

Access Management and User Accountability for WLANs

A White Paper



vernier[™]
NETWORKS

Vernier Networks, Inc.
465 National Avenue
Mountain View, California 94043
www.vernier.net

Introduction

“We have met the enemy, and he is us.” Read the latest FBI/CSI *Computer Crime and Security Survey*, and that adage from the old *Pogo* comic strip is likely to be your conclusion. The survey found that insider abuse of network access was the second most common form of network attack. Insider abuse was reported by 80% of survey respondents—second only to virus incidents (82%). And—just as astonishing—disgruntled employees (77%) were ranked just behind independent hackers (82%) as a likely source of attacks.¹ As these numbers show, organizations who want to secure their networks need to do more than erect a defensive perimeter to keep out strangers. They need to find a way to prevent attacks from insiders, as well.

Notwithstanding some sensational stories in industry publications, WLANs (wireless LANs) don’t create new security problems. They simply make manifest the security problems that already exist, such as this threat from insiders. LANs, wired or wireless, are not secure. Employees and other trusted users can do myriad things—many of them illicit—once they gain access to a LAN.

Before wireless computing, organizations tended to ignore this threat. Physical barriers, such as doors and walls, kept outside hackers off the network. Inside a building, no one was going to tap a wire to gain surreptitious access to the network. Since every user has a password-protected account, the network was deemed to be safe—a false impression, as the FBI/CSI numbers show. Insiders have been abusing networks for years. As organizations move more operations and assets online, their vulnerability to attacks and sabotage from within will only increase.

Fortunately, these problems can be solved. Just as WLANs expose the vulnerabilities of enterprise networks—such as the free-for-all access privileges available to anyone who can get on the network—so WLAN security and management solutions show a way forward for enterprises who want to secure and manage both their wired and wireless networks.

¹ 2003 CSI/FBI *Computer Crime and Security Survey*, Computer Security Institute.

From Managing Ports to Managing Users

Before the age of WLANs, network administrators usually managed ports, rather than users. When a new employee arrived, he or she was assigned an office with a PC sitting on a desk. The PC was connected to a network port in the wall. The only way employees accessed the network was through the computers in their offices. The network could be secured—theoretically—by ensuring that every PC in every office enforced a simple login procedure. If there was trouble on the network, administrators could trace it to a port and, hence, to a user.

Wireless access points and mobile computing devices completely undermine this security model. Now a wireless access point connects to a port in the wall. Any wireless user, friendly or hostile, who happens to be nearby can now access the network. There is no longer a direct relationship between users and ports, and physical barriers no longer prevent malicious users from gaining access to online resources.

This situation creates two problems for administrators managing user accounts and network security. First, it forces administrators to provision different levels of security for a single location to accommodate a rapidly changing pool of users. Consider the case of a conference room. It may be used for a board meeting in the morning, an executive staff meeting at lunch, a customer briefing in the afternoon, and a temporary workspace for auditors in the evening. How does a network administrator ensure that the network access in this room is provisioned appropriately for each group of users? In this case and in many others, mobile computing forces administrators to grapple with user account “moves, adds, and changes” at a vastly accelerated pace. Permissions at a location need to change continually, because different users are working at that location.

Second, because mobile users do not have to be sitting at a desk to access the network, it's easier for them to execute attacks without being detected. Only a very bold employee would try hacking into a Finance system from an accountant's desk while the accountant is away at lunch. It takes a lot less nerve to execute the same attack from a nearby hallway, using a wireless device such as a Pocket PC.

The best way to ensure that only authorized users access the network and that, once on the network, users do not engage in illicit activities, is to deploy a user-based access management system. These systems assign specific access rights to users based on their roles in an organization. By tailoring network access to individual users based on who they are, the work they are doing, and the locations where they are working, enterprises can achieve the control they have been missing on both their wired and wireless networks. Examples of user-based access rights include:

- Limiting access by role; for example, allowing only managers to access a server running a project-management application.

- Limiting network access by location; for example, allowing only members of the Finance department to access the network in the Finance building, and allowing users in public areas such as lobbies to access the Internet but not internal resources.
- Limiting network access by time; for example, disallowing access in certain departments after hours.

By maintaining session logs of network activity, user-based access management systems enable administrators to track the activities of users and to identify individuals engaging in malicious or suspicious behavior. By managing users, rather than ports, these systems give IT departments the precision they need to ensure that each user has the access rights he or she needs—and only those rights. By eliminating unfettered access to the network, these systems reduce the ability of insiders to execute security attacks on the network.

Thinking in Terms of Services

Focusing on users is a good first step toward addressing the need for comprehensive network security on wired and wireless networks. To improve not just security, but productivity, as well, administrators should begin to think more in terms of services, rather than devices.

In any organization, there are likely to be two divergent views of the network. Administrators view the network as a collection of cables and special devices for optimizing the flow of traffic along those cables. Users, on the other hand, view the network as a source of services: email, Web access, application access, and—in organizations adopting Voice over Internet Protocol (VoIP) telephony—voice communications. Services are user-specific; they benefit individual users.

Administrators need to recognize that their ultimate mission is to guarantee these services for users. Instead of focusing on cables, routers, and other network devices, they need to focus more on the services that these products support. Network management systems need to be intelligent enough to enable administrators to identify users on the network and to ensure that each user is getting the services he or she requires.

This service orientation aligns with the investments organizations are making in network security. Security is ultimately based on services. Viruses and worms don't attack the network per se; they attack specific services on the network, such as the RPC service on Windows platforms. To thwart these attacks, administrators can reprogram the interfaces for these services (for example, blocking access through a particular port). The success of this programming will be measured in terms of service—service performance and availability—for end users.

The next generation of network management solutions should enable administrators to 1) manage and monitor access for individual users on the network, and 2) provision services, such as email and VoIP for those users, and monitor the performance and availability of those services over time.

WLAN management systems, such as WLAN Security Gateways, can provide the foundation for these solutions. Operating at both Layer 2 and Layer 3 in the network stack, WLAN Security Gateways perform packet filtering and policy-based traffic management on all IP traffic flowing past, regardless of whether the traffic's source or destination is wired or wireless. Designed to work in an environment where any traffic flow could be hostile, these products provide the user- and service-based precision that enterprises need in order to secure their networks from all threats—internal and external—and to deliver the mission-critical services that users require.

About Vernier Networks

Founded in March 2001, Vernier Networks develops innovative systems and software to protect, manage, and enhance wireless networks. Vernier's intelligent, networking technology allows network managers to centralize wireless LAN usage policies, secure wireless network access at the edge, and deploy scalable wireless mobility across the enterprise. Vernier Networks has been honored with a 2003 Product of the Year Award from Network Magazine, Network Computing Editors' Choice Award, and Best of Show award at NetWorld+Interop. A privately held company, Vernier Networks is the first spinout company of Packet Design, LLC; a technology development company founded by entrepreneurs Judy Estrin and Bill Carrico. For more information, visit the Vernier Networks web site at: www.vernier.net or contact a Vernier representative at info@vernier.net