

CS 6238 Secure Computer Systems
Spring 2007
Homework 1
Due Date: 2/13/07

1. Microsoft claims that the new Vista operating system is the most secure system to date. On what basis can such a claim be made? In particular, consider the design principles in Schroeder and Saltzer paper and discuss how they may or may not have been applied to Vista design, implementation and deployment. Also, can the Vista vulnerabilities that have been reported recently be explained because certain principles were not followed? Explain your answer.
2. VMware is a popular virtualization system. Discuss if it can be classified as process-based or host-based or both? Is it hosted or host-less? How does it relate to the Xen virtual machine monitor?
3. The IA-64 architecture developed by Intel and HP also provides hardware support for isolating software systems similar to the SPL and PPL bits of the x-86 architecture. In this question, using the Web as a resource, explore the IA-64 architecture, discuss its hardware support for isolating software systems and compare it with x86.

Intel's virtualization technology

(<http://www.intel.com/technology/virtualization/index.htm>) was developed to better support virtualization. What additional support is provided VT for virtualization beyond the memory protection schemes of the x-86 and IA-64 architectures?

4. In the paper available at http://www.usenix.org/publications/library/proceedings/sec04/tech/full_papers/sailer/sailer.pdf, the authors explore an integrity measurement scheme and show how it can be used to detect root-kit attacks. What is a root-kit attack and how does the scheme detect such attacks. Explain the scheme described in the paper and discuss why it works (or when it may not work).
5. If the keystroke features provide sufficient entropy, users can choose an easy password like their login name. In particular, assume that the password for account a , pwd_a , is simply a . In this case, the entire entropy of the hardened password will come from the key stroke feature values. Would you implement this the same way as was discussed in class or there is a better way to implement it? How will you compute the entropy of such a scheme?