Cost-Effective Protection of Information Systems

Chair: **John Campbell, National Security Agency**
Panelists: **Tim Ehrsam, Oracle Corporation**
Ronald Knode, Computer Sciences Corporation
Paul Livingston, Intelink Management Office
Bill Stewart, Booz-Allen & Hamilton Inc.
Jim Williams, Booz-Allen & Hamilton Inc.

Today we have a world containing many federated distributed systems. These are systems having components located in different physical locations, locations sometimes thousands of miles apart. These are systems where, although parts of which are owned by different parties, many of the parts need to communicate with each other. The Internet and Intelink are two such examples. In the Internet, for example, I own my terminal, but I want to communicate, and do transactions with my bank, a bookseller and an auction house. I want to send personal mail to friends. And I want to do this safely.

Some systems require more safety. With electronic commerce, or with military operations, we want a lot of safety. Electronic commerce users will not use the system if they feel that their payments could be redirected. Many military systems demand a high degree of safety or security, without which a tremendous amount of harm could be done. In both types of systems people with different roles are given differing capabilities. Some users are able to view data, but only certain data. . Some users are permitted to read a particular file, database table or web page. Others should be able to write, modify or delete these files. Others may be given more capabilities. Still others are limited to executing programs.

Various mechanisms and methodologies have been suggested to provide this security. For example, certificates, physical tokens, VPNs, PKIs, proxy servers, firewalls, encryption, intrusion detection and Communities of Interest are all being proposed to solve the security problems. Frequently, however, the costs of purchasing, setting up and running these security mechanisms are ignored. Initial costs can be high and are often the results of lack-of-security afterthoughts. Operational and maintenance costs for security could be much higher than the initial costs and are often entirely overlooked. These costs need to be considered and accurately estimated in any development. For example, what is the per seat cost of security per year over the estimated lifetime of the system? But, can you project this cost more than a year or two due to the dynamic nature of the environment and changes in technology, knowledge about vulnerabilities, new or more effective technologies, requirements changes, etc.? How robust and flexible are the security solutions? For example, if new capabilities require additional holes in a firewall, how effective is the firewall after these additions are made? Or, if newly discovered vulnerabilities necessitate changes in security, how easily and cost effective can these changes be made?

There are other cost considerations. If I have need of a capability now, how much is it costing me while I wait until a long lead-time security system is put in place until I can use that capability? Lost customers? Lost opportunities? Inability to collect or gather information that I need now? On the other hand, if I do not have adequate security, what is that lack of security costing me? John Davis, of the National Computer Security Center stated that: “Risk is what companies must live with when they allocate limited monies and resources for network security.” I believe that this statement can be broadened to encompass all of information security. We system designers are accepting risk.

Some are still looking for cost-free, totally secure, user-friendly, no maintenance systems. While we are unable to identify such systems, the Panel will attempt to answer many of the above questions, based on systems that they know and have helped to develop. They will give insights in tradeoffs employed, such as between rigorous security requirements, and the limitations of time, personnel and other resources.

This panel will examine three or four real systems and the security features of each. They will describe why the security solutions that were built into the systems were chosen and the impact of the chosen solution on the functionality, security, operation and costs of that particular system. The insights that they provide should be of use to the Session attendees who are planning or designing in their own systems.

Tim Ehrsam
Manager, Security Technologies
Oracle Corporation

Abstract:

Commercial and government organizations are deploying database management system (DBMS) technology as the backbone for their electronic commerce and Internet-based computing applications. As one would expect, these organizations require high performance, scaleable, fault-tolerant systems that can efficiently and securely process transactions from thousands of concurrent, distributed clients. As application requirements for performance increase, multi-vendor, multi-component architectures to support these requirements are becoming more complex. However, commercial off-the-shelf technologies are being utilized for a variety of new web-based applications that support these application requirements in terms of both performance and security.

Historically, client/server applications were developed and the security of these "two-tier" applications was fairly straightforward. The client application was written and tested to verify correctness. The client application communicated directly with the backend commercial DBMS, which had already been evaluated as meeting various internationally recognized security metrics (e.g., Orange Book, ITSEC). Additionally, the networks were "closed" to protect the information from flowing outside the defined community of interest. Therefore, even if there was a security flaw in the application code, the damage was restricted to those already possessing sufficient "need to know."

Today's "service centric" application architectures are more complex. They include multiple tiers on multiple platforms performing specific tasks. For example, a browser client might authenticate to a web page that accesses information stored in a database behind a firewall, with the database obtaining authorizations for the user based upon information stored in a directory. Therefore, the application architecture must rely upon, for example, 1) a Secure Sockets Layer (SSL) connection to the web application server, 2) a secure connection through a firewall to the database, 3) a secure lookup of user information in a (LDAP) directory, and 4) mutual authentication of each of these interfaces using smartcards, Kerberos, X.509 certificates, or passwords.

While the integration of these components may add complexity to the application (versus client/server), organizations require this type of configuration to enhance security. This architecture, while more complex than client/server, is more performant, supports a variety of user authentication mechanisms, and adds layers of protection as the application process flows between tiers. In essence, each layer has the capability to re-verify the transaction as it passes through its realm. This gives rise to applications that are cost-effective and secure.

It is for this and other reasons that organizations in defense, healthcare, social services, and electronic commerce are deploying applications with multi-tier architectures. In addition to process isolation and separation for performance and throughput, these additional layers add to the security of the overall system. The presentation will describe customer implementations of this architecture and the benefits and challenges involved in their deployment.