Privacy policies

Many countries require organizations that collect personal information to publish a privacy policy that will outline how the company will handle and use this information. Find a copy of the privacy policy for an organization that has asked you to provide personal information. Does their policy address all of the principles discussed in the text? (Reference Section 18.3). Which areas are lacking?

Edward Jackson

3/14/2015 12:18:57 PM

Hospital Policies

The privacy policy I selected comes from Halifax Hospital. Halifax is a hospital where I worked in the IT department some four plus years. I was an employee, patient, and an advocate of the many services the hospital provided. Of course, I had never actually read through their privacy policy. So, I went to their web site, at halifaxhealth.org, and found their posted policies. The core privacy components included: Right to Access; Right to Amend or Correct; and, Right to an Accounting of Disclosures.

The Right to Access policy covered a patient's direct access to medical and billing information. Additionally, a patient can request any notes and images related to medical care, however (for some reason), a patient cannot request psychotherapy notes. Something I found interesting---under the Patient Access Section---is that the policy states that requests *can be denied* under certain circumstances, but, they do not say which circumstances would result in denied access (Halifax Health, 2015). That is a little odd if you ask me.

Under the Right to Amend or Correct, this policy allows to amend or change medical information that is wrong, when it concerns them. For a patient to change something, they must submit a request for change. Once again, however, the hospital may deny this request. There were four reasons stated that a request may be denied: (1) If the information, record, or file does not belong to the hospital (which makes sense); (2) Is not information the patient does not have access to (this one seemed a little odd to me); (3) Is not information kept by the hospital itself; and, (4) if the information requesting change is already up to date (this also sounds like a loophole). (Halifax Health, 2015)

Next, the Right to an Accounting of Disclosures allows the patient to request a list of places, companies, and organizations where the patient's information may have been sent to. A couple of caveats with this "list," is that it only goes back six years, and, the patient may be charge for the list (Halifax Health, 2015).

One major thing I thought was missing from all the policies were the laws. Nearly everything that was in the policies, has some state or federal law governing the patient's rights. For example, Sarbanes and Oxley (SOX) for the accounting information, and HIPAA, which covers the security of patient information, especially electronic records (Kim & Solomon, 2012, p. 9). While the policies are meant just to be a brief overview (there were links to more detailed policies), I did find the policies a little vague in areas---even for just a summary.

References

Halifax Health. (2015). Patient rights and responsibilities. Retrieved from http://www.halifaxhealth.org/patient-rights-responsibilities

Kim, D., & Solomon, M. (2012). *Fundamentals of information systems security*. Jones & Bartlett Learning, LLC.

Secure network client OS

All operating systems have a set of "kernel" code that contains the basic core of the operating system. The kernel code allows the user to control the hardware and many of the applications used by the computer. A number of "security kernels" have been designed that are intended to protect the operating system from unauthorized modification as well as controlling access to the OS and ensuring that the operating system functions correctly.

One obvious disadvantage to deploying an OS with a security kernel is that the security code incurs additional processing overhead. What other disadvantages and advantages might be involved? If considered as a client OS to be deployed across an organization, under what circumstances would the disadvantages of a security kernel be justified? Why?

Edward Jackson

3/14/2015 1:25:52 PM

The Kernel can be good

In my research, I learned that there are three main types of security; they are monolithic, microkernel, and hybrid. A monolithic kernel is a single program that performs all tasks (like in UNIX and BSD), whereas the microkernel and hybrid kernels perform more specialized roles (Fink, 2005). The microkernel, which is used in QNX and HURD, use hardware and software in a fundamental way, and employ the use of outside components to perform larger, more time-consuming tasks. For example, because the

microkernel focuses on fundamental operations, a message passing process handles requests between one server to the next. The advantage of this is reduced maintenance, easier software development (due to not requiring reboots), and if one kernel goes bad, it can be easily replaced with a mirror kernel (meaning, less system crashes) (Fink, 2005). Of course, the disadvantages are this kernel type is that it requires more system memory for processing, bugs are much harder to detect, it requires more outside components for processing, and because of all that, the whole process management can be more complicated, which is not good for developers and system administrators.

