Name:

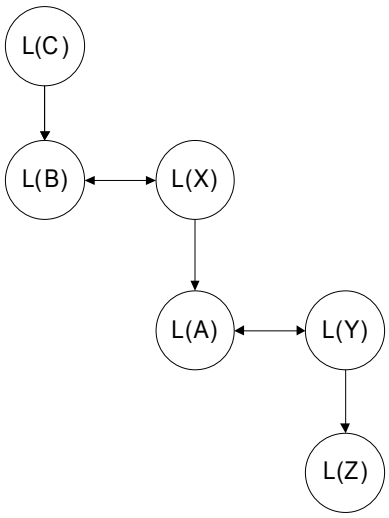
Information Assurance: Homework 6 – Comments

Due Nov 3, 2010

1. Consider the protection state defined by the following Access Control Matrix (ACM). Identify a set of security labels that could enforce the protection state in the ACM under the Bell-LaPadula (BLP) confidentiality model. Be sure to show the dominates relationship between the security labels you define.

	X	**Y**	**Z**
A	w	rw	r
B	rw	r	r
C	r	r	r

It turns out that this ACM can be represented by clearance level-only security labels. If you assume originally that each subject an object has it's own level, you can create a matrix based on the level relationships. Consider an arrow represents the dominates relationship. Then you can drop a dominates graph like



Then you can satisfy this relationship with 4 levels. e.g.,

- *L(C) = Highest*
- *L(B) = L(X) = High*
- *L(A) = L(Y) = Medium*
- *L(Z) = Low*

Where Highest > High > Medium > Low

Name:

Of course, this is a pretty simple case, so you might have just eyeballed the ACM and came up with a set of levels. However, it seems many did not understand the concept of security labels.

- *If they correctly defined the security 'clearance'/'level' (some additionally added categories which is fine if it is correct) of each subject (A,B,C) and object (X, Y, Z), and showed the DOM relationshipcorrectly , they got full points.*
- *Some did something like this : A{X,Y, etc} DOM B {X, Z, etc} . This is not a label.*
- *Some misunderstood the matrix by interpreting X,Y,Z as subject and A,B,C as object.*
- *```Some just defined the labels for subject or just the objects.*

2. This question works with the list of products evaluated by the Common Criteria http://www.commoncriteriaportal.org/products.html. In particular, you will be looking at products "**Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition**" and "**Cisco IOS IPSec on the Integrated Services Routers, VPN Services Module (VPNSM) and IPSec VPN Shared Port Adapted (SPA), incluiding VLAN Separation"**. For each of these products answer questions a – h.

For the Windows Product

a. Does the security target follow a protection profile (PP)? If so, what PP?

Controlled Access Protection Profile (CAPP).

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 security target identifies security requirements that do not come directly from CAPP.

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

N/A

d. What EAL was the product was certified at?

EAL4+

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

ALC_FLR.3 and AVA_VLA.3. Only one needs to be mentioned in the answer.

Name:

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

EAL3

g. Which country was the product certified in?

The certification report shows us that the product was evaluated using the US interpretation.

h. Which company (or companies) performed the evaluation?

SAIC did the evaluation.

For the Cisco product.

a. Does the security target follow a protection profile (PP)? If so, what PP?

N/A

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

N/A

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

The TOE Security Requirements Section of the Security Target describes all of the security requirements. Two of them are FAU_GEN.1 and FAU_SAR.1

d. What EAL was the product was certified at?

EAL4+

e. Where there any extensions to a standard EAL?

ALC_FLR.1 is identified in the Security Target and called out in the Common Criteria product table.

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

N/A

g. Which country was the product certified in?

The Certification Report shows that the product was evaluated under the US interpretation.

h. Which company (or companies) performed the evaluation?

Name:

ARCA Common Criteria Testing Laboratory

Answer the following question in general.

i. Would all the product certifications you examined in parts a-h be acceptable to the US Government?

In this case both products are evaluated under the US interpretation. Even if they were evaluated by labs in another Common Criteria country, the evaluation should still be valid.

j. What is the highest EAL evaluation you can find in the list? Give the name of one product evaluated at that EAL.

