



Secure Wireless Management

SECURITY ANALYSIS

Code Red Systems Ltd.
21 HaVaad HaLeumi
POB 16120, Jerusalem, Israel
T +972-2-642-3401, F +972-2-678-3403
Email: info@code-red.biz
Web: <http://www.code-red.biz>

Feb 2006

Profiling and Securing Endpoint Devices Using AirStop and IBM Access Connections

By Drew Tick, CEO
Code Red Systems

“Organizations have felt the sting of focusing security on the perimeter while neglecting to secure the end points (such as desktops, laptops) in the enterprise.”

Michael Rasmussen, Forrester Research

Overview

The past ten years have seen tremendous strides in perimeter security based on protecting networks from external attacks. Recently, however, the demands of the mobile workforce and “anytime, anywhere” computing have seen a multiplying of endpoint communications adapters. Laptops have gone from external modem and Ethernet cards to five or more embedded communications devices including: LAN, Wireless LAN (WLAN), Bluetooth, Firewire (1394), Fax/Modem, Infrared, USB devices and more.

More connectivity means more security threats. Each communications adapter is not only a way for authorized users to connect with the outside world, but it is also a backdoor for intruders seeking to gain access to endpoint computers and the network.

IBM’s Access Connections is a configuration tool which provides users with a certain hardware profile according to their computing environment. Code Red’s AirStop software gives dynamic port control and centrally managed security enforcement on endpoint devices. Together they can be used for a comprehensive endpoint configuration and security solution.

While some administrators may consider using a profiling tool to secure endpoint devices, this document describes the purpose of profiling tools and why it is also necessary to include security enforcement software, such as Code Red’s AirStop, as part of any comprehensive endpoint configuration and security solution.

Secure Wireless Management

“Unauthorized access... showed a dramatic cost increase... as the second most significant contributor to computer crime losses during the past year.”

CSI/FBI 2005 Computer Crime and Security Survey

The Problem

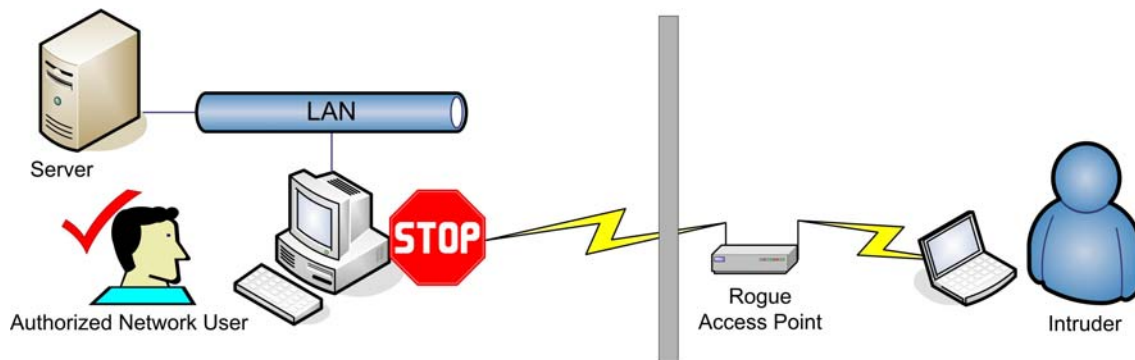
According to the CSI / FBI Computer Crime and Security Survey for 2005, the dollar amount lost due to unauthorized access mounted to over \$30 million. With the improvements in perimeter security, many of these attacks can be traced to a lack of endpoint security.

Research firm IDC defines endpoint security as centrally managed client security and likened it to a 21st century digitized watchdog protecting users from "a cesspool squirming with destructive technological deviants."

By default most communications adapters are “always on”. This can lead to dangerous bridging situations where two or more communications adapters are being used at the same time.

For example, an authorized user with a Centrino® based laptop can be connected to the network using a standard wired Ethernet port. At the same time, an intruder can boot up a wireless access point causing the authorized Centrino based laptop using Microsoft’s Wireless Zero Configuration®, to automatically connect to the access point. The intruder can then use the wireless connection to the laptop and its routing tables to hack into the wired network.