In hybrid kernels, like the Linux kernel, the kernel is built around the concept modularity, meaning, only the necessary components required can be loaded into memory and used to perform operations (Fink, 2005). This aides in the faster development time, as well as not requiring reboots. The issue with the hybrid kernel, is that modularity creates the need to design, manage, and secure multiple interfaces. This means, the more interfaces there are, the more chances for exploitation and bugs there may be. Thus, this is one reason why you hear about the Linux kernel being hacked quite often.

The main advantages of using a security kernel, in general, is that there is a layer of abstraction between the system and applications. This can mean less crashes, less reboots, faster development for applications, and quicker integration of both hardware and software. Of course, with the good, comes the bad. The main disadvantages include complexity in processes, possible bugs (which will be more difficult to track down), and maintaining and securing outside interfaces and components the kernel may interact with. One reason why implementing a security kernel is practical, despite its disadvantages, is if security is a major concern, and the company has the system admins and development teams to properly manage a security kernel. Updates and patches need to be regularly applied, systems need to be hardened, and employees need to continually update their security knowledge and skills. To me, I would use a Linux/Unix box if “up time” was paramount. Operating systems with security kernels tend to have more up time…this is due to the reduced reboots and application crashes (because applications can run in separate kernel processes).

References

Fink, Jay. (2005, October). Different kernel designs overview. Retrieved from http://www.systhread.net/texts/200510kdiff.php

Kim, D., & Solomon, M. (2012). *Fundamentals of information systems security*. Jones & Bartlett Learning, LLC.

Legal and Ethical Aspects, Internet Security, and Operating System Security

Just as much of this class discusses technical solutions to security problems, there are also legal and criminal consequences to malicious activities that protect organizations and their assets.

Please click the Overview button below for a brief summary of the concepts that are being covered in this unit.

Brief Overview of Unit 5

Various internet security protocols and standards are widely used to protect commerce and secure personal information on the internet.

All operating systems have security vulnerabilities, and each manages security functions a little differently. The broad feature set of Linux provides a wide exposure to attacks and vulnerabilities. By using the security controls inherent in Linux, as well as configuring applications and add-on packages carefully, you can create Linux systems with a high degree of security. Windows, which is the most popular operating system in the world, faces the majority of malicious activities. A variety of design challenges exist for Microsoft in its mission to secure Windows.

Outcomes

After completing this unit, you should be able to:

- Evaluate best practices in privacy.
- Critique root process security.
- Discuss attacks against a Web security protocol.

Course outcome(s) practiced in this unit:

IT541-5: Explain the return on investment of various security implementations

What do you have to do in this unit?

- Complete assigned Reading.
- Participate in Discussion.
- Complete unit Assignment.
- Participate in Seminar or complete Alternative Assignment.
- Read Overview.
- Complete Learning Activities.

Readings for Unit 5

Read the following chapters in *Computer Security: Principles and Practice*:

