DOWNLOAD PDF NETWORKING SECURITY AND STANDARDS

Chapter 1 : Network Security Essentials: Applications and Standards, 6th Edition | InformIT

Brief Description: This standard describes the requirements for placement of assets on the campus network, access to the campus network, transport of data across the network, and management of the network against security threats.

Features Comprehensive up-to-date survey of cryptography, authentication, and digital signatures. Gives the students a solid yet concise overview of the fundamental algorithms and techniques underlying network security. Integrated, comprehensive, up-to-date coverage of Internet-based security tools and applications. This is the only book that provides this coverage. Unified, comprehensive treatment of mutual trust topics. Key management and user authentication are fundamental to the successful use of cryptographic services. This treatment gives the student a systematic and comprehensive understanding of the issues involved. Excellent collection of homework problems. Approximately problems reinforce material in the text and also introduce new concepts and techniques. Problems are included at the end of each chapter. Comprehensive, up-to-date coverage of IP Security. IPSec is one of the most complex, and one of the most important, new network security standards. This book gives a clear and detailed technical treatment of the topic. Comprehensive, up-to-date coverage of wireless network Security. The student gains an understanding of the importance of this topic. These are the two most important approaches to email security. The book gives the student an understanding of both schemes at a detailed, technical level. Comprehensive and unified discussion of intruders and viruses. The threats of intruders hackers and viruses are distinct, but there are also similarities. By treating the two in successive chapters and in a unified way, the student gains a greater understanding of both topics. Firewalls are an integral part of any network security capability. A Computerized Test Generator is provided. The book makes liberal use of figures and tables to clarify concepts. A list of key words, a recommended reading list, and recommended Web sites appear at the end of each chapter. A Glossary, a list of acronyms, and an up-to-date bibliography appear at the end of the book. An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and the author. Sign-up information for the mailing list is provided at the Companion Website. The Author Web site includes an additional set of homework problems, with solutions, that the student can access for self-study to help reinforce concepts. For username and password information, please contact your Pearson Representative. A chapter-by-chapter set of question that can be used by the instructor for quizzes or made available to the student for self-study. A set of slides covering all chapters, suitable for use in lecturing. Solutions to end-of-chapter Review Questions and Problems. Suggested project assignments for all of the project categories listed below. Figures and Tables Sample Reading and Report Assignments Programming Projects Link to online premium content Online Appendices Supporting Documents Projects For many instructors, an important component of a course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. This book provides unparalleled support in that area. The IRC not only includes guidance on how to assign and structure the projects, but also includes a set of suggested projects that covers a broad range of topics from the text: A series of research assignments that instruct the student to research a particular topic on the Internet and write a report. This exercise is designed to illuminate the key issues in intrusion detection and prevention. A broad range of topics that can be implemented in any suitable language on any platform. A series of projects that involve programming and experimenting with concepts from the book. A set of exercises to examine current infrastructure and practices of an existing organization. A set of suggested writing assignments, by chapter, designed to engage the student in a deep understanding of the topic and to reinforce their knowledge of hard facts and problem-solving techniques. A list of papers in the literature that can be assigned for the student to read and then write a short report. Student Resources Access to the Companion Website and access to the online premium content is located at www. Students must use the access card located in the front of the book to register and access the online premium content. If there is no access card, students can purchase access by going to www. The following content is available through the Companion Web site: To limit the size and cost of the book, three chapters of the book are provided in PDF format. There are numerous interesting topics that support material

found in the text but whose inclusion is not warranted in the printed text. A number of online appendices cover these topics for the interested student. Homework problems and solutions: To aid the student in understanding the material, a separate set of homework problems with solutions are available. These enable the students to test their understanding of the text. A number of papers from the professional literature, many hard to find, are provided for further reading. A variety of other useful documents are referenced in the text and provided online. New to this edition is a set of homework problems with solutions available on the Web site. Students can enhance their understanding of the material by working out the solutions to these problems and then checking their answers. An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. Links to important sites, organized according to the chapters of the book, so that the student can visit sites related to the material currently being studied to get up-to-date and supplementary information. Links to course pages by professors teaching from the book. This can give other instructors useful ideas. An errata sheet for the book is updated monthly as needed. A set of PowerPoint Lecture Slides for use in lecturing. A set of practice homework problems, with solutions.

