

Name:

Information Assurance: Homework 1 – Answer comments

4. Consider the following topics. You have 8 positive marks and an optional 8 negative marks that you can apply to these topics. We will touch on most of these topics this semester. Your feedback will influence the degree we go into these topics this and future semesters. For example, if you are very interested in Information warfare and Disaster recovery, you may split your positive marks between these two. If Hardware Security does not interest you, you may apply your negative marks to this topic. You should apply all positive marks. You do not need to apply negative marks.

The ordered list of topics and points is below. There was a fair variation in the point assignments. A few people were strongly opposed to the highest point total topic, perhaps because of the pejorative term of “Ethical hacking”. Certainly some people hide behind that term while doing some things they probably shouldn't. Most folks were at least mildly positive to the cryptography topic. The folks with more security experience were less interested in that topic. Security ethics was not much desired, I assume because many in the class have previously taken semester long ethics classes.

This list will help guide emphasis and some of the extra topics. Some of the lower valued topics will still be covered since they are elements of the core computer security cannon.

Ethical hacking and software vulnerabilities	51
Public Key Infrastructure and other network security protocols	43
Cryptographic theory and algorithms	40
Computer Forensics	37.5
Information Warfare	31
Security System Development Processes	29.5
Disaster Recovery	21.5
Hardware support for security	19.5
Computer security and the law	17.5
Database security	17.5
System Evaluation and Accreditation	15.5
Security of Critical Infrastructures such as Process Control or SCADA systems	5.5
Physical Security	-.75

Name:

EMSEC	-3.5
Security and Ethics	-6.5

5. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof. Briefly explain your reasoning.
- Mary forges Bob's name on a check.

Integrity, specifically origin or source integrity. Mary is misrepresenting herself as Bob. Some people tried to make an argument on confidentiality arguing that Mary was able to get physical access to the checks. I don't think that is a very strong argument. Others made an argument for availability, that Mary would write checks to make some money no longer available to Bob. That is a reasonable argument but a secondary effect of the integrity violation that enabled the withdrawal.

- Mary forges Bob's name on a check with his knowledge and permission.

Also, an integrity violation. Even if Mary is not tricking Bob, she is misrepresenting her identity to the bank.

- Larry incorrectly configures his scanning tool and ends up using 90% of the network bandwidth in his computer lab.

Availability violation. The network resources are no longer available to the rest of the lab users.

- Sara sniffs traffic to retrieve Anna's FTP account information.

Primarily this is a confidentiality violation. While the FTP protocol does not encrypt, Sara is going to some effort to access Anna's account information. Using the account information, Sara may go onto commit integrity and additional confidentiality violations by using Anna's FTP account.

- Margret's computer is infected via an unpatched OS bug causing her computer to run slowing and send out unauthorized traffic.

I was looking for availability violation here. Because of the infection, Margret no longer has access to her CPU resources. But people made reasonable arguments for confidentiality and integrity violations too. The infection presumably can access sensitive information on the system and can send it off. The infection can cause an integrity violation by change files on the system. It may also represent an origin integrity violation, if other systems assume that network traffic coming from Marget's machine is authorized by Marget. Some people made the argument that it is an integrity violation

Name:

because of the presence of the OS bug in the first place. This is true in the broad meaning of system integrity of trustworthiness, but it was not an active element in this scenario.

- f. Blaine registers the domain name goggle.com and other close typos of google.com, and he presents an interface similar to google's on these URL's.

Most people identified this as primarily an integrity violation. People are tricked into thinking that typed google.com correctly, and they are interacting with the real google site. This might lead onto violations of confidentiality with the users search information and perhaps more directly sensitive information being made available to Blaine. Some people also argued this was an availability violation against google. If they had access to the name variations, they could redirect people to the correct site.

6. Given the mechanism state (*the*) policy that could be enforced by this mechanism.

Several folks make simple restatements of the mechanisms. The policy should express the intent of implementing the mechanism. Some folks tried to identify the class of policy, but I was looking for a specific example policy. Each mechanism could have a number of policies. An example in each case is listed below.

- a. Parent of child enrolling in grade school must present two ID's showing current address.

Children must attend the school in their neighborhood.

- b. Credit card can only be activated by calling specified number from the home phone.

The credit card must be activated by the owner of the card.

- c. New passwords must be at least eight characters and include a combination of alphabetic and non-alphabetic characters.

The customer account must be protected by a strong password (difficult to guess).

7. Given the policy briefly outline an enforcing mechanism.

- a. Students should not copy other student's computer problem solutions.

Most people talked about file system protection mechanisms. Some gave procedure mechanisms such as forcing students to solve the problem in a lab without speaking. A few simple relied on a punishment mechanism of expulsion or failing if caught copying.

Name:

- b. Employees must not send personal email from their work addresses.

Again many people outlined a filtering scheme of black listing or white listing email addresses. One person suggested randomly selecting an email each day for each employee and mailing a copy to their boss.

- c. Company proprietary information must be protected from unauthorized access.

Most people outlined some sort of encryption and access control system.