

COMP3441/9441 Tutorial Week 12

Security Architecture Issues

1. A client has come to your firm and wants to implement security monitoring, to respond to a finding of a security assessment recently conducted on their infrastructure. (If you attended last week's lecture, you may use one of the gateway solutions you designed in Exercise #1 or #2.) Design a security monitoring solution with the following features:
 - (a) Ability to detect intrusions or attacks in the environment
 - (b) Ability to detect unauthorized access or transactions on critical servers or applications
 - (c) Identify vulnerabilities on systems in the environment
 - (d) Ability to detect inappropriate activities by users conducted from corporate resources and/or during work hours
 - (e) Record keeping and retention of suspicious transactions or inappropriate activities
 - (f) Ability to support investigations and legal prosecution

Identify the security monitoring solutions, components, or systems that will satisfy each of the feature statements above.

Draw a security monitoring solution that meets all the feature requirements. Include the components and configuration to allow the solution to be centrally managed.

2. The next solution you need to design must be able to provide secure and high integrity transaction processing for an Internet site that will be handling transactions of value. Taking a basic Internet gateway solution, describe what additional components and systems you need to add to include the following features in the secure transaction solution.
 - (a) Secure web browsing from the Internet
 - (b) Secure web transactions that involve reading and writing data from a database or involving an application layer
 - (c) Strong authentication, to assure you have some confidence that users are who they claim to be
 - (d) Auditing functions to protect the business offering the secure services, in the event there is a dispute or a complaint that needs to be investigated

Bonus: Security monitoring is required for this solution. What special considerations or problems are there to do security monitoring for this solution? Describe a solution that will provide security monitoring in this case.

These questions are taken from K. Valios, *Security Architecture Issues*, UNSW COMP3441/9441 Seminar Slides, Week 11, Oct. 2003.