WHITE PAPER

Enterprise Wireless LAN Security

Preface

This paper describes the challenges today's administrators face when planning data protection for their wireless networks. Paramount in this discussion are the existing Motorola solutions in place now to meet and exceed the data protection expectations of enterprise-class administrators, and Motorola's 802.11n support plan.

Users within segregated large enterprise network environments share the commonality of the data within their corporate LAN, but not necessarily the data residing within carefully defined and proprietary WLAN segments. These WLANs are typically restricted to just those users requiring access to it.

While large corporate LANs are still somewhat viable, they are increasingly being augmented by multiple WLAN segments devised to support unique blends of multi-media and traditional data traffic. Whether these WLAN segments reside in close proximity of one another or in remote locations, each requires unique security mechanisms and must be able to periodically grant and restrict user permissions across their virtual networks.

Today's network administrator's must devise security schemes general enough for all to share access to corporate assets, while simultaneously providing provisional or temporary restrictions to specific mission-critical network resources and domains. No single security method can optimally protect data corporately while simultaneously protecting segregated network segments from unsolicited user access.

For this reason, today's network administrators can be equated to "wireless traffic cops" who enforce laws at both the federal (corporate) and local (individual WLAN) level. Federal laws can be seen as security mechanisms providing data protection for corporate assets regardless of one's local domain restrictions. These "federal" security mechanisms are designed to protect data from unauthorized access and the hacking of corporate resources. Security mechanisms at the "local" level are often mechanisms authenticating user credentials before access is granted to a WLAN whose data is interpreted as proprietary.
Only through deploying an intuitive combination of these federal and local security mechanisms can an enterprise class network administrator enforce a "lawful" population of network segments whose security infractions are kept at the absolute minimum. Fortunately, the savvy network administrator has numerous options available to them for both local and remote wired and wireless deployments.

This paper describes the security challenges network administrators face defining and implementing security mechanisms within diverse wired and wireless network environments.

Paramount in this discussion are the existing Motorola solutions in place now to meet and exceed the data protection expectations of enterprise-class administrators, and Motorola's plan to support 802.11n as products are introduced.

WLAN Stability

The medium over which a WLAN operates is air, which by its nature is insecure and somewhat "lawless." Regardless of the safeguards defined when planning and installing a wireless network, wireless devices, by nature, still self-deploy and have the capability to connect to unknown clients and devices. With the infiltration of wireless enabled messaging devices, the number of mobile devices continually probing for stronger connections is unprecedented.

A wireless access point physically connected to a wired network can broadcast the sensitive network credentials a wireless "outlaw" needs to hack into an entire enterprise network, and in doing so roam remotely from one network segment to the next. While a network's enterprise-class infrastructure is typically supported by Ethernet wire, its data repositories are still exposed on the WLAN over the series of wireless device associations stemming down from a switch, to its connected access port radio and passed over the air to mobile devices. Without proper security measures, any mobile device can treat your wireless network like a "lawless" town and stealthily eavesdrop on all of its network traffic and resources.

The default security mechanism afforded most consumer-grade wireless devices are woefully insufficient beyond the access requirements of your local Starbucks coffee-house network. Entry class mobile device security mechanisms provided by consumer-grade vendors are not sufficient to secure enterprise WLANs, which require encryption beyond WEP, additional access control filtering, intrusion detection, and 24 x 7 monitoring. In response to these business risks, Motorola has been proactively developing solutions with exactly this kind of multi-tiered enterprise data protection in mind.

Motorola has recently equipped its wireless switch solution set with the following WLAN stability mechanisms to meet (and exceed) the needs of expanding wireless networks and provide administrators with additional options as their data protection needs expand:

NAC

Using *Network Access Control* (NAC), Motorola switch hardware and software grants access to specific network resources. NAC performs a user and MU (mobile unit) authorization check for resources without a NAC agent. NAC verifies a MU's compliance with the switch's security policy. The Motorola switch family supports the EAP/802.1x type of NAC. However, the switch also provides a means to bypass NAC authentication for MUs without NAC 802.1x support (printers, phones, PDAs etc.). NAC protects data proliferating your wireless infrastructure by:

