CIS 4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 1/15/20

Homework 1

PROBLEM #1.1:

Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case indicate the degree of importance of the requirement.

SOLUTION:
Confidentiality: System must keep personal information private in the system and during transmission. If an attacker gains access to someones PIN number they could gain access to their account.
Integrity: Financial data can only be modified by supplying funds from another account or cash (withdraw or deposit). Editing financial information could be catastrophic for the bank, allowing an attacker to withdraw an infinite amount of funds.
Availability: Availability of the host is important, but individual teller machines is less so.

PROBLEM #1.2:

Repeat Problem 1.1 for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller.

SOLUTION:

Confidentiality: Company keeps call logs but users may not want others to know who they are calling however it is not crucial to keep private. Low security should be enough.
Integrity: Users should be assured that the number they are calling is actually routing to the correct number.
Availability: System should be available whenever someone tries to call a number.

PROBLEM #1.3:

Consider a desktop publishing system used to produce documents for various organizations.

a Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.

b Give an example of a type of publication in which data integrity is the most important requirement.

c Give an example in which system availability is the most important requirement.

SOLUTION:

a If system is publishing corporate proprietary information, the company will not want anyone else to have access to the documents.

b Laws and regulations need be be assured that they are valid and have not been tamped with.

c If system is publishing news then is should be available any time.

PROBLEM #1.4:

For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability and integrity respectively. Justify your answers.

a An organization managing public information on its Web server.

b A law enforcement organization managing extremely sensitive information.

c A financial organization managing routine administrative information (non privacy-related information).

d An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

e A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

SOLUTION:

a **Confidentiality:** Low, information is already public.
Integrity: Medium, if many people are looking at this information is should be correct. But it would not catastrophic if information was changed.
Availability: Medium, if a lot of people are using this web server, then it should be available as much as possible.

b **Confidentiality:** High, extremely sensitive data should only be able to be viewed by authorized users.
Integrity: High, if data was lost or modified it could impact investigations.
Availability: Medium, if system is unavailable, users would be unable to work.

c **Confidentiality:** Low, routine administrative information does not need a lot of protection.
Integrity: Medium, would not be a huge deal if this information was corrupted.
Availability: High, if the data is used frequently, then having it available when necessary is important.

d **Confidentiality:** Pre-solicitation data should be high priority level routine data less so.

Integrity: Pre-solicitation data should be medium as well as routine administrative data and the entire system,
Availability: Pre-solicitation data low, routine data medium, whole system medium.

e **Confidentiality:** Real-time data would not seem important to keep confidential, low, administrative data, medium, system medium.
Integrity: Modifying real-time data could lead to power failures throughout the military installation, high. Administrative data should be medium.
Availability: Real-time data should be available at all times by the SCADA system, or there could be power outages, high. Routine administrative data should be medium if the data is used often.

PROBLEM #1.5:

Consider the following general code for allowing access to a resource:

```
DWORD dwRet = isAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
     }
```

a Explain the security flaw in this program.

b Rewrite the code to avoid this flaw.
Hint: Consider the design principal of fail-safe defaults.

SOLUTION:

a The security flaw in this code comes from if the `isAccessAllowed()` function is unable to execute properly. Security check needs to proceed if there are no errors, not if it is equal to a single error.

b

```
DWORD dwRet = isAccessAllowed(...);
if (dwRet == NO_ERROR) {
    //Secure check OK.
    //Perform task.
} else {
    //Security check failed.
    //Inform user that access is denied.
}
```

PROBLEM #1.6:

Develop and attack tree for gaining access to the contents of a physical safe.

SOLUTION: