

Security on the Run

John Pescatore

The wireless world is a wonderful thing, unless you are concerned about security.

ANALYSIS

There is always a gap between the adoption of a new technology and security of the technology reaching the due diligence level, opening a potential Pandora's Box of problems. The benefits of wireless data connectivity to PCs, personal digital assistants (PDAs) and cellphones — any time, any where connectivity — are hard to resist, but the risks are many. This issue of the Mobile and Wireless Spotlight focuses on the critical security issues associated with enterprise use of wireless technologies.

A recent Gartner survey showed that 50 percent of enterprises plan to procure and deploy wireless LANs (WLANs) based on the 802.11 standard. Gartner believes that 20 percent of enterprises already have rogue WLANs in use, deployed by users who were not willing to wait for approved systems to be installed by their IT organization.

If proper security precautions are not taken, such WLANs make an enterprise vulnerable to "drive-by hacking". Gartner provides guidance on benefiting from WLANs, while keeping hackers at bay (see DF-13-8250, "Deploying Safe Wireless LANs"). Martin Reynold's "What's Up With WEP?" (HARD-WW-DP-0093) expands on the technical shortcomings in the current 802.11b security standards.

We recommend that you use application-level security over any wireless connection to avoid vulnerability and interoperability problems in the security features built in at the radio frequency level. Martin Reynold's "Bluetooth's Security Systems: Handle with Care!" (HARD-WW-DP-0092) extends this recommendation to the use of Bluetooth for cable replacement and personal-area networks.

Gartner tracks new technologies through a hype cycle — from the peak of inflated expectation, through the trough of disillusionment, up the slope of enlightenment as the technology overcomes initial problems to the plateau of productivity. Bluetooth has rapidly moved through the initial stages of this cycle and will progress out of the trough of disillusionment as it overcomes its inherent lack of strong security.

Another overhyped wireless area — mobile commerce, using WAP — is also wallowing in the trough of disillusionment. Because the private key infrastructure (PKI) industry found it hard to sell to the wired Web, vendors turned to the wireless Web for the next wave of PKI spending. Vic Wheatman's "Wireless Authentication via PKI: WTLS Is Enough for Now" (M-14-1815) outlines Gartner's view of the reality behind wireless PKI and details the likely progression of key standards in WAP and Wireless Transport Layer Security (WTLS).

Much of the focus in mobile and wireless security has been on protecting the over-the-air signal. However, Gartner believes the largest category of risk today is in the data that is stored on the mobile device, whether on a cellphone, PDA or laptop computer. John Girard details Gartner's policy recommendation for keeping mobile devices secure (see TG-14-2859, TG-14-2860 and TG-14-2861), and provides a Magic Quadrant examining the market for laptop encryption products (see M-13-4933, "Laptop Data Protection Magic Quadrant").

Finally, Geoff Johnson takes a regional focus on wireless security, looking at the key security issues that are unique to the Asia/Pacific wireless market (see TG-13-8270, "Mobile Security in Asia/Pacific"). The Asia/Pacific region has seen the most rapid growth in the use of data and Internet-enabled cellphones because of the DoCoMo i-mode system. Users have received ever-more unsolicited messages and e-mails, and newer technologies raise the specter of cellphone viruses becoming a reality.

Features

Bluetooth's Security Systems: Handle with Care! (HARD-WW-DP-0092) Explores how to implement Bluetooth's security features to safeguard your data. **By Martin Reynolds**

Avoid Gaps and Strengthen Security in Mobile Networks (TG-14-2859) Tips on minimizing security risks from mobile, Internet-connected devices. **By John Girard**

Five Dumb Ways to Expose Mobile Network Vulnerabilities (TG-14-2861) Exposes the vulnerabilities of environments open to wireless and mobile devices. **By John Girard**

Nine Smart Ways to Improve Mobile Network Security (TG-14-2860) Tips on achieving secure mobile networking. **By John Girard**

Laptop Data Protection Magic Quadrant (M-13-4933) What's on the market to stop a stolen laptop from invalidating your security? **By John Girard**

Wireless Authentication via PKI: WTLS is Enough for Now (M-14-1815) Surviving the transition period before strong authentication for wireless transactions arrives. **By Vic Wheatman**

Mobile Security in Asia/Pacific (TG-13-8270) Cultural and legal minefields in Asia/Pacific. **By Geoff Johnson**

Root Trust Compromise Risks: Time to Face Them! (HARD-WW-DP-0094) Backup for the root certificates offered by PK vendors. **By Martin Reynolds**

What's up with WEP? (HARD-WW-DP-0093) Security weaknesses in the WEP algorithms. **By Martin Reynolds**

Deploying Safe Wireless LANs (DF-13-8250) Tips on keeping hackers out of your WLAN. **By John Pescatore, John Girard, Bob Egan, Ken Dulaney and Martin Reynolds**

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509