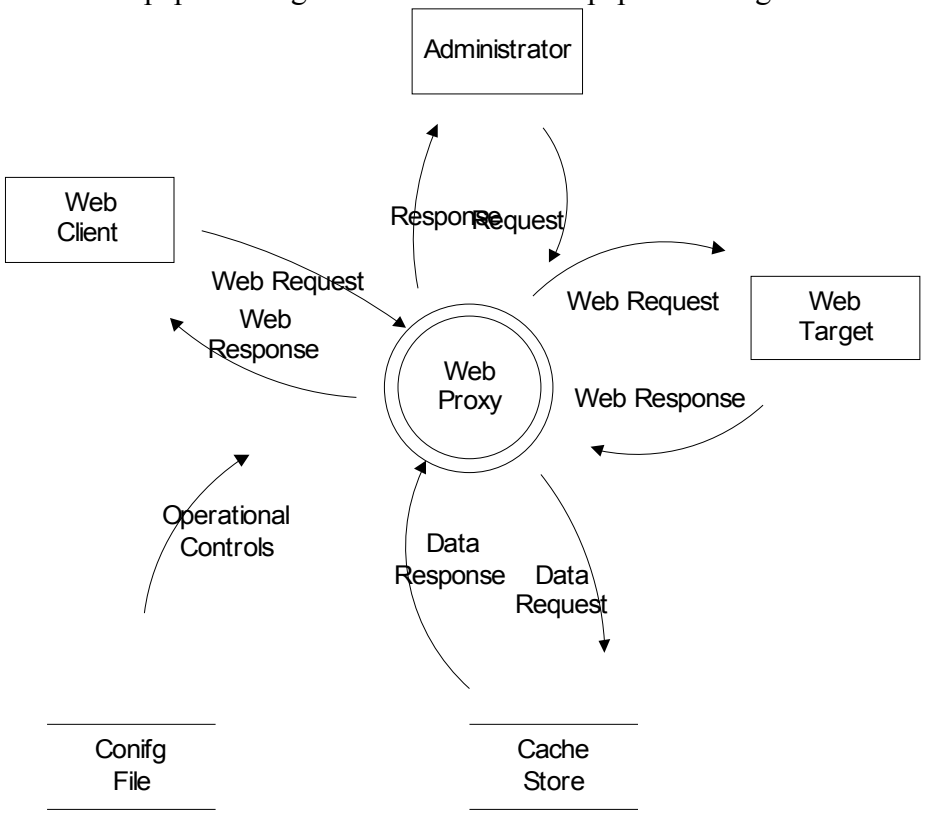
There is one product evaluated at EAL7+.
Tenix Interactive Link Data Diode Device, Gigabit Variant, Version 3.0

There are two products evaluated at EAL7.
Tenix Interactive Link Data Diode Device Version 2.1
Compucat Secure Optical Switch, part numbers 1105-0062-04 and 1105-0067-04

Name:

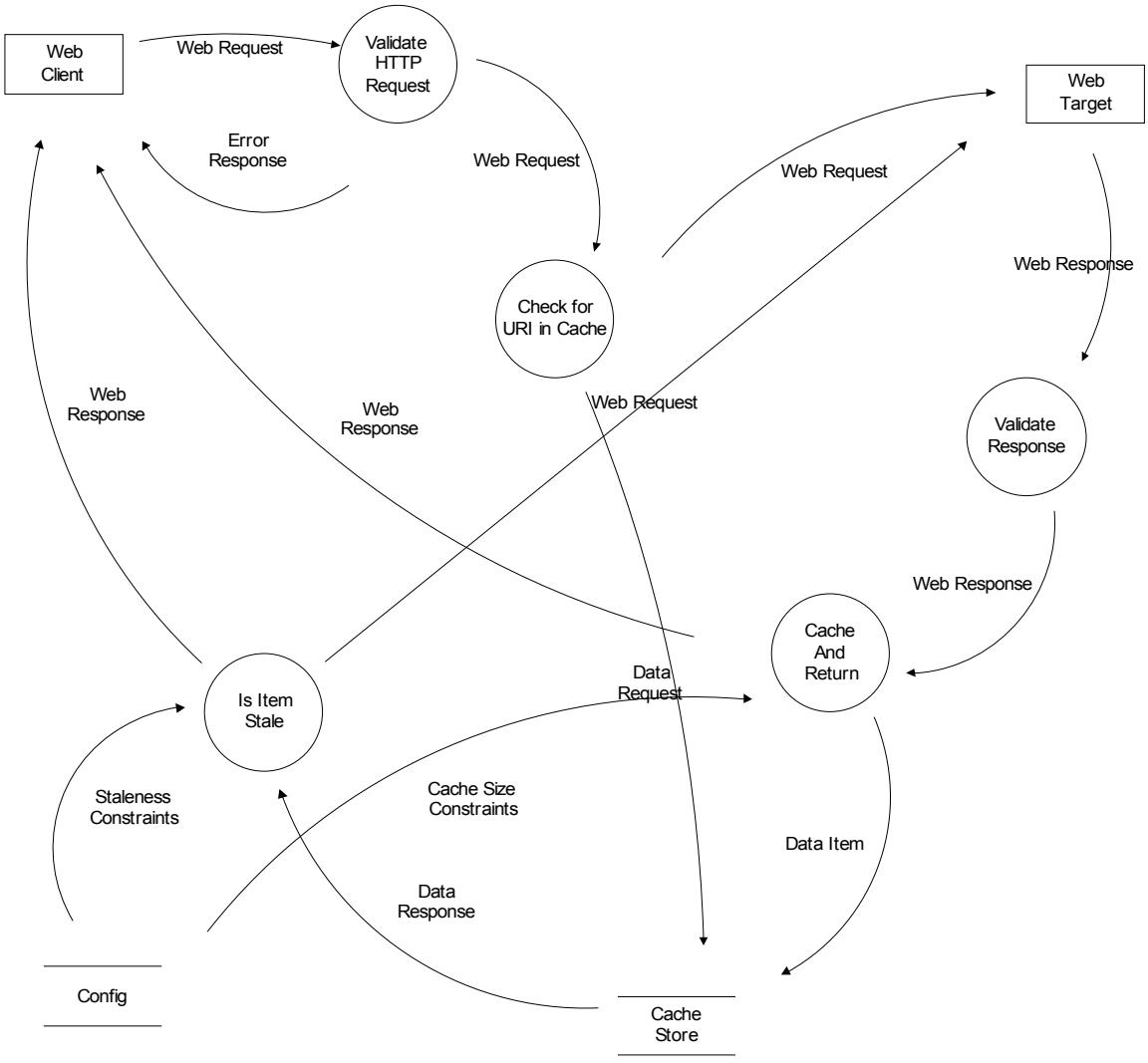
2. This question addresses the design of a web cache system. The web cache system intercepts HTTP requests. If the response has been previously cached, the cached response is returned. Otherwise, the request is passed onto the real target. The response is cached in addition to sending it onto the original requesting client.

