SECURING WiMAX WIRELESS COMMUNICATIONS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Many government and business organizations are using wireless networks, enabling their employees and contractors with wireless-enabled devices, such as smart phones, to connect to the Internet and the organization's networks. Wireless networks support increased flexibility for organizations, and easier and less costly installations than wired technologies.

Wireless technologies use radio waves instead of direct physical connections to transmit data between networks and devices. While supporting ease of use and installation, and a mobile workforce, wireless networks like any other communication network are vulnerable to risks that could compromise the confidentiality, integrity, and availability of information systems and information. Without proper security precautions, information can be intercepted and altered more easily than when transmitted through physical connections.

The U.S. Government Accountability Office (GAO) recently analyzed leading security practices of federal government organizations for deploying and monitoring wireless networks and technologies in its report, *Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk* (GAO-11-43, November 2010). The GAO recommended that federal agencies implement additional practices to secure their wireless networks, and that governmentwide oversight of wireless networks be improved.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST), which is responsible for developing standards and guidelines for information security under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, has issued several publications explaining secure wireless communications and recommending good practices for protecting wireless transmissions; the most recent is NIST Special Publication (SP) 800-127, *Guide to Securing WiMAX Wireless Communications.*

WiMAX is a widely used technology for communicating over wireless metropolitan area networks (WMANs). These networks, which provide services over an area approximately the size of a city, are usually operated by an organization such as an Internet service provider, a government agency, or a business.

The term *WiMAX* was originally an acronym standing for Worldwide Interoperability for Microwave Access, but it is no longer used as an acronym. WiMAX is a trademark of the WiMAX Forum, an industry trade association that defines the content and scope of

WiMAX technology and publishes technical specifications, which are based on voluntary industry standards.

NIST Special Publication 800-127, *Guide to Securing WiMAX Wireless Communications: Recommendations of the National Institute of Standards and Technology*

Written by Karen Scarfone (formerly of NIST) and by Cyrus Tibbs and Matthew Sexton (of Booz Allen Hamilton), this publication provides information to organizations about WiMAX security capabilities. WiMAX is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.16 family of standards, which were developed through consensus-based standards development processes.

The guide discusses the security of the WiMAX air interface and of user subscriber devices, including security services for device and user authentication; data confidentiality; data integrity; and replay protection. NIST recommends specific courses of action that federal agencies can take to improve the security of their wireless communications; these recommended practices can also assist other organizations considering the implementation of WiMAX systems.

NIST SP 800-127 explains the technology components that compose the WiMAX operating environments, the development of the IEEE 802.16 family of standards, and the product certification program conducted by the WiMAX Forum. One section of the report discusses the WiMAX security mechanisms included in IEEE 802.16 standards, and indicates their functions. Another section examines common vulnerabilities and threats involving WiMAX technologies and recommends countermeasures to improve security.

Included in the appendices to the guide are a glossary of key terms used, a list of acronyms and abbreviations used, and a list of references.

NIST SP 800-127 can be accessed from the NIST Web page: http://csrc.nist.gov/publications/PubsSPs.html.

Vulnerabilities, Threats, and Countermeasures

Some of the **vulnerabilities** of WiMAX technology are not addressed in the IEEE 802.16 specifications. The IEEE 802.16 standards specify two basic security services: authentication and confidentiality. Authentication is the process of verifying the identity of a WiMAX device. Confidentiality in the IEEE 802.16 specifications is limited to protecting the contents of WiMAX data messages so that only authorized devices can view them. The IEEE 802.16 standards do not address other security services such as availability and confidentiality protection for wireless management messages. These services and end-to-end security (device-to device) services must be provided through additional security controls that are not specified in the IEEE standards.

WiMAX systems are susceptible to WiMAX-specific **threats** as well as threats common to all wireless technologies. WiMAX network threats include compromising the radio links between WiMAX nodes. Line-of-sight (LOS) WiMAX systems pose a greater challenge to attack than do non-line-of-sight (NLOS) systems because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. Non-line-of-sight systems provide wireless coverage over large geographic regions; this feature expands the potential staging areas for both clients and adversaries.

