Name:

Information Assurance: Homework 6 (updated question 1, fix DFD)

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

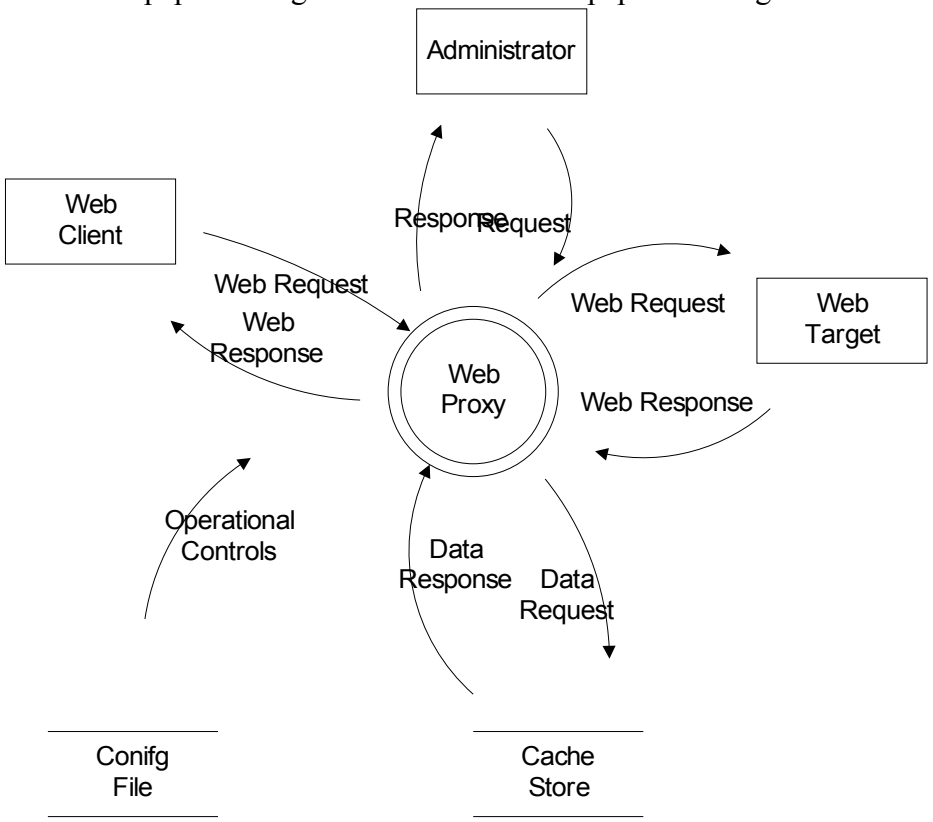
2. This question works with the list of products evaluated by the Common Criteria http://www.commoncriteriaportal.org/products.html. In particular, you will be looking at products "**Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 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.
    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 country was the product certified in?
    h. Which company (or companies) performed the evaluation?

    Answer the following question in general.
    i. Would all the product certifications you examined in parts a-h be acceptable to the US Government?
    j. What is the highest EAL evaluation you can find in the list? Give the name of one product evaluated at that EAL.

Name:

3. 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.



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.

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.