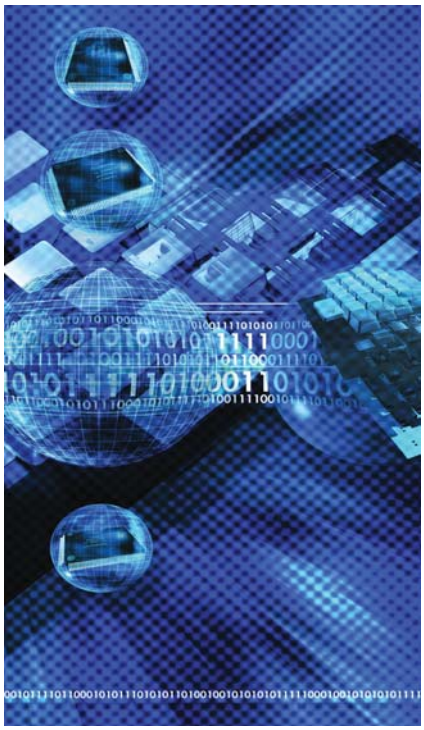
Systems and Network Analysis Center
Information Assurance Directorate

Security Guidance for Bluetooth Wireless Keyboards and Mice



OVERVIEW

The Challenge

~ Many U.S. Government customers want to use wireless keyboards and mice on their networks, particularly in conference rooms for audio/video systems. How can this be done while imposing as little risk as possible to the connected network?

The Solution

~ NSA/CSS' System and Network Attack Center released a security advisory, IAA-004-2004, that provides recommendations on using Bluetooth technology. The advisory can be found on SIPRNET at:

www.iad.nsa.smil.mil/resources/library

Bluetooth is a short-range wireless personal area network (PAN) technology found in cell phones, personal digital assistants, laptop computers, headsets, and peripherals. In 2003, Bluetooth devices began shