

prevent casual or inadvertent eavesdropping. Only those network devices that share a common Subnet ID can exchange packets. Setting a common Subnet ID is the bare-minimum security policy one should adopt for an RMG wireless network.

- 3) MAC address filtering: RMG access points implement MAC address filtering to only allow specific MAC address access to an access point. This technique is an important part of our security story and allows an IT manager to control the valid MAC addresses for any given access point.
- 4) When these two mechanisms are combined with either 128bit DES packet encryption and user authentication via the industry proven RADIUS authentication protocol, our security story becomes sufficiently robust to protect against all but the most determined intruders.

RMG uses the BSAFE technology from RSA, which is an exceptionally well-proven, rigorously examined and industry-accepted technology. BSAFE provides effective security for e-commerce, numerous VPN solutions and RMG wireless networks.

While an effective security policy must go beyond simply securing the data link, RMG is committed to providing our users with the best-of-breed link security solutions.

RMG secure products are used in applications that span Home-LAN user to secure military applications.



RadioLAN Marketing Group

RadioLAN Marketing Group
185 Lewis Road - Suite 30
San Jose, California 95111

Phone: 408-365-6200

Fax: 408-365-7675

Email: info@radiolan.com

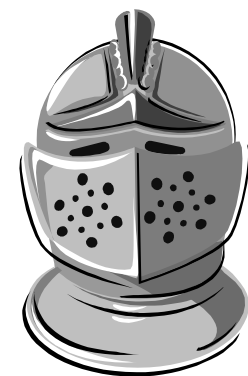


RadioLAN Marketing Group

Security for Wireless Systems

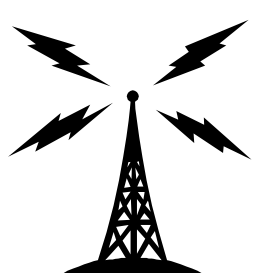
A Backgrounder

*The leader in 5 GHz
Wireless Networking*



www.radiolan.com

Security for Wireless Systems



The Wireless Opportunity

Wireless LANs provide freedom and flexibility to both mobile and stationary

users. Unfortunately, the very characteristics that enable this freedom make wireless LANs vulnerable. This is an issue that network users and administrators must guard against.

Wireless LANs are now widely deployed. Since it is not practical to confine a wireless signal to a physically secure environment, wireless networks are susceptible to unauthorized access. This puts the onus of security on the network and its infrastructure in a way that is not required in a wired network. This includes policy management, VPNs, and authentication, as well as securing and encrypting the data link.

Wireless Security Needs

One question asked by IT professionals in deploying a wireless LAN is how do we stop users reading traffic not routed to them, modifying that traffic or using the network facilities without authorization. A wireless network must be confidential, restricted, and controllable.

Whether wired or wireless, there is no such thing as a completely secure digital link. One can only define a comparative meas-

ure of security in terms of a time and effort to compromise the link. Generally a secure link can be thought of as any link to which the cost of a compromise (in time or other resources) is significantly greater than the value of the contained data or the facility provided by such a compromise.



Exposure of the encryption is the single biggest weakness of a wireless security system as it significantly reduces the cost of compromise. Exposing the encryption of a data stream to all comers provides the opportunity for an interloper to work quietly and undetected on ways to crack the encryption, including brute force attacks. Many of WEPs problems derive from the ease with which packets can be sniffed from the network and analyzed independently of authentication and encryption. The ability to sniff packets is inherently dangerous.

The next barrier to compromise is the strength of encryption. Encryption is used extensively to provide authentication and security. The level of security is derived from the robustness of the encryption algorithms combine with the methods of deployment. Generally speaking, the longer the key used in encryption, the greater degree of security afforded to the network.

Managing the Risk

Managing the risk of a security hole comes down to answering the two fundamental questions:

- 1) **How difficult is it to participate in the packet flow?**
- 2) **How long will it take to crack the encryption, assuming an eavesdropper can obtain access the wireless LAN?**

At RMG, we believe that the best approach to security is to address both these issues, that is, to provide maximum coverage at minimal cost of complexity. If an uninvited user can't see packets, they can't even begin the process of cracking the encryption system. If they vault that hurdle, and can see the packets, then it should then take them a considerable amount of time to crack the encryption.

RMG Security

RMG is fully compliant with all IEEE 802.3 specifications, assuring our users of LAN privacy and security. Customers are assured of Guaranteed Delivery and Workgroup Pairing. These Layer 2 specifications allow the network manager to maintain authorization tables and workgroup identification, which allows for both roaming of legal clients and non-authorization of illegal clients.

- 1) There are no public domain drivers for RMG products. No drivers will pass radio subnet information or encrypted packets unless they are on the same subnet or the private key is known. This provides a first barrier to entry for the would-be hacker. They first need to write a driver for a product about which there is no public information.
- 2) There is a logical 'password' called the Subnet ID, which will