Chapter 2 : Wireless Networking Standards - calendrierdelascience.com

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

Today, my colleague Chris and I will be talking to you about the ways that network security standards change and how that affects you and your apps. Unfortunately, all protocols age, and as they are in the public more attacks are found over time. Even worse, the algorithms upon which these standards rely have a built-in shelf life. That means that as they age and as computers get faster, those algorithms become vulnerable to attacks like collisions, factorization and brute force. When you hear about these scary attacks, you wonder what you can do to prevent your app from appearing in the press the next time a big attach happens. Chris will then give you an update on app transport security, which is a mechanism that you can use in your apps in order to ensure that best practices are enforced. You have to go through on a regular basis and make sure that your app is up to date. And to know what to change, you should be following standards bodies, academic research and industry best practices. If you are a developer or a library developer, you may be using a third-party library in your app. And those can be very risky. A library that you integrated three years ago is already out of date and maybe using weakened security. That means that your users are not getting the security that you want. We also make available App Transport Security, or ATS, in order for you to be able to enforce those best practices in your app, as long as you are avoiding ATS exceptions. Finally, when those attacks happen, before those attacks happen you have to remind your clients, investors and managers that it is worth the maintenance cost to update your app so that when the next attack happens you are not scrambling to remediate the problem wasting time and energy and money as your app appears in the press named as one of the bad apps. Specifically, in the area of encryption, cryptographic hashes, public keys, protocols, and revocation. In particular, RC 4 is vulnerable to an attack where the key is recoverable within as little as three days. So, now is the time to upgrade. Those will ensure that you have both the best encryption and can detect when that data has been modified. Speaking of modified data. As you know, cryptographic hashes are a mechanism that allows you to detect when the input data has been changed. A collision attack is where two different inputs produce the exact same output. We removed trust in all MD-5 signed certificates across our platforms in previous years. SHA-1 just recently had an attack. The Shouted attack was performed earlier this year, and so this is the freshest information. Instead, you should be using any of the SHA-2 family of hashes in order to get that best security and avoid these collision attacks. Public keys, as you know, are a mechanism that provides an identity, a sort of identity for you. Such that other people can verify that something you signed was signed by you and not someone else. And can be used to send you encrypted data that only you can decrypt with your private key. But unfortunately, RSA key sizes smaller than bits are vulnerable to factorization attacks. But the reality is even bit RSA key sizes are not good enough. And we expect that an attack on a bit RSA key is imminent. In order to avoid these removals and ensure that you have best security, you should be using RSA key sizes greater than or equal to bits, or any of the elliptic curves that are trusted on our platforms. Protocols, as you know, are the mechanism that you actually use to talk to servers. Unfortunately, some of these protocols are weak or provide no security in particular. That means that anyone listening in knows exactly that data. And so, you should be avoiding these when you configure your servers. We removed the use of SSL Version 3 back in fall of Chris will be talking more about that a little bit later. Revocation is the mechanism that clients use to verify the certificate and determine whether that certificate should be trusted in the event that a certificate is mishandled or missed issued. And of course, the worst thing you can do in the area of revocation is not check it. First, as usual, a server requests a certificate from a trusted third-party called a certificate authority. The server then uses that certificate to identify itself to clients connecting to it. The client, in order to verify that identity, then requests information as to the status of that certificate from the certificate authority. The certificate authority replies back with a signed message indicating the status of the certificate that the client is looking at. The client verifies that response and then uses that status to determine whether to continue the

