RF BARRIER

Product is First to Defend Enterprises Against 'Parking Lot Attacks'

SUNNYVALE, Calif., July 28, 2008 -- Meru Networks introduced RF Barrier, the first IEEE 802.11-based technology for proactively defending wireless networks against eavesdroppers and "parking lot" attackers, who attempt to record and observe network traffic from outside a building's perimeter in order to steal sensitive and valuable information.

RF Barrier uses wireless LAN technology to block the radio-frequency (RF) signals from the corporate network as they exit the building, without disrupting internal WLAN operation. This limits an attacker's ability to eavesdrop on data and perform offline analysis.

"Parking lot" attacks take advantage of wireless propagation, or bleed-through, from within a building through the perimeter and out to a parking lot or other surrounding area. These attacks are entirely passive in nature, generating no network traffic or other sign they are occurring, and are therefore undetectable by conventional wireless intrusion prevention systems (WIPS). In an activity known as "wardriving," attackers drive around the perimeters of enterprises and retail sites, looking for vulnerable or exposed networks. A number of successful and costly parking lot attacks have been perpetrated, one of the most notable involving the theft of millions of users' credit-card records.

RF Barrier is the first solution using exclusively 802.11 technology to offer wireless perimeter protection for organizations with regulatory requirements or policies regarding data privacy, such as retailers, financial and government institutions, manufacturers and health-care organizations. RF Barrier protects clients with legacy security mechanisms, such as handhelds and scanners equipped only with WEP or WPA/TKIP, as well as modern WPA2- and EAP-based networks, where it helps prevent the exposure of potentially exploitable information such as user identities. Furthermore, it provides physical wireless security in remote branch offices where no IT personnel are present to detect or stop an attack from outside the site's physical boundaries.

Mounting a Perimeter Defense for the Enterprise

"Previously, both wireless security and infrastructure vendors have focused on protecting the connection and the back-end network, while the perimeter -- where attacks cannot be detected -- has remained undefended," said Joe Epstein, Meru's senior director of technology. "RF Barrier mounts a strong defense by blocking signals from the designated wireless network from being effectively decoded outside the perimeter. For example, a retailer need no longer worry about the 'bleeding' of its financial data beyond the walls of the building from legacy devices that don't support the newest and most advanced security standards. As the first solution to provide cost-effective perimeter wireless protection, RF Barrier can greatly expand the network manager's confidence in the security of both legacy and modern wireless networks."

"The Information Stops Here"
Chicago-based produce wholesaler Anthony Marano Company has tested RF Barrier and plans to deploy it later this year. Chris Nowak, chief technology officer, said the company was seeking to protect its Wi-Fi voice infrastructure, which supports virtually all of its communication with customers and vendors.

"Our Nokia Wi-Fi smart phones handle sensitive voice calls as well as confidential emails and contact information," Nowak said. "With our warehouse adjacent to an interstate highway and other major roads, no one is comfortable with blasting a Wi-Fi signal all over the place. RF Barrier lets us decide exactly where we want to draw the border around the coverage area, and we know that the information stops right here. And we can keep our infrastructure tuned to maximum power without worrying about the consequences of signal bleeding. RF Barrier dramatically reduces the risk of parking lot-type security attacks -- and means we won't have to make excuses to management later."

How RF Barrier Works
RF Barrier (patent pending) is installed by mounting a Meru Networks wireless access point along the inside perimeter of a building, and an advanced external antenna outside the perimeter. RF Barrier technology inspects the traffic in real time to determine which part belongs to the WLAN (and is therefore designated as sensitive) and uses the external antenna to block outbound traffic at the RF layer. Would-be attackers are limited in their ability to see useful packet information about the internal network.

Because RF Barrier uses directional antennas and selective enforcement technology, it has no impact on signals within the building or from other networks. Internal clients connect normally, with enterprise access points serving them at full speed. RF Barrier can be turned on and off as needed, giving enterprises the flexibility to allow access at certain times of day while restricting it at others.

Meru's Comprehensive Wireless Security Solution
RF Barrier is the latest addition to Meru's comprehensive security solution, which provides security across all four of the major areas subject to active wireless threats: perimeter defense, connection defense, network defense and remote threat defense. Other components of the Meru security portfolio are:

- Rogue prevention, which detects and identifies rogues based on the wired network to which a rogue is connected as well as its over-the-air signaling
- AirFirewall, based on Meru physical security technology that can eliminate, rather than just contain or mitigate, rogue access points and evil twins attackers
- Per-user, per-application stateful firewall to allow policy enforcement based on both the user's identity and the nature of the traffic
- Signature-based firewalling, for enforcing policies on peer-to-peer applications such as Skype, as well as application flows within end-to-end encrypted VPN tunnels

- Location-based policy enforcement, which implements security decisions based on the location from which an unauthorized user is accessing the network
- Comprehensive voice and video security, which prevent the introduction of local or network-wide vulnerabilities in the presence of voice, video or heavy data traffic
- FIPS 140-2-certified algorithms, with military-grade encryption and key negotiation, including EAP-TLS and AES-CCMP using 802.11i
- Secure remote access points, which extend enterprise security policies and network to the home offices of telecommuters and hotel rooms for mobile employees.

