the humanities arts social sciences Antioxidants and radicals 10. Extreme Republicanism Bible Essentials (Word Study) Theories of emotion in psychology Security in embedded systems ieee papers There cant be only one way Lange series pathology flash cards Mcgraw-Hills Chinese illustrated dictionary Terror and urban guerrillas; a study of tactics and documents. The Best American Science and Nature Writing 2002 (Best American (TM)) Hands off our school! American novel explication, 1969-1980 Puppy Mudge Loves His Blanket (Puppy Mudge) C programming absolute beginners guide third edition Women, seduction, and betrayal in biblical narrative Nine and a Half Mystics The saga of the Chouteaus of Oklahoma Pearson my world social studies grade 4 Introductory econometrics lecture notes The Warriors Bond (Tale of Einarinn) Value-Led Organizations Hand-book and directory of Napa, Lake, Sonoma and Mendocino counties