connection to the server. But unfortunately, OCSP has some drawbacks. As you can see from that previous description It requires an additional network connection for every connection to the server. That means that your connections in your apps appear slower and none of us want that. Furthermore, OCSP is performed in the clear. That means that all of the traffic indicating which certificate the client wants checked is visible to anybody watching. And the reason that OCSP is performed in the clear is that it you would need it to establish a secure connection. So, if you had to establish a secure connection to get OCSP, you might end up in a circular problem. Since all that information is in the clear. Anyone who is listening can and find out what servers that client is connecting to. Furthermore, that third-party certificate authority can aggregate data as to which IP address is which clients are talking to which servers and sell that to anybody they want. These 2 drawbacks are the reason that we do not have OCSP enabled by default. As before, the server gets a certificate from the certificate authority. But before sending that certificate to a client, the server requests the OCSP response from the certificate authority. And when it gets that signed response back, the server verifies it and then sends it along with the certificate to the client. The client can then verify both the certificate and the revocation status simultaneously. We are aware that enabling OCSP in some of the open source server implementations does have drawbacks. But we, nonetheless, encourage you to fix those issues and to adopt OCSP in order to improve the security and the speed of your app. In particular, the malicious server just need omit the stapled OCSP response and the client will never know that that malicious server has a revoked certificate. And it starts with us. First, we gather information from certificate transparency logs. Certificate transparency logs or CT logs contain cryptographic proofs of the existence of a certificate. We use the information from the certificate transparency logs to find out about all of the certificates that are trusted on our platforms. And if you want to help us gather information about your certificates in your apps and your servers, you should verify that your certificates are logged to a CT log. With that information, we now know all of the certificate authorities that are trusted on our platforms. And from that information we can request all of the revocation information from those certificate authorities. We then gather all of that revocation information back. We aggregate it into a single efficient bundle, and then make it available to all of our clients. Those clients check in periodically with us to get that bundled revocation information, and use that latest status revocation information when checking server certificates that they are using. If the client hits a certificate that is listed there, the client will then perform OCSP. The client uses this to verify that the certificate really is revoked. So, we think this is a dramatic improvement on the existing state of revocation on our platforms. It has a dramatic improvement in the privacy compromise area. The bundle that we provide of revocation information is the same across all of our clients and all of our platforms. So, we never know which clients are connecting to which servers. Furthermore, only certificates that are in that list require the additional OCSP connection. So, only the limited set of certificates there risk that additional privacy compromise if your servers are not using OCSP Stapling. Another huge advantage is that the information is automatically updated. That means that the client always have that freshest revocation information available to them when making all of their connections and this means that you also get this for free. First we talked about encryption and using authenticated encryption ciphers in your servers and your apps. We talked about hashes and how to avoid collision attacks. We talked about public keys and using strong public keys that are not subject to factorization. We also talked about protocols and using the latest protocols like TLS 1. First, I announced that we would be removing trust in any SHA-1 signed certificate for connections to TLS servers across all of our platforms. I also announced that we would be removing trust in certificates using key sizes smaller than bit RSA, also in all TLS connections to servers. First, this does not affect root certificates. In particular, root certificates are not subject to the type of collision attacks that we are worried about with the SHA Also, we already removed all roots certificates using key sizes smaller than bits back in fall of These trust removals also do not affect enterprise distributed certificates through mobile device management or MDM. But we know that it takes time for enterprises and users to update all of their certificates and their infrastructures to use the latest algorithms. I promise that we will be removing trust in those certificates later on. So now is the time to start updating, not then. If you are in Safari, you see an error dialog that looks something like this. Because you may never connect to this server through Safari. The good news is that all certificate authorities

trusted on our platforms only issue certificates that are not subject to these removals and you can find a list of all of the root certificates that are trusted on our platforms at this link.

Chapter 3 : IT Security Standard: Network Security - Information Security - Cal Poly, San Luis Obispo

The Network Security Standard provides measures to prevent, detect, and correct network compromises. The standard is based on both new practices and best practices currently in use at RIT. Please consult the checklist or the standard below for a complete list of requirements.