RF Barrier Helps Deter Eavesdroppers

By Lisa Phifer

July 28, 2008

Today, Meru Networks announced RF Barrier, the next salvo in the industry's on-going battle against piggybackers and hackers who access networks from parking lots or other areas within range of a corporate WLAN’s signal. Unlike counter-measures that use encryption to scramble sensitive data, RF Barrier fights fire with fire by transmitting over Wi-Fi signals that would otherwise propagate farther than intended.

"Wireless security has largely been about applying wired techniques [like encryption and IPS]," said Joe Epstein, Meru's senior director of technology. "But most really damaging attacks have taken advantage of wireless signal bleed into areas like parking lots. Those [passive eavesdropping attacks] are the worst because they cannot be detected electronically. This is where RF Barrier comes in, to stop signals from reaching perimeter attackers."

Cranking up the volume

To insulate a building with RF Barrier, Meru mounts one specialized 802.11a/b/g access point on each exterior wall—typically, one AP per 100 linear feet. Each AP is equipped with special firmware and two antennas. An interior omni antenna listens passively for inside WLAN transmissions, while an exterior directional antenna transmits innocuous 802.11 frames simultaneously over each transmission.

"A parking lot attacker will pick up both signals," said Epstein. "But the exterior antenna will be much closer and its transmissions will be much stronger. If [attackers] see inside transmissions at all, it will only be for short periods, and signal will be very degraded. This approach is highly effective against eavesdropping attacks mounted from outside."

Meru recommends that customers walk around outside after installation, carrying any Wi-Fi capable laptop or phone. If RF Barrier is working properly, those outside Wi-Fi clients will not receive enough beaconed information to even list the WLAN as an available network.

However, RF Barrier transmits selectively, only when required to block a transmission. "Transmitting all the time would be harmful," emphasized Epstein. "Continuous transmission or RF jamming would have a major impact on neighboring networks. That would just not be acceptable in most business environments."

Reducing the impact

Of course, RF Barrier is not the only way to mitigate passive Wi-Fi eavesdropping. High-security facilities that do not ban Wi-Fi altogether sometimes employ specialized building materials like RF-shielded paint, wallpaper, or windows.

"RF paint is incredibly expensive and not terribly effective," said Epstein. "As soon as someone opens a door, you have signal leakage. And working in a building without any windows is not that comfortable. It might be fine for NSA, but it just won't work for most banks or retail stores."

Instead, many businesses use less exotic steps like directional antennas that focus more signal inside than out and reduced transmit power. While such measures can cut signal bleed, they rarely prevent it altogether. In particular, turning APs down can reduce performance for inside "corner cases" while doing little to stop serious attackers with high-gain directional antennas.

Assembling the pieces

As a WLAN vendor, Meru also provides conventional security measures like FIPS-certified AES encryption and AirFirewall intrusion prevention.

"Those strategies make a lot of sense, but they are implemented and used by humans, and they can still have vulnerabilities," said Epstein. "For example, retailers have issues with older devices that only support WEP or shared keys. Even devices that support EAP-TLS still send certificates in the clear, potentially leaking a lot of information. Encryption alone just can't stop attackers from seeing SSIDs the way that RF Barrier can."

Epstein believes that RF Barrier will be especially attractive to businesses with distributed offices that operate without on-site IT staff, such as retail stores and bank branches. In such cases, RF Barrier provides added insurance against mistakes or leaks that might otherwise go unnoticed.

For example, produce wholesaler Anthony Marano Company installed RF Barrier to protect its Wi-Fi voice network. Located right next to I-55 in Chicago, the company was especially concerned about signal bleed from its warehouse onto the adjacent highway.

"Our Nokia Wi-Fi smart phones handle sensitive voice calls as well as confidential e-mails," said Chris Nowak, CTO. "RF Barrier lets us decide exactly where we want to draw the border around the coverage area, and we know the information stops right here...RF Barrier dramatically reduces the risk of parking lot-type security attacks—and that means we won't have to make excuses to management later."