- Blocking or quarantining non-compliant devices from connecting to a WLAN
- Providing 802.1x based pre-admission control to block devices at the authentication stage
- Working with any NAC solution conducting 802.1x and dynamic VLAN assignment
- Providing qualified interoperability with MS NAP and Symantec NAC solution

Wireless Firewall

Firewalls protect networks from unauthorized Internet traffic. Motorola's switch supported firewalls allow authorized traffic while blocking unauthorized traffic. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. Messages entering or leaving the Intranet pass through the firewall. The firewall examines each message and blocks those not meeting the defined security criteria (much like a customs agent checking a passport before allowing entry to a country). The Motorola switch family supports Stateful Layer 2 and Role-Based firewalls providing the following data protection mechanisms:

Stateful Layer 2 Firewalls

- Use Layer 2 as the most common deployment option
- Provide a fully stateful firewall in Layer 2 mode
- Allow established sessions to continue uninterrupted after a MU roams between an AP and a switch
- Handle Layer 2 attacks, including (just to name a few); Arp cache poisoning/Arp Spoofing, DHCP Rogue server attack, DHCP starvation, broadcast storms, incomplete Fragment attack checks, suspicious activity checks

Role-Based Firewalls

- Base the security policy on user group, location, encryption strength etc.
- Follow a user as they move across different APs and switches

Wireless with WPA2 (More Secure than Wired)

Snooping traffic on a wired LAN is not difficult if you have physical access to the domain's wired infrastructure. However, snooping WPA2 traffic is next to impossible. As a result, WPA2 has been made a data security option supported by nearly all of Motorola's enterprise-class wireless infrastructure offerings.

Wi-Fi Protected Access 2 (WPA2) is the follow-on security method to WPA. The "shared medium" nature of wireless traffic and widespread criticism of WEP resulted in the development of the cryptographically secure WPA2. WPA2 uses the *Advanced Encryption Standard* (AES). Virtually no known wireless attacks exist against AES! CCMP is the security standard used by AES. CCMP computes a *Message Integrity Check* (MIC) using a proven *Cipher Block Chaining* (CBC) technique. Like TKIP, the keys an administrator provides derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The result is an encryption scheme as secure as any Motorola provides in our enterprise-class wireless infrastructure family of devices.

Distributed Security Enforcement with Centralized Policy for 802.11n Support

Motorola's distributed security enforcement strategy for scaling to 802.11n support includes:

- Wireless encryption/decryption occurring at the AP
- Policy enforcement occurring at the AP
- Policies following the user as they move from AP to AP without an impact to ongoing traffic

Rogue Device Detection

Wireless deployments afford network administrators freedom from the constraints of wired environments. However, mobile devices may lack the data protection mechanisms of a wired infrastructure. Consequently, an open door could be created for unauthorized (rogue) devices to violate the poorly enforced laws of an immature security scheme, thus rendering investments in wired security useless.

Motorola's holistic approach to monitoring ensures WLAN policies are enforced and rogue devices are promptly detected and removed. The following describes two of Motorola's enterprise class solutions designed to equip today's wireless traffic cop with the tools they need catch wireless rogue offenders and keep them from violating the privacy of your wireless domain.

By converting the physical dimensions of a network segment into a representative site map, both Motorola's *Wireless Intrusion Protection Software* (WIPS) and Motorola's *RF Management Software* (RFMS) can accurately track the deployment of and operation of authorized devices and use their location to triangulate the location of potentially hostile devices.

Motorola Wireless Intrusion Protection

Wireless IPS (WIPS) is an industry leading monitoring solution enabling network administrators to proactively close network security holes and mitigate the risk of security breaches. WIPS uses distributed sensors and pre-positioned device radios to (among other things) detect the presence of 802.11 a/b/g rogue devices.

WIPS sensors continuously monitor WLAN activity and report network events to a centralized server. The WIPS management server correlates and analyzes the data to provide real-time rogue detection, policy enforcement and intrusion protection. If an un-authorized device is detected, WIPS has the means of interrogating the rouge to obtain valuable data to aid forensics, reporting and recording the event.

By converting the physical dimensions of a network segment into a representative site map, both WIPS and RFMS can accurately track the deployment and operation of authorized devices and use their location to triangulate the location of potentially hostile devices to provide another level of forensics.

WIPS provides the following data protection mechanisms:

- **Air Lockdown** - Enables network administrators to terminate a connection between a WLAN and an associated access point or MU upon the detection of a threat. If the connected device is an access point, the WIPS server de-authenticates and disassociates all MUs associated with it. If the device is an MU, the server terminates the MUs connection to the access point.
- **Wireless Termination** – Allows an administrator to terminate a connection between a WLAN and any access point or MU associated with it.
- **WEP Cloaking** – Enables an AP-5131 to actively transmit WEP cloaking frames for protecting legacy devices (similar to an AP300's existing WEP cloaking functionality).
- **AP-51xx Sensor Conversion** - Allows a customer to deploy a single AP-5131 (dual radio model) as both a traditional infrastructure access point and a WIPS sensor. Sensor conversion on an AP-5131 provides infrastructure support on one radio while scanning on the other radio and using the frames received by the sensor to provide WIPS algorithms. The WIPS Sensor and AP-5131 run simultaneously.

RF Management Software (RFMS)

Intrusion protection is of limited value if it is difficult for an IT administrator to initially detect and categorize potentially hostile devices. RFMS provides network administrators simple visual data to react to a rogue identified by WIPS.

With the 3.0 release of RFMS, RFMS becomes Motorola's central enterprise WLAN network management solution. Motorola RFMS provides a single *Manager-of-Manager* (MoM) console from which you can plan, monitor and detect threats within wireless networks.

RFMS submits a request to gather signal strength data from at least three detecting devices deployed and authorized within a RFMS supported site. Once obtained, RFMS creates a dynamic object of each detecting switch to obtain RSSI data used to triangulate the rogue's location. Once RFMS has detected the presence of a rogue and can position it within a site (within 10 meters of its actual location), rogue detection data is processed and displayed.

Once located, a rogue displays within the site map as an access port radio with a red X over the device (defining it as operating illegally). The rogue device displays a pulsating red box around the device to further distinguish it from devices placed and authorized within the site. The detected rogue device will remain on the site map for two minutes, after which Motorola RFMS clears the device from the site and log its detection and removal.

Meeting and Exceeding the Defense Department's FIPS Criteria

The *Department of Defense* (DoD) requires commercial WLAN systems incorporate extensive measures to protect the voice and data traffic proliferating a wireless network. In standardizing their WLAN security requirements, the DoD defined *Federal Information Processing Standards* (FIPS) 140-2 and Common Criteria, including WLAN Access System Protection Profile requirements.

Like most typical DoD WLAN deployments (and their inherent data protection challenges), retail, healthcare, financial and wireless carrier businesses are under increasing pressure to ensure information is secure across their wireless networks. The majority of these institutions are implementing the same standards mandated by the U.S. government. For this reason, FIPS certification has become central to demonstrating a WLAN security deployment accepted by IT professionals for its maturity.

During FIPS 140-2 and Common Criteria certification, a wireless solution must pass a series of comprehensive security tests, including a vulnerability and penetration analysis. The wireless solution's design metaphor and its source code are scrutinized by experts to ensure its compliance with advanced cryptographic standards.

Motorola's enterprise-class RFS7000 and WS5100 switch platforms have satisfied FIPS pre-validation requirements and have been placed on the FIPS 140-2 pre-validation list.

The RFS7000 and WS5100 have also entered the Common Criteria evaluation process at the Common Criteria Evaluation Assurance Level 4 (EAL4). This represents the highest compliance level with the U.S. government's Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments.

The Motorola RFS7000 and WS5100 are currently the only wireless/RF switch products undergoing the Common Criteria evaluation at EAL4 with the specified U.S. government protection profile for basic robustness environments. This will ensure Motorola's enterprise class switch solutions are properly certified to meet and exceed the emerging FIPS requirement. Motorola expects to receive final FIPS 140-2 and Common Criteria EAL4 validation in 2008, well in advance of the competition.

MOTOROLA

motorola.com