

The Wireless Industry Can No Longer Ignore Device Security



Decision Point:	Optimizing Wireless Device Solutions
The Bottom Line:	Enterprises and service providers currently underestimate the security risks that next-generation wireless devices create. It's critical that companies implement holistic security solutions with consideration for the transmission and user interface limitations of wireless devices coupled with the computing power and the variety of wide- and local-area communication protocols that they support.
Who Should Read:	CSO, CTO, CIO, CEO, VP of marketing

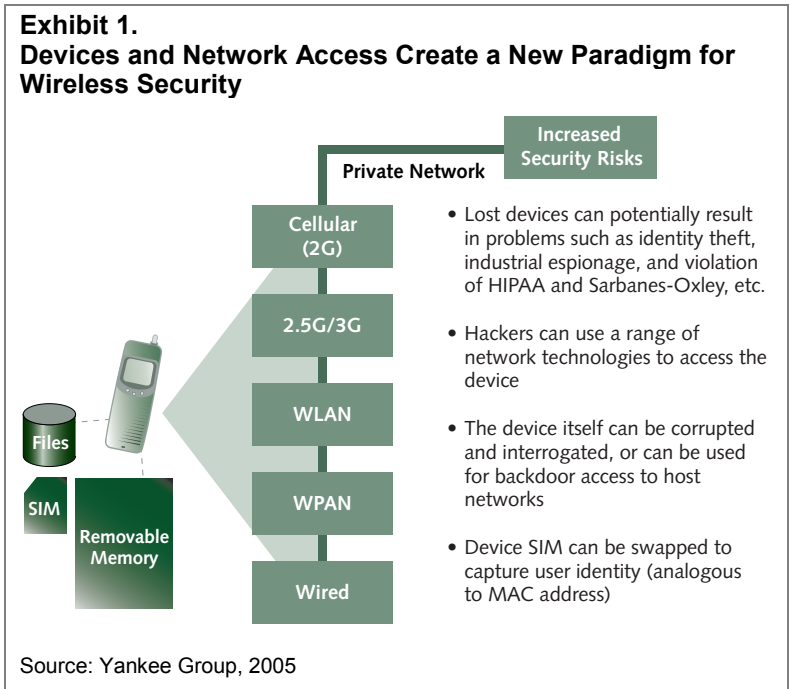
Wireless Global Practice Leader: Keith Mallinson, kmallinson@yankeegroup.com, 617-880-0375

Next-Generation Services Create a Slew of Security Concerns for Wireless Devices

The evolution of wireless from traditional circuit-switched voice to next-generation Internet Protocol (IP) voice and data services creates a variety of security challenges. Traditional circuit-switched architectures essentially are based on closed network environments and specialized technologies. IP utilizes standard protocols and the networks are more open. Wireless devices that traditionally were used for voice and messaging applications are becoming more general purpose and can store significantly more data.

With the transition to IP, a broad range of security issues confront the wireless industry, from those relating to internet-based back-office integration, such as profile management portals, to rogue access points on wireless LAN networks and wireless devices and handsets. This DecisionNote focuses on the emerging security requirements for wireless handsets that support next-generation services.

Devices increasingly support a variety of wireless communication technologies that hackers could compromise. In addition, removable memory and profiles, the user interface, and the physical size and variety of data stored on wireless devices create increased security risks that enterprises and service providers are not adequately addressing (see Exhibit 1).



Broad Adoption of Wireless Security Solutions Is Lacking

The proliferation of advanced wireless applications makes it critical for enterprises and service providers to implement robust device security solutions. Enterprises risk violating regulatory mandates, such as Sarbanes-Oxley and HIPAA (in the medical industry), by having solutions that inadequately protect data stored on devices from interrogation and tampering by hackers. When hackers compromise personal information, the enterprise or service provider responsible is legally obliged to inform all affected individuals. The devices themselves can be the victim of viruses, worms and Trojan horses. Since the Cabir virus, which was the first reported virus designed for mobile devices, hackers have developed a slew of viruses, worms and Trojans to infect mobile devices using a variety of communication techniques, including Bluetooth, MMS and SMS. We expect the variety and potency of mobile device viruses will continue to increase. Enterprise and service provider networks are also vulnerable to attacks by hackers using techniques that take control of the wireless devices. This might range from hackers breaching simple authentication mechanisms by swapping the SIM cards in the handsets of unsuspecting users, to advanced techniques that use worm and Trojan viruses.

A variety of companies offer security solutions. For example, Research In Motion (RIM) has an advanced security solution for mobile e-mail that benefits from having a network operations center and a vertically integrated architecture. Handset vendors such as Nokia offer integrated VPN clients, and others including Columbitech, NetMotion and Padcom offer VPN solutions optimized for wireless devices. Pure-play companies such as Bluefire Security Technologies and Intellisync have developed a suite of security solutions specifically targeting wireless devices. Companies including Qpass and GoRemote offer managed security solutions and companies such as F-Secure, McAfee and Symantec offer virus protection software specifically designed for wireless devices.

Current device security solutions are fragmented and there is a demand for solutions that integrate device security into broader based security management and enforcement solutions. Furthermore, service providers and enterprises need to become more educated about the security risks they face. Recent high-profile security breaches experienced by mobile service providers illustrate this, including one in which hackers compromised personal information Paris Hilton stored via her SideKick device. In addition, in the Yankee Group *2004 Enterprise Wireless Technology Survey*, 31% of respondents stated that they didn't understand wireless wide-area network security and 20% indicated that they didn't fully understand wireless LAN security. Although enterprises that are most vulnerable to security breaches—such as financial and healthcare organizations—currently address security issues, broad industry adoption is lacking.

Recommendations for Enterprises and Service Providers

- **Evaluate and address security issues created with the proliferation of advanced wireless devices.** They must adopt a holistic approach to security that considers the computing and communication power of wireless devices coupled with their challenging user interfaces and limited transmission capabilities.
- **Establish security policies and procedures that can be enforced, and contingencies for managing security problems without major disruptions for users.** Once companies have implemented security measures, the single biggest threat is the users—who are inclined to bypass prudent security practices because of the inconvenience they create and a lack of understanding and guidance.
- **Anticipate and manage the global impact of wireless devices in enterprise and consumer settings and across an endless variety of applications.** On-device security management is critical, with consideration for the entire range of usage modes and associated security requirements that might include authentication, encryption, tamperproof data and auto destruct, virus protection, integrity monitoring, firewall and VPN, depending on the device's operating characteristics.