

Information Assurance: Homework 7 Answers and Notes

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.

There are many concerns with this claim. While it is nice that their product has been deployed "in the wild", the deployment environment is not really specified. What is the configuration? How widely was the service advertised? What it deployed behind firewalls or otherwise restricted? Beyond deployment, there are also concerns about how well the vendor is detecting break ins. It could be that an adversary has successfully breached the system without their detection.

- b. Then he tells you that they hired a penetration testing team and fixed all the problems that team found.

Bringing in a penetration test team is a step better. At least they likely have performed some form of systematic analysis, so you don't have to wonder whether anyone tried to attack the system. There are concerns here too. Have the fixes been tested? What are the biases of the particular pen test team? Did the penetration testing team share all of their results?

- c. Then he tells you that they have passed Common Criteria evaluation for the LSPP profile at EAL 1.

CC evaluation gives you a specific security target to examine, so you have a firm idea of what kind of security they are claiming. You will need to determine whether the requirements in a security target based on LSPP is appropriate for your needs. LSPP is very OS centric. If you are looking at a network-centric application, this may not be a valid target. In addition, EAL1 is only functional testing, and very minimal assurance. So you don't have much evidence that they security functionality claims are really what is going to happen.

- d. Then he tells you that they have passed Common Criteria evaluation for the LSPP profile at EAL 6.

Again we have the structure of the CC documentation, so you know what is being claimed. We have the same concerns that the PP is appropriate. With EAL6, we have much stronger assurance requirements, so we can have greater faith that the application will work as advertised. There might be some concern that EAL6 is too much. Meeting

EAL6 requirements will likely add to the cost of the product. If it is a critical application, this cost is most likely worth it.

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=?

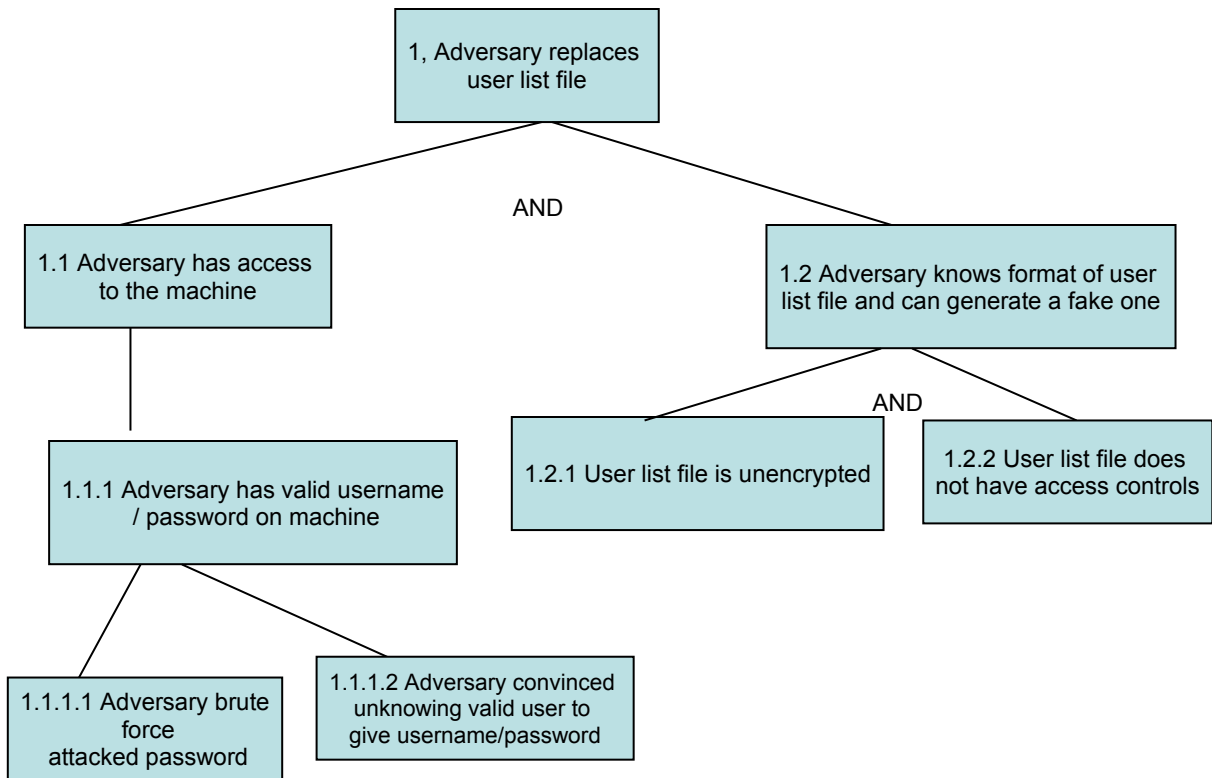
Entry points=1.1.1 ACCheck.CheckAccess()

Assets=Data protected by the access control policy.

