Assignment1-Sol

Friday, February 1, 2019 06:21

A. Non-repudiation

[10 pts] What is non-repudiation in terms of computer security, and how does it relate to the C-I-A Triad?

Non-repudiation is the ability of a system to confirm that a sender cannot convincingly deny having sent something. It's importance is ensuring users cannot send malicious traffic and later deny it was them, which also means users are protected from impersonation. Relates to CIA by strengthening integrity guarantees in a network setting.

B. Vulnerability and Harms

[5 pts] Provide an example of a vulnerability in your home computer system.

Grader discretion, answer demonstrates the student understands what a vulnerability is. Answer should be something that is a vulnerability, not a control or an exploit to the system.

Examples:

No battery backup, unencrypted harddrives, weak Wi-Fi passwords, etc.

[5 pts] What harm might come if the vulnerability described above is exploited?

Answer should show the student knows what harm is. Example answers:

Data loss should power be cut with no battery backup, loss of confidentiality of data, intruders sniffing your Wi-Fi packets on your network.

C. Mechanisms

[10pts] Describe two example control mechanisms that might exist for an IoT device

Example Answers: Password protected access, Firewalls, movement sensors (to detect if someone is trying to take the device), biometric protections.

D. Vulnerabilities

[5pts] Find one recent (2017 or 2018) computer security attacks that have been reported in the media, and discuss the vulnerabilities that were the root cause of the attacks, and how we can prevent those attacks in the future.

Example Answer (Shivan Desai):

Equifax, an American credit company suffered a cyber-attack over the course of a few months. Detected in July of 2017, it contained the personal data of 143 million American, British and Canadiancustomers, as well as 200,000 credit card numbers. The vulnerability that attackers exploited to access Equifax's system was in the Apache Struts web-application software, a widely used enterprise platform. According to the official description of the bug, the software had incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header.

Even though the web-application is to be blamed for the massive attack, a fix to this specific bug was actually released two months before the attack actually took place.Equifax had two months to patch the software, but they ignored this issue until

they finally discovered the attack.

We can prevent similar attacks in the future by having better exception handling code, and validating the user input to prevent any suspicious activity.Even more important is to constantly look for and apply software patches for any 3rdparty software that the organization uses.

E. Classifying Policy Violations

(2 pts each) Classify each of the following as a violation of C-I-A, or of some combination thereof. Explain your answers in 1 to 2 sentences.

A student looks over the shoulder of another student during an exam.

C

Your pet cat pulls out the power cord to your computer.

A is the main, I can be argued for

Two students conspire to give each other better grades in a peer-graded assignment.

I is the main, C can be argued for (students know each other's grades now)

A user mis-types the recipient's email address and their sent email is bounced back to them.

A - recipient does not have access to data they should have received (email was not sent anywhere else, it bounced back to them).

F. Classifying Mechanisms

[10pts] Classify each of the following as a prevention, detection, or recovery mechanism:

A firewall is placed between a server-machine and it's connection to the Internet.

Firewalls are a prevention measure. Blocks unauthorized clients to a private network

Anti-virus running on a person's home computer/laptop.

Anti-viruses is an example of Detection/recovery. Anti-virus scans your computer for known viruses and dangerous files, and may attempt to remove them, recovering from the security breach. It can also contribute to prevention if you use it to scan files you download before running them.

[5pts extra credit] Provide an example for each of Prevention, Detection, and Recovery in which it is more important than the other two.

Example Answer (Credit: Ian Zanger):

Prevention may be most important in systems where errors cause grave consequences. Consider the system that is responsible for launching nuclear weapons. It is of dire consequences to prevent their misuse and only launch when absolutely meant to. This is more important than detection because it is quite obvious if they were to launch incorrectly.

Detection may be most important in situations with low stakes. Take your average business email, for example –it likely contains a message of little consequence, such as scheduling a meeting. If someone writes such an email and accidentally addresses it to the wrong person, this is a minor security breach. Since the contents of the email aren’t that sensitive, it’s not a major priority to prevent this sort of breach. Since emails are so easily sent and the accidental receiver can just ignore it, recovery is not an issue. What is important is detection –the user that sent the email would want to know that the intended recipient did not get it, sincethis could interfere with plans they are trying to make, such as a meeting.

Recovery may be most important in a situation such as a natural disaster. Consider a catastrophic tornado hitting a building that contains a company's servers, for example. There is no way to prevent the tornado itself. You could try to prevent damage from the tornado by building a solid building to house your servers, but this can be very expensive –and how likely is a tornado anyways? Detection is not a priority since such an event is well-publicized and employees will witness it. Recovery is most important. Disasters happen unpredictably, but as long as you have a backup of your data at another location, loss of data and money can be minimized.

G. Mechanisms

[10 pts] Joanna runs a very successful bakery, and wants to keep her secret cupcake recipe secret at all costs. She demands her bakers report any contact with her competition to her, even if it is only social contact. Will this have the desired effect? Why or why not?

The point of this question is to make the students think about how to deal with an insider threat. The scenario was slightly outrageous, but it highlights the difficulties in dealing with threats from inside an organization.