A combination of management, operational, and technical **countermeasures** should be used to reduce or mitigate the risks inherent in WiMAX systems.

• **Management countermeasures** deal with problems related to risk, system planning, or security assessment by an organization's management. Organizations should develop a wireless security policy that addresses WiMAX technology. A security policy is an organization's foundation for designing, implementing, and maintaining properly secured technologies. WiMAX policy should cover the design and operation of the technical infrastructure and the behavior of users.

• **Operational countermeasures** include controls that are executed by people, such as personnel security, physical environment protection, configuration management, security awareness and training, and incident response. These controls should be documented in a system security plan (SSP) which is maintained by all parties involved with WiMAX system operations. SSPs are living documents that provide an overview of the security requirements of a system and describe the controls in place to meet those requirements; this includes all system hardware and software, policies, roles and responsibilities, and other documentation materials. The documentation is a security control, since it formalizes security and operational procedures for a system.

Physical security is fundamental to ensuring that only authorized personnel have access to WiMAX equipment. Physical security includes measures such as physical access control systems, personnel security and identification, and external boundary protection.

Organizations should consider the implications of spectrum allocation as it impacts system availability. Due to the proliferation of unlicensed wireless technologies, interference may become an implementation obstacle when systems are operating in an unlicensed spectrum. Counter-interference technologies should be used to ensure system availability.

Site surveys are used to construct the foundation for a WiMAX system's design to ensure system availability. Long-distance radio transmissions should be tailored and optimized for radio frequency (RF) obstacles and interference sources. Site surveys help limit range to provide an organization with operational awareness of a system's coverage area. Site survey tools include terrain maps, global positioning systems, RF propagation models, spectrum analyzers, packet analyzers, and additional tools which provide a more thorough understanding of the environment's RF landscape. Conducting a WMAN site

survey requires specialized skills, and it is typically provided as part of the overall vendor solution. Organizations should, at a minimum, involve themselves in the site survey process and document its findings in the system security plan.

As with all wireless technologies, operational countermeasures may not provide protection against general wireless threats such as denial of service, eavesdropping, man-in-the-middle, and message replay. Operational controls often require highly specialized expertise and rely upon the use of both management and technical controls.

• **Technical countermeasures** are system safeguards, such as authentication measures, access control, auditing, and communication protection. Technical countermeasures are often designed into WiMAX systems before implementation and vary widely between vendors. Before implementing a WiMAX system, an organization should consult WiMAX vendors to gain a better understanding of potential system reconfiguration constraints and the need for compensating controls to address technical security needs that the WiMAX product may not address. Technical countermeasures include protection of confidentiality and integrity, support for authentication and authorization, client device security, and regulation application of software patches, upgrades, and updates.

NIST Recommendations for Improving WiMAX System Security

NIST recommends that organizations take the following steps to improve WiMAX system security:

• **Develop a robust WMAN security policy and enforce it.**

A security policy is an organization's foundation for designing, implementing, and maintaining properly secured technologies. WMAN policy should address the design and operation of the technical infrastructure and the behavior of users. Client devices should be configured to comply with WMAN policies, such as disabling unneeded services and altering default configurations. In addition, policy-driven software solutions can be implemented on client devices to prevent or allow certain actions to take place when specific conditions are met. Policy-driven software helps ensure that client devices and users comply with an organization's defined policies.

• **Assess WiMAX technical countermeasures before implementing a vendor's WiMAX technology.**

Currently, few WiMAX products employ Federal Information Processing Standard (FIPS)-validated cryptographic modules. Consequently, vendors often integrate their WiMAX products with other security solutions that meet FIPS requirements. WiMAX interoperability certifications do not extend to these add-on approaches, which means there may be no assurance that the vendor's offering will function as intended. Given the diversity in potential approaches and the risk that integration issues could affect the security of the system, organizations should work closely with WiMAX vendors to gain a better understanding of potential system configuration constraints. Organizations should

independently determine the need for compensating controls to address technical security functionality that the WiMAX product may not address.

