

Information Assurance: Homework 7

Due November 15, 2005.

1. A vendor is trying to convince you of the trustworthiness of his system. He gives you a series of assurance evidence. For each piece of evidence, identify a concern (if any) you would have with that evidence.
 - a. First he tells you that product has been deployed in an Internet environment for 6 months and no breakins have been detected.
 - b. Then he tells you that they hired a penetration testing team and fixed all the problems that team found.
 - c. Then he tells you that they have passed Common Criteria evaluation for the LSPP profile at EAL 1.
 - d. Then he tells you that they have passed Common Criteria evaluation for the LSPP profile at EAL 6.

2. This question involves using Threat Modeling techniques to help design the security of an access control library called "A. Datum Access Control API". A data flow diagram (DFD) showing some of the interactions of key library components is shown on the next page.

Here are the two potential threat profiles for the API.

ID = 10

Name=Replace the list that maps users to constant ID's, with a new list file. By replacing the user list file, you could map an unprivileged user name to a privileged user ID.

STRIDE classification=Tampering, Spoofing

Mitigated=?

Entry points=User list file

Assets=Ability to change the evaluation of the access control policy.

ID=11

Name=Use non-standard path to trick API into granting access to user who should not have access. For example, using ".." to confuse the path parsing.

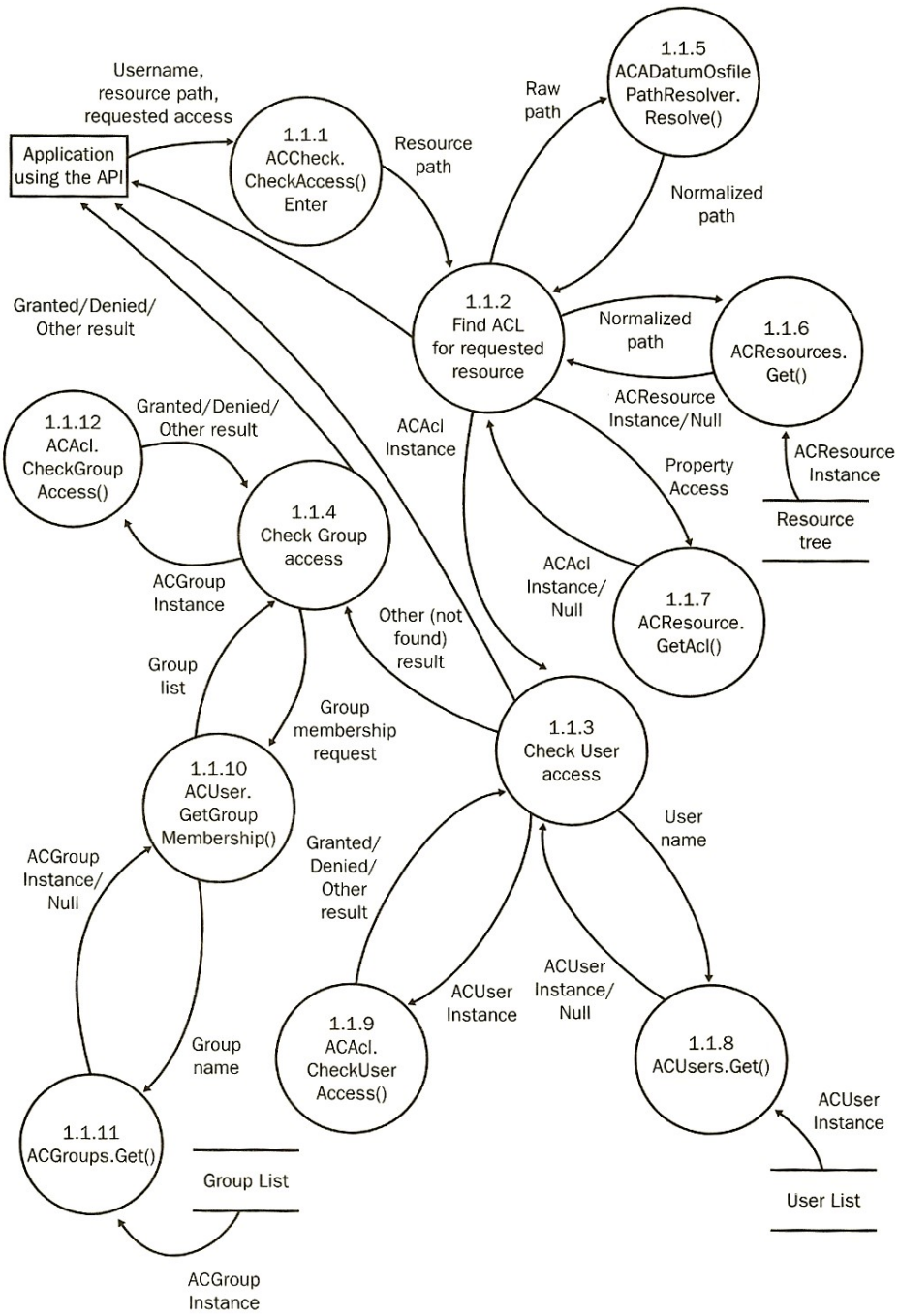
STRIDE classification=Information disclosure.

Mitigated=?

Entry points=1.1.1 ACCheck.CheckAccess()

Assets=Data protected by the access control policy.

- a. Write a threat tree for each threat profile
- b. Examine the DFD. Are the threats adequately mitigated now? If so now? If not, what could you change to mitigate?



3. This question works with the list of products evaluated by the Common Criteria <http://www.commoncriteriaportal.org/public/expert/index.php?menu=7>. In particular, you will be looking at products “IBM AIX 5L for POWER V 5.2, Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 “ and “Arbor Networks Peakflow X version 3.1.4”
 - a. Does the security target follow a protection profile (PP)? If so, what PP?
 - b. If it follows a PP, does it specify any additional security functional requirements? If so, list one of the additional requirements.
 - c. If it does not follow a PP, list two of the security functional requirements from the security target.
 - d. What EAL was the product was certified at?
 - e. Where there any extensions to a standard EAL? If so what?
 - f. What EAL was the PP (if any) certified at?
 - g. Which company was the sponsor for the certification?
 - h. What is the highest level certification you see in the list?