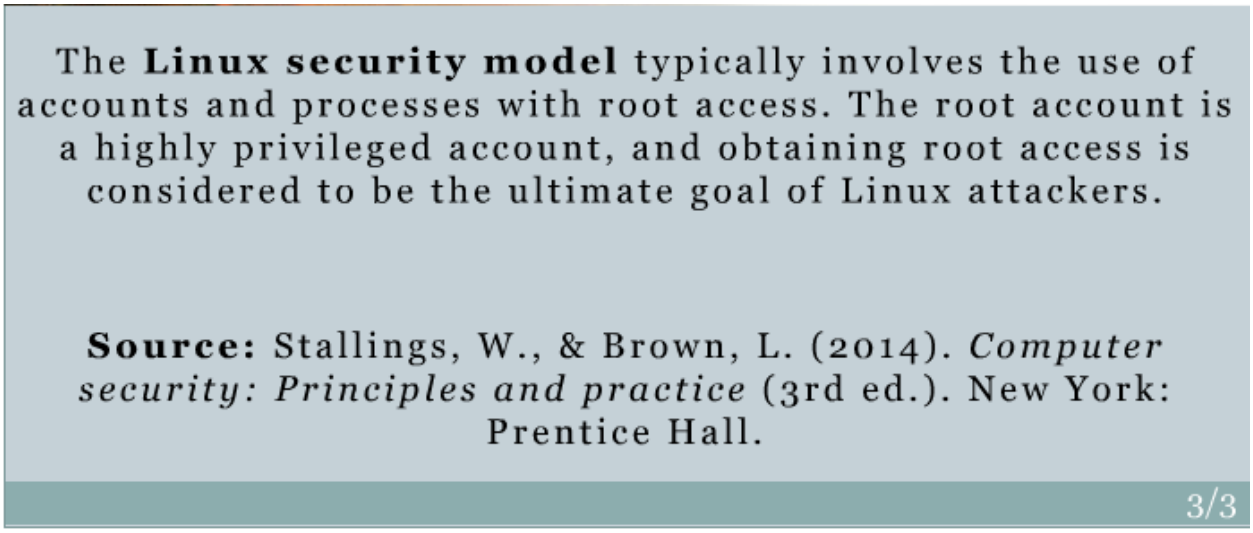
- Chapter 18: “Legal and Ethical Aspects”
- Chapter 21: “Internet Security Protocols and Standards”
- Chapter 22: “Internet Authentication Applications”
- Chapter 23: “Linux Security”
- Chapter 24: “Windows and Windows Vista Security”

Chapter 18 considers the ethics and legal areas of Computer Security. Chapter 21 presents several popular standards and protocols for providing secure use of the Internet. In Chapter 22 you will obtain an overview of Identity Management, PKI, and authentication protocols. Chapter 23 provides an overview of the security architecture used for the Linux operating system. Finally, Chapter 24 explains the Windows operating system security design.

ELITE
ESJ

In the process of protecting organizations, laws are put in place to identify and create consequences for criminal behavior.

Secure Sockets Layer (SSL) uses TCP to provide a reliable and secure end-to-end service. SSL uses two layers of protocols to ensure security. IPv4 and IPv6 require specific security precautions to work around inherent flaws in their initial designs. IPSec is a popular protocol for creating point-to-point VPN tunnels over IP.



Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allow you to come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

Option 1: Attend Seminar:

You are encouraged to attend the graded Seminar as an active participant. If you cannot attend, you may submit the alternative assignment to the unit Seminar Dropbox.

In this week's Seminar legal and ethical aspects of internet security and operating system security will be discussed.

Remember, if you do not participate in the weekly Seminar, you need to complete the alternative assignment.

Assignment 5

Outcomes addressed in this activity:

Unit Outcomes:

• Evaluate best practices in privacy.

• Critique root process security.

• Discuss attacks against a Web security protocol.

Course Outcomes:

IT541-5: Explain the return on investment of various security implementations.

Assignment Instructions

This Assignment provides a "hands on" element to your studies. It gives you the opportunity to work with the

procedures and see how they operate in real-world environments. Read and perform the lab entitled "IT 541

Assignment 5 Lab" found in Doc Sharing; use the lab sheet included at the end of the lab file to submit your

results.

Directions for Submitting Your Assignment:

Use the Lab #5 Worksheet document found at the back of the lab instructions as a guide for what to submit,

and save it as a Word document entitled Username-IT541 Assignment-Unit#.doc (Example: TAllen- IT541

Assignment-Unit5.doc). Submit your file by selecting the Unit 5: Assignment Dropbox by the end of Unit 5.

Assignment Requirements:

• Answers contain sufficient information to adequately answer the questions

• No spelling errors

• No grammar errors

*Two points will be deducted from your grade for each occurrence of not meeting these requirements.

For more information and examples of APA formatting, see the resources in Doc Sharing or visit the KU

Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and

discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity