New publication offers security tips for WiMAX networks

October 7 2009

Government agencies and other organizations planning to use WiMAX -- Worldwide Interoperability for Microwave Access—networks can get technical advice on improving the security of their systems from a draft computer security guide prepared by the National Institute of Standards and Technology.

WiMAX is a wireless protocol that can cover an area that incorporates a few miles such as a campus or small town. It has a larger reach than the more familiar "WiFi" networks used in offices or homes, but smaller than wireless areas covered by cell phones. The technology, guided by standards issued by IEEE, originally was designed to provide last-mile broadband wireless access as an alternative to cable, digital subscriber line (DSL) or T1 service. In recent years its focus has shifted to provide a more cellular-like, mobile architecture to serve a broader audience.

WiMAX was used after the December 2004 tsunami in Aceh, Indonesia after the communication infrastructure was destroyed and also after Hurricane Katrina along the coast of the Gulf of Mexico.

Special Publication 800-127 "Guide to Security for WiMAX Technologies" discusses WiMAX technology's topologies, components, certifications, security features and related security concerns. It covers the IEEE 802.16 standard for WiMAX and its evolution up to the 2009 version.

The main threat to WiMAX networks occurs when the radio links

between WiMAX nodes are compromised. The systems are then susceptible to denial of service attacks, eavesdropping, message modification and resource misappropriation.

SP 800-127 recommends taking advantage of built-in security features to protect the data confidentiality on the network. It also suggests that organizations using WiMAX technology should:

- Develop a robust WiMAX security policy and enforce it.
- Pay particular attention to WiMAX technical countermeasure capabilities before implementing WiMAX technology.
- Use WiMAX technology that supports Extensible Authentication Protocol methods as recommended in NIST SP 800-120 (available at http://www.csrc.nist.gov/publications/PubsSPs.html#800-120.)
- Implement Federal Information Processing Standards-validated encryption to protect their data communications.

More information: The draft version of NIST SP 800-127 is open for public comment through October 30, 2009. The document is available online at csrc.nist.gov/publications/PubsDrafts.html#800-127

Source: National Institute of Standards and Technology (news : web)