Panel Discussion Outline

Title: A view from the trenches: leveraging security technology in the networked client/server environment

Panel members:

- G. Mark Hardy, INFOSEC Consultant, AXENT Technologies, Inc.
- Three others to be determined

Issues, viewpoints, and questions addressed:

Computing environments are being exposed to ever more hostile environments. Hackers, corporate espionage agents, disgruntled employees, contractors, and curious insiders all represent varying degrees of threat to systems today. How does one create adequate defenses in this increasingly hostile environment?

Statistics show three-quarters of security events originate from within an organization. A firewall, at best, addresses only 25% of the potential security problem. Native security capabilities are often inadequate, and are rarely used to their full effectiveness. The prudent security manager will apply centrally administered point protection to all client/server components, including network components, clients, servers, firewalls, routers, etc.

Intrusion detection is an essential component of a security policy. However, the "classic" approach of manually reviewing security logs offers a fine after-the-fact view of security, but represents a failed security policy. The security manager must implement automated tools that monitor and detect intrusion attempts, and respond immediately with corrective action. Security detection and response increases, cost of audit decreases, exposure is reduced.

The foundation of an effective information security program is a statement of security policy. Without this reference point, efforts to enhance or enforce security are, at best, suboptimal "fixes" without any guarantee of completeness. For a policy to be effective, it must be disseminated and enforced. Not only must users know, understand, and comply with security policy, but also each system in the client/server environment must have this same "understanding". A security policy that cannot be translated from paper to an on-line definition will not be enforced as thoroughly as one that can be.

Tools exist to perform annual or periodic audits. However, the benefits from these "snapshot" inspections are often short-lived. An effective security manager must be able to repeat, on a daily basis if necessary, a thorough check of all security relevant system settings and parameters so as to take prompt, decisive action to correct deficiencies. With this capability, the manager and the auditor share the same tools, share the same goals (secure the system), and can bridge the animosity frequently present between these two elements of an organization.

Our computing paradigm has changed significantly over the past several years. Whereas critical information and applications once existed exclusively on mainframes in protected locations, mobile computing, high density removable media, wide-area networking and public network connectivity have increased tremendously the probability of data compromise, destruction, or manipulation. By examining the role of the client in a client/server architecture, one ascertains the magnitude of the "uncontrolled access" threat.

Security systems are traditionally certified and designed to resist logical attacks. Because stolen notebook computers offer the opponent virtually unlimited access in terms of time and hardware tampering, many controls cease to protect as strongly as they would in the case of electronic access. The key to protecting information on the desktop is "passive" encryption, that is, activity that does not require the constant application of effort on the part of the operator. Security is often only as effective as it is non-invasive. The security manager should have the capability to configure desktop and mobile systems to enforce security without requiring the user to take deliberate action each time a sensitive file is created, copied, or deleted.

A security manager should put himself or herself into the role of an opponent (or thief) when assessing what information and processes are of value. By taking a critical "outside" view of systems and practices,

one can better predict the types of attacks one may encounter, the target of these attacks, and the source of the intrusions. Armed with

this additional knowledge, a security policy is much more likely to be responsive to the electronic “threat axis” from which intrusions will probably occur.

The panel discussion would address these topics, directed by questions or feedback from the audience. The above is listed as a sample of the types of direction such a presentation would take.

Disclaimer: although AXENT develops and markets security products for the client/server marketplace, this presentation is not designed as a “sales pitch”. No specific products will be mentioned. The goal of the session is to raise in the minds of security managers the issues frequently confronted in the marketplace, define a conceptual set of security solutions, and explain how these capabilities can be used effectively.

SPEAKER BIO G. Mark Hardy, Information Security Consultant

Mr. Hardy has served as an information security expert since 1976. He has written the Client/Server Security Handbook, and was a contributing author to Network Security Secrets. Mr. Hardy served on several ANSI Accredited Standards Committees, including X9F, Financial Information Security Subcommittee, and X9E9, Security for Wholesale Financial Telecommunications. He presents half-day seminars on client/server security in nearly 40 cities across the U.S. and Canada each year, and is a frequent speaker at security conferences and shows.

Presentation Outline

Many companies are touting Virtual Private Network (VPN) solutions, but do they represent a complete solution to secure remote access control? Most solutions do not address security at either end of the VPN connection, or what happens to the sensitive files once they are downloaded across the VPN (data at rest). A VPN only represents one component of an effective remote secure access solution.

This presentation examines the necessary elements of an effective remote security solution, including VPN, multi-factor access, data encryption, one-time passwords, discretionary file access control, and secure deletion. It addresses the three factors that provide true Remote Access Security:

- Virtual Private Network
- Two-Factor User Authentication
- Local and Remote Access Control

An example of such a “security briefcase” will be demonstrated to provide a proof-of-concept for enhanced secure remote access.