a. The top level Data Flow Diagram (DFD) is shown below. Expand the multi-process node in this diagram one level. Use your best intuition on how a web cache process might be constructed. This next level DFD will still be relatively high level. You can submit this as a paper during class or as a scanned paper drawing.



There are many options for fleshing out the major steps of a web cache. The DFD below is one example. It highlights the major steps for validating requests and responses, checking for items in cache, and fetching items from the original target if they are not in cache.

Name:



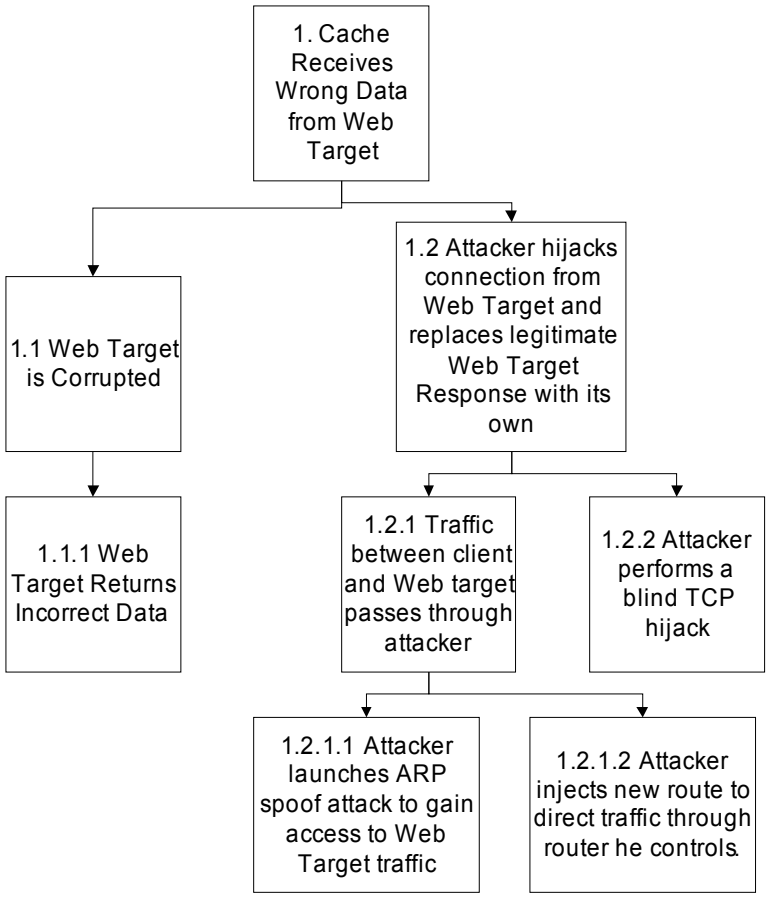
b. Identify two threats that could occur in this system. Be sure to label each threat according to the STRIDE criteria discussed in class and in the threat modeling reading.

Again, there are many possible threats. Here are two:

1. *Malicious client sends malformed URL with the goal of crashing or injecting his own code in the web cache process. From STRIDE, this threat follows Denial of Service (if long URL causes crash) or Elevation of Privilege (if it succeeds in remote execution).*
2. *Malicious server returns incorrect data in response to request. From STRIDE, this threat follows Tampering (returning wrong data) and Denial of Server (future requested for the cached data will get the wrong data).*

Name:

c. Create a threat tree to expand one of the threats identified in part b.



d. Identify a control that would mitigate at least one of the attack paths in the attack tree you created in part c.

Any of the paths that include the 1.2 node would be protected by using SSL to communicate with the web target.

Any of the paths that include the 1.2 node would also be protected if you had a hash or some other sort of finger print to validate the response.