- **Require mutual authentication for WiMAX devices.**

WiMAX technology supports mutual device authentication between a base station (BS) and a user's subscriber unit (i.e., mobile phone, laptop, or similar device), but the feature must be activated to realize the benefit of the approach. Organizations should strongly consider WiMAX solutions capable of supporting Extensible Authentication Protocol (EAP) methods for mutual authentication as recommended in NIST SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*. EAP methods that support mutual device authentication usually support integrated user authentication using passwords, smart cards, biometrics, or some combination of these mechanisms. WiMAX solutions that cannot meet these criteria should employ a different means of authentication at a higher layer, such as encryption overlay or virtual private network (VPN). Specifically, native IEEE 802.16-2004 authentication does not support mutual device authentication and thus should be avoided.

- **Implement FIPS-validated encryption algorithms employing FIPS-validated cryptographic modules to protect data communications.**

WiMAX communications consist of management and data messages. Management messages are used to govern communications parameters necessary to maintain wireless links, and data messages carry the data to be transmitted over wireless links. Encryption is not applied to management messages to increase the efficiency of network operations, while data messages are encrypted natively in accordance with the IEEE standards. IEEE 802.16e-2005 and IEEE 802.16-2009 support FIPS 197, *Advanced Encryption Standard (AES)*. IEEE 802.16-2004 supports the Data Encryption Standard in Cipher Block Chaining mode (DES-CBC). DES-CBC has several well-documented weaknesses, making it a vulnerable encryption algorithm that should not be used to protect data messages. In 2005, the Data Encryption Standard (FIPS 46-3) was withdrawn.

Federal agency communications that require protection through encryption must use products with cryptographic functionality that is validated under the NIST Cryptographic Module Validation Program (CMVP), as meeting requirements specified in FIPS 140, *Security Requirements for Cryptographic Modules*. For WiMAX solutions that do not support FIPS-validated algorithms employing FIPS-validated cryptographic modules, organizations that must protect the confidentiality of their WiMAX communications should deploy overlay encryption solutions, such as a FIPS-validated VPN solution.

The GAO report notes that "Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks."

Future Activities

NIST plans to develop additional guidance on wireless security covering:

• Technical steps to mitigate the risk posed by dual-connected laptops;
• Governmentwide secure configurations for wireless functionality on laptops and for BlackBerry smart phones;
• Appropriate ways to centralize management of wireless technologies based on business need; and
• Criteria for selecting tools and the appropriate frequency of wireless security assessments, along with recommendations for continuous monitoring of wireless networks.

For More Information

IEEE Standards. WiMAX has evolved from a standard for wireless metro area networking to a specification for a broader, more cellular-like architecture. The IEEE 802.16 family of standards serves a broad market, and WiMAX technology continues to adapt to market demands and to provide enhanced user mobility. An amendment, IEEE 802.16e-2005, enabled mobile WiMAX operations and provided significant security enhancements to the predecessor standard by incorporating more robust mutual authentication mechanisms, as well as support for the Advanced Encryption Standard (AES). Certification of products implementing IEEE 802.16e-2005 was initiated in 2008.

The IEEE standards that specify WiMAX technology are:

IEEE Standard 802.16-2004, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE, 2004.

IEEE Standard 802.16e-2005, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*, IEEE, 2005.

IEEE Standard 802.16-2009, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems*, IEEE, 2009.

IEEE Standard 802.16j-2009, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems: Amendment 1: Multiple Relay Specification*, IEEE, 2009.

Information on the WiMAX Forum™ can be found at http://www.wimaxforum.org/home/.

Information on the WiMAX Forum™ program for certification of products can be found at http://www.wimaxforum.org/certification/program.

The Government Accountability Office (GAO) Report 11-43, *Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk* (November 2010) is available at http://www.gao.gov/new.items/d1143.pdf.

NIST publications that provide guidance and baseline requirements for information system configuration and security measures for wireless devices include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
NIST Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
NIST SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*.

For information about NIST standards and guidelines for information security, as well as other security-related publications, see the NIST Web page http://csrc.nist.gov/publications/index.html.

Information about the NIST Cryptographic Module Validation Program (CMVP) can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.