

Name:

## Information Assurance: Homework 5 Answers and Comments

Due October 17, 2007

1. Consider the Clark-Wilson and Biba strict integrity models.
  - a. What does Clark-Wilson provide that Biba does not?

*The Clark-Wilson model discusses certifying processes in addition to enforcement. It also directly addresses separation of duty.*

- b. What does Biba provide that Clark-Wilson does not?

*Clark-Wilson can be used to model a Biba scenario, so strictly speaking Biba adds nothing. However, the two models are very different stylistically. Biba's model provides a very compact set of rules for data access that could be layered on existing OS implementations.*

- c. If you were designing a high integrity system, which integrity model do you think would give you the best guidance and why?

*While you could argue either side of this, I would probably choose to think in terms of Clark-Wilson. The Clark-Wilson model addresses a bigger problem of how systems should be set up and maintained (with the certification rules) not just how access rules should be enforced once the system is up and running.*

2. If a trusted OS only provides weak tranquility, can we still say it implements a mandatory access control (MAC) policy? Why or why not?

*With weak tranquility, a trusted user or trusted program can change the levels of subjects and objects during the operation of the system. Strictly speaking this is still a mandatory system because non-privileged users are not changing the levels of subjects or objects. However, as in the case of users running within a clearance range, an unprivileged user may well be invoking the trusted program to change levels for him. If the implications of giving this control to the non-privileged user are not well thought out, the benefits of MAC may quickly be lost.*

*In an extreme case, assume you have a system that supports clearance ranges for subjects, and the system administrator gave all users very wide ranges (system high to system low). Say in this system, the users complained about having to invoke the trusted program to change level, so the system administrator rigged their environment to automatically run the level adjust program when their processes failed to access due to a MAC error. In this very extreme case, there is no real mandatory access control because the subjects levels change at will.*

Name:

*In a less extreme case, there are still restrictions on non-privileged users even if you given them some leeway to adjust level within a range. However, the system designer must carefully consider the implications of loosening the strict Bell-LaPadula model for their environment.*

3. Given the security levels:  $W > X > Y > Z$ , and the categories A, B, and C, specify the accesses allowed (read, pure-write or append, read-write) under the Bell-LaPadula model. Assume DAC allows all access.

- a. Andrew at  $W:\{\}$  and Document at  $Y:\{\}$

*SL(Andrew) dominates SL(document). Read is allowed.*

- b. Beverly at  $Y:\{A,B,C\}$  and Document at  $Z:\{B\}$

*SL(Beverly) dominates SL(document). Read is allowed.*

- c. Clarence at  $W:\{A,B\}$  and Document at  $Y:\{B,C\}$

*SL(Clarence) does not dominate SL(Document), and SL(Document) does not dominate SL(Clarence). No access is allowed.*

- d. Darrin at  $Y:\{A,C\}$  and Document at  $Y:\{A,C\}$

*SL(Darrin) dominates SL(document), and SL(Document) dominates SL(Darrin). Read and Write are allowed.*

- e. Eleanor at  $Z:\{\}$  and Document at  $W:\{C\}$

*SL(Document) dominates SL(Eleanor). Pure-Write or Append is allowed.*

4. Consider the access allowed with the labels above interpreted as integrity levels under the strict Biba integrity model.

- a. Andrew at  $W:\{\}$  and Document at  $Y:\{\}$

*IL(Andrew) dominates IL(Document). Pure Write or append is allowed.*

- b. Beverly at  $Y:\{A,B,C\}$  and Document at  $Z:\{B\}$

*IL(Beverly) dominates IL(Document). Pure Write or Append is allowed.*

- c. Clarence at  $W:\{A,B\}$  and Document at  $Y:\{B,C\}$

Name:

*IL(Clarence) does not dominate IL(Document), and IL(Document) does not dominate IL(Clarence). No access is allowed.*

d. Darrin at  $Y:\{A,C\}$  and Document at  $Y:\{A,C\}$

*IL(Darrin) dominates IL(Document), and IL(Document) dominates IL(Darrin). Read and Write are allowed.*

e. Eleanor at  $Z:\{\}$  and Document at  $W:\{C\}$

*IL(Document) dominates IL(Eleanor). Read is allowed*

5. This question works with the list of products evaluated by the Common Criteria <http://www.commoncriteriaportal.org/public/expert/index.php?menu=8>. In particular, you will be looking at products “Check Point VPN-1/FireWall-1 NGX “ and “IBM AIX 5L for POWER V5.3, Technology level 5300-05-02 with Argus Systems Group PitBull Foundation Suite 5.0 and optional IBM Virtual IO Server (VIOS) Version 1.3”

*First addressing Check Point VPN-1/FireWall-1 NGX*

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

*The security target identifies three protection profiles in Section 1.3.3.*

- *Intrusion Detection System System Protection Profile, Version 1.5, March 9, 2005*
- *U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 2000*
- *U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000*

*However, it says that it does not support the AVA\_VLA.3 feature required of the second two protection profiles, and it only claims conformance to the first protection profile. I looked in the Common Criteria Evaluation Methodology documents to find out what AVA\_VLA was. It turns out it was renamed to AVA\_VAN from version 2.x to 3.x. It is described in part 3 as a software assurance feature: AVA = vulnerability assessment and VLA/VAN = vulnerability analysis. However, the comment these being required for the protection profiles confused me. As an assurance feature, this should have only affected the EAL level.*

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

*The functionality requirements are described in section 5.1 of the security target. This section has a number of tables that map features to originating protection profiles or*

Name:

*other motivations. A number of features were added to support VPN requirements including*

*FDP\_UCT.1 = Basic Data Exchange Confidentiality.*

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

*N/A. Follows protection profiles.*

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

*EAL4+*

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

*Yes, section 5.2 of the security target discusses the assurance requirements. One extra assurance requirement is identified: ALC\_FLR.3 = Systematic Flaw Remediation.*

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

*All the protection profiles were evaluated at EAL2.*

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

*This is identified in the certification report. Check Point sponsored the certification.*

*Now addressing IBM AIX 5L for POWER V5.3, Technology level 5300-05-02 with Argus Systems Group PitBull Foundation Suite 5.0 and optional IBM Virtual IO Server (VIOS) Version 1.3.*

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

*LSPP*

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

*The security functional requirements are defined in section 5.2 of the security target. It looks like it follows the functionality requirements pretty closely. Some of the features it attributes to both LSPP and the common criteria part two. FDP\_RIP.3-AIX (hard disk drive residual information protection) is attributed to the ECD, but I don't know what the ECD is.*

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

*N/A follows protection profile.*

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

*EAL4+*

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

*Section 5.4 of the security target defines the security assurance features. It states that the EAL is extended by ALC\_FLR.1 = A defect handling procedure is in place.*

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

Name:

*EAL3*

g. Which company was the sponsor for the certification?

*This is indicated in the certification report as IBM Corporation.*

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

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

*Another Tenix product is also evaluated at EAL7.*