This type of wireless bridging attack is illustrated below:



Simultaneous connection of any two communications adapters is a security breach. This not only goes for the wired and wireless Ethernet connection, but also Bluetooth, infrared, Fax/Modem and other communications devices.

While control of these devices helps prevent inbound attacks, there are also storage devices, such as USB Mass Storage Devices and CD-R/W Drives, which should also be controlled to prevent outbound leakage of classified information.



Secure Wireless Management

“Access Connections is a connectivity-assistant program for your ThinkPad computer. With Access Connections, you can quickly switch network settings and Internet settings by selecting a location profile.”

Access Connections Product Description, Lenovo Web Site

The Solution

It is important to differentiate between profiling tools and security policy enforcement software. Profiling tools give default use of certain adapters in particular environments for the sake of user convenience, while security policy enforcement software forces usage of specific adapters in specific situations to prevent unauthorized access.

Profiling tools can assist users in choosing the correct hardware, however, they are not designed to protect the network or the computing device. Security policy enforcement software is designed to protect both the device and access to the network by limiting user options in terms of communications adapters.

Security enforcement means that the IT administrator is in control and the end-user must conform to the company’s security policy. When using a profiling tool, the user can remove the software, change the configuration and add new devices. The profiling software will simply accept these changes as a new configuration of the laptop. Therefore, profiling tools cannot be defined as “Security Enforcement” solutions.

Security enforcement software does not allow users to remove or change the software and must also account for new hardware installed by the end-user. Since AirStop is security policy enforcement software, it cannot be removed or configured by the end-user. It has its own password which only allows administrators to change the configuration.

IBM Access Connections is a configuration tool. It has a limited number of adapters under its control and is not meant to enforce security policy. For example, using Access Connections a profile can be created to allow or disallow use of a WiFi or Bluetooth connection, but these definitions are static and do not dynamically enable or disable communications ports according to end-user behavior. Likewise the profile can be changed or removed by the user. Moreover, the user may install new communications adapters which automatically bypass the previous configuration settings.

AirStop enables and disabled communications adapters on the driver level according to the security policy set by the administrator. The end-user cannot change these definitions even when selecting a different profile. If the end-user attempts to manually enable an “AirStopped” device or install a new one, the software will dynamically shut it down in less than one second.

From a management perspective, AirStop was designed according to the requirements of IT professionals. For example, the software can be distributed from a central location using distribution software such as Microsoft’s SMS or other standard software distribution platform. Configuration and upgrades for specific user groups are provided using the same distribution mechanism.



Secure Wireless Management

In addition, AirStop has a web based server which may be used to collect information from all AirStop clients. It monitors the activity of all the communications adapters in the organization, and enables review of historical data for specific computers over time.

Since Access Connections is a profiling tool, it does not have centralized management and configuration, nor does it have a server for monitoring client activity.

The Conclusion

Demands of mobile computing have given rise to the need for “anytime, anywhere” communications. This has resulted in the inclusion of a number of wired and wireless communications devices as standard equipment in desktops, laptops and PDAs.

While this has indeed made it easier to communicate it has also created a situation where it is easier than ever for hackers to gain access to end-user devices themselves or use their routing tables to gain access to corporate networks.

Profiling tools, such as IBM’s Access Connections, are designed to assist users in selecting the correct communications adapters in a particular environment. Since they can easily be removed or re-configured according to user preferences, these tools should not be used for protecting end-user devices or network access. At the same time, security enforcement software is designed to take rules as defined by the system administrator and enforce them on all end-user devices, in all situations, to protect both the devices and the network.

Therefore it is recommended to implement endpoint solutions, which not only simplify end-user configuration, but more importantly, enforce security policy and protect both devices and the network from external attacks.

Accordingly, administrators should leverage IBM Access Connections for simplifying end-user configuration and use AirStop for enforcing security policy on endpoint devices.