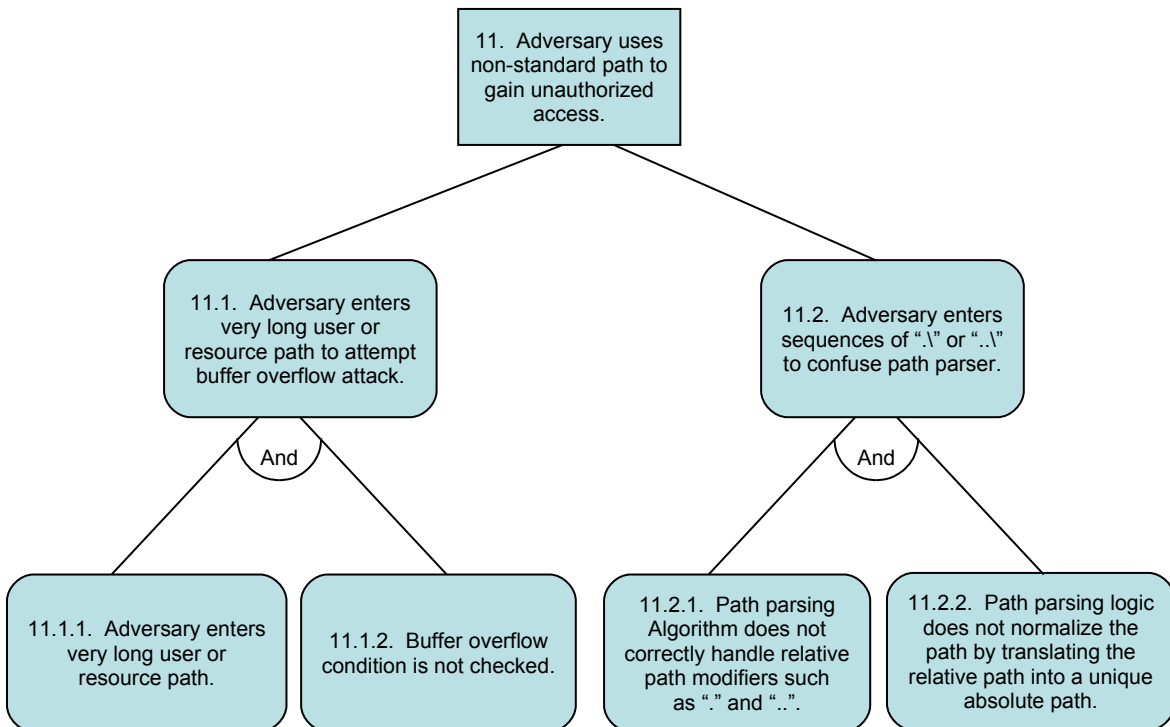
- a. Write a threat tree for each threat profile

Even with the DFD, you don't have enough information about the whole system to come up with a definitive analysis. So you will be making some assumptions about how things probably operate based on the DFD and your knowledge of how applications are generally configured on operating systems.

Tree for Threat ID=10 from Matt Stockton.



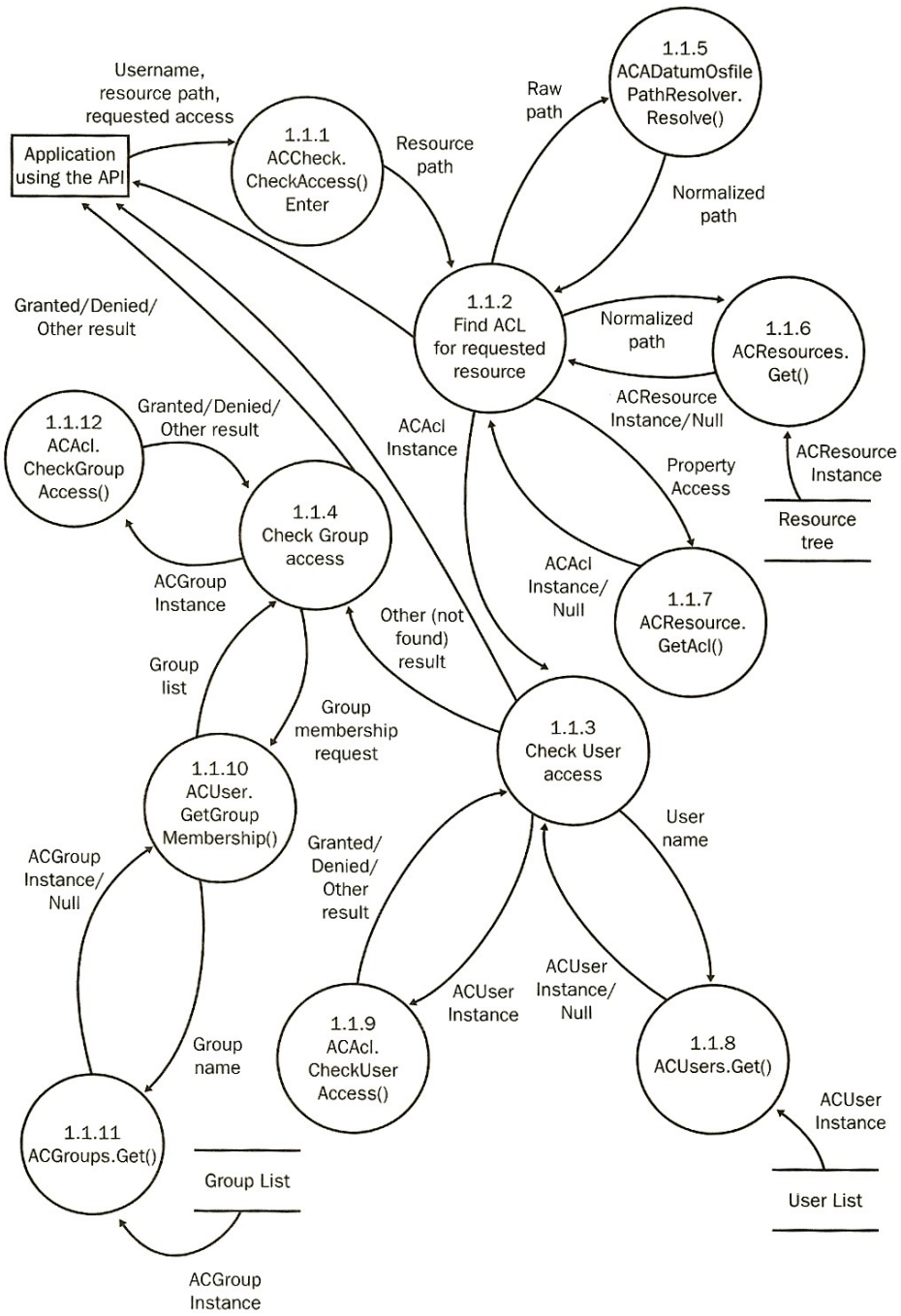
Tree for Threat ID=11 from Amit Srivastava.



- b. Examine the DFD. Are the threats adequately mitigated now? If so now? If not, what could you change to mitigate?

For threat ID=10, the DFD does not give us any information about whether the threat is mitigated. Without additional information, we must assume the worst. Since the tree has many and branches, there are really only two unique paths through the tree, and they only differ on how the attacker gains password information. So if we mitigate by encrypting the user list or correctly configuring the access control we should be good. Of course, if the attacker is able to gain high privilege access to pass through the access control or to find the key to decrypt the file, then the mitigations fail. Therefore, mitigating at several points along the path is a good idea (defense in depth). Some people also mentioned keeping a file hash to detect unexpected changes to the file.

For threat ID=11, DFD does give some indication that there is an attempt to mitigate the problem through the presence of module 1.1.5 the path resolver. However, the DFD does not indicate that path length is checked, so the left branch might be an unmitigated threat.



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?

The IBM security target follows the LSPP.

The Arbor Networks security target is not based on a protection profile.

- b. If it follows a PP, does it specify any additional security functional requirements? If so, list one of the additional requirements.

Table 5.2 in the IBM security target summarizes the security functional requirements and identifies where they came from. Section 5.1 talks about FDP_RIP.3 -AIX as an extension of the standard FDP_RIP family of requirements. In addition the table identifies several SFR's that are higher in the hierarchy. It also identifies some SFR's that come from CC rather than LSPP.

- c. If it does not follow a PP, list two of the security functional requirements from the security target.

From table 5.1 in the Peakflow X security target, we see a list of all the security functional requirements. Two specific requirements are FIA_ATD.1 and FMT_MOF.1.

- d. What EAL was the product was certified at?

The IBM product is evaluated at EAL4+.

The Arbor Networks product is evaluated at EAL2.

- e. Where there any extensions to a standard EAL? If so what?

In the IBM security target section 1.3, ALC_FLR.1 is identified as an augmentation to the standard EAL4.

Arbor Network's security target does not identify any extensions.

- f. What EAL was the PP (if any) certified at?

The LSPP is evaluated at EAL3.

- g. Which company was the sponsor for the certification?

IBM and Arbor Networks sponsored their own evaluations.

h. What is the highest level certification you see in the list?

There is one EAL7 evaluated product. Tenix Interactive Link Data Diode Device Version 2.1. Several people noted that the text says that the EAL hierarchy has only been specified in the CEM to EAL 4 or EAL 5. However, that information is several years old, and NIST is continually expanding the CEM. Last year the highest assurance level was EAL5+.