ComS 431
Homework 1

Sean Gordon

Aug 23, 2020

---

1)

A *threat* is what we are trying to protect against.
A *vulnerability* is a weakness or gap in our defenses.
A *risk* is the potential for loss or damages as a result of a *threat* exploting a *vulnerability*.

---

2)

(a)

Confideniality: The system must ensure the user's PIN is kept confidential from any passerbys or moderators of the ATM. This example is of high importance.
Integrity: The transactions done via the ATM system must preserve the bank account integrity. This example is of medium importance
Availability: The ATM machine itself must be physically available and operable to those that wish to use it. This example is of low importance

(b)

i. Confidentiality is affected here. To resolve this, the data could be encrypted before transfer.
ii. Non-repudiation is broken here. To resolve this, the ATM would remove the functionality to increase/decrease account monetary value.
iii. Integrity is affected here. To resolve this, the ATM would not allow transactions without stable internet connection.

---

3)

(a) If the call to IsAccessAllowed fails but the error is not of the same type as ERROR, the user will be allowed to continue.

(b) Rewritten Pseudocode to Avoid Security Flaw

```
DWORD dwRet = IsAccessAllowed(...);

if isNotError(dwRet) then
    // Security check OK.
else
    // Security check failed.
    //Inform user that access is denied.
end if
```