Network Security Brief Description: This standard describes the requirements for placement of assets on the campus network, access to the campus network, transport of data across the network, and management of the network against security threats. These controls are determined based on the classification of the data, services provided and associated risk to the university if these assets were compromised. Controls established through policy and standards specific to computing devices on campus protect against vulnerabilities such as: Poor user practices e. The network security standard identifies requirements that enhance the protection against and detection of security threats. This standard follows the same principles. The campus network interface to the public network is configured to deny traffic inbound to the campus network by default and to allow inbound network traffic by exception following the ITS Firewall Pinhole request process. Asset placement on the network: This includes traffic in and out of the Critical Services Zone and between computing devices within the zone itself. It must also deny network traffic by default and allow network traffic by exception. All university and auxiliary organization owned assets must be registered using the IP Address Request with ITS Network Administration before connecting to the campus network. University and auxiliary organization owned assets connecting to the Trusted Asset Zone must comply with university configuration and maintenance standards. Access to the Cal Poly network must be authenticated at a user level with a unique identifier. Level 1 data must be transported across the campus network in accordance with the IT Security: Computing Devices standard for encryption. Network traffic in support of the management of networking devices must be logically segmented into a Network Management Zone. Access to the Network Management Zone is restricted to authorized devices used for Network Management purposes. Network traffic is monitored for unusual or unauthorized activities or conditions at interfaces with Critical Network Zones and the campus network border. Critical Asset Zone - A collection of High Risk Enterprise devices that are grouped together and segmented from the rest of the campus network via perimeter and access controls. Trusted Asset Zone - A collection of university or auxiliary owned assets connected to the campus network that are included in the scope of the IT Security: Public User Access Zone - A collection of non-university or non-auxiliary owned assets connected to the campus network on segments designated for assets not specifically configured or managed in accordance with the IT Security: Responsible for implementation and management of network based controls in association with this standard. Responsible for communicating to the campus appropriate connection points zones based on this standard. Communicates with application users the capability of the application to encrypt appropriate data when transported across the network. Responsible for updating device registration information following the university network asset review process. Computing Device Users Responsible for understanding that all university or auxiliary owned computing devices must be in compliance with university information security standards in order to connect to the network in a Trusted Asset Zone. Responsible for understanding that all non-university or non-auxiliary owned computing devices must be granted an exception before connecting to the network in a Trusted Asset Zone. Systems found in non-compliance with this standard may be removed from the network until they do comply. Related Procedures and Resources:

Chapter 4 : Communication and Network Security Standard | calendrierdelascience.com

*Networking Security and Standards [Weidong Kou] on calendrierdelascience.com *FREE* shipping on qualifying offers. Security is the science and technology of secure communications and resource protection from security violation such as unauthorized access and modification.*

History[edit] Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the s. TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organisations and citizens across Europe. The committee is looking in particular at the security of infrastructures, devices, services and protocols, as well as security tools and techniques to ensure security. It offers security advice and guidance to users, manufacturers and network and infrastructure operators. Its standards are freely available on-line. A principal work item effort is the production of a global cyber security ecosystem of standardization and other activities. The latest versions of BS is BS The certification once obtained lasts three years. Depending on the auditing organisation, no or some intermediate audits may be carried out during the three years. The measurement standards are used for the static program analysis of software, a software testing practice that identifies critical vulnerabilities in the code and architecture of a software system. The Automated Source Code Security standard is a measure of how easily an application can suffer unauthorized penetration which may result in stolen information, altered records, or other forms of malicious behavior. The Automated Source Code Reliability standard is a measure of the availability, fault tolerance, recoverability, and data integrity of an application. The Reliability standard measures the risk of potential application failures and the stability of an application when confronted with unexpected conditions. Standard of Good Practice[edit] Main article: The ISF continues to update the SoGP every two years with the exception of ; the latest version was published in Originally the Standard of Good Practice was a private document available only to ISF members, but the ISF has since made the full document available for sale to the general public. Upon identification of a new patch, entities are required to evaluate applicability of a patch and then complete mitigation or installation activities within 35 calendar days of completion of assessment of applicability. These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best-practice industry processes. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document. This document emphasizes the importance of self assessments as well as risk assessments. It allows many different software and hardware products to be integrated and tested in a secure way. The RFC provides a general and broad overview of information security including network security, incident response, or security policies. The document is very practical and focusing on day-to-day operations. This guidance applies to end-users i. Since , the committee has been developing a multi-part series of standards and technical reports on the subject of IACS security. They are also submitted to IEC for consideration as standards and specifications in the IEC series of international standards following the IEC standards development process. All ISA standards and technical reports are organized into four general categories called General, Policies and Procedures, System and Component. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model. The fourth category includes work products that describe the specific

product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products. The ISASecure scheme requires that all test tools be evaluated and approved to ensure the tools meet functional requirements necessary and sufficient to execute all required product tests and that test results will be consistent among the recognized tools. The certification labs must also meet ISO lab accreditation requirements to ensure consistent application of certification requirements and recognized tools. IEC [edit] The IEC cybersecurity standards are multi-industry standards listing cybersecurity protection methods and techniques. The comments are reviewed by various IEC committees where comments are discussed and changes are made as agreed upon. Each has defined their own scheme based upon the referenced standards and procedures which describes their test methods, surveillance audit policy, public documentation policies, and other specific aspects of their program. In the automation system market space most cybersecurity certifications have been done by exida. Global Accreditation and Recognition[edit] A global infrastructure has been established to ensure consistent evaluation per these standards. Certification Bodies are accredited to perform the auditing, assessment, and testing work by an Accreditation Body AB. There is often one national AB in each country. The IASME Governance standard was developed to enable businesses to achieve an accreditation similar to ISO but with reduced complexity, cost, and administrative overhead specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO The cost of the certification is progressively graduated based upon the employee population of the SME e. Some insurance companies reduce premiums for cybersecurity related coverage based upon the IASME certification. The ANPR aims to enhance the ability of large, interconnected financial services entities to prevent and recover from cyber attacks, and goes beyond existing requirements.

Chapter 5 : IoT Standards & Protocols Guide | Comparisons on Network, Wireless Comms, Security, Indus

Electronic messages traveling across the internet are under constant threat from data thieves, but new security standards created with the technical guidance of the National Institute of Standards and Technology (NIST) will reduce the risk of messages being intercepted or stolen. These standards.

Background[edit] Anyone within the geographical network range of an open, unencrypted wireless network can " sniff ", or capture and record, the traffic , gain unauthorized access to internal network resources as well as to the internet, and then use the information and resources to perform disruptive or illegal acts. Such security breaches have become important concerns for both enterprise and home networks. If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. However, lack of knowledge among users about the security issues inherent in setting up such systems often may allow others nearby access to the connection. The threat situation[edit] Main article: Computer security Wireless security is just an aspect of computer security; however, organizations may be particularly vulnerable to security breaches [4] caused by rogue access points. If an employee trusted entity brings in a wireless router and plugs it into an unsecured switchport, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer using an open USB port, they may create a breach in network security that would allow access to confidential materials. However, there are effective countermeasures like disabling open switchports during switch configuration and VLAN configuration to limit network access that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices. Threats and Vulnerabilites in an industrial M2M context[edit] Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e. M2M communication in industrial applications. Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. The air interface and link corruption risk[edit] There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level. Modes of unauthorized access[edit] The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply. Accidental association[edit] Violation of the security perimeter of a corporate network can come from a number of different methods and intents. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network. Accidental association is a case of wireless vulnerability called as "mis-association". Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks VPNs offer no barrier. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level. Ad hoc networks[edit] Ad hoc networks can pose a security threat. Ad hoc networks are defined as [peer to peer] networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security. Thus the user may not even know they have an unsecured

Ad hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. Even barcode readers , handheld PDAs , and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points. Identity theft MAC spoofing [edit] Identity theft or MAC spoofing occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires, [10] and the hacker can easily get around that hurdle. MAC filtering is effective only for small residential SOHO networks, since it provides protection only when the wireless device is "off the air". Anyone with an In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack. Man-in-the-middle attacks[edit] A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP Access Point. Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks. These cause legitimate users to not be able to get on the network and may even cause the network to crash. The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery. The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. For closed networks like home users and organizations the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. For commercial providers, hotspots , and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Another solution is to require the users to connect securely to a privileged network using VPN. Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However, there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. A wireless intrusion prevention system[edit] Main article: A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization.

DOWNLOAD PDF NETWORKING SECURITY AND STANDARDS

Chapter 6 : Wireless security - Wikipedia

Minimum security standards for devices attached to the UC Berkeley electronic communication network are linked to this document as Appendix A: (Minimum Standards for Security of Berkeley Campus Networked Devices). These standards change periodically.

Chapter 7 : Network Security Standard | RIT Information Security

The IEEE , a family of Smart Transducer Interface Standards, describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

Chapter 8 : ISO/IEC IT network security standard

The practice of proper deployment of the security standards has become the focus on risk mitigation in the use of wireless networking. This document will be reviewed by the Network and Security Committees in months to ensure that it reflects the current state of the art in wireless technologies.

Chapter 9 : Your Apps and Evolving Network Security Standards - WWDC - Videos - Apple Developer

Many standards and guideline documents have been developed in recent years to aid management in the area of information security. The two most important are ISO , which deals primarily with process security, and the Common Criteria, which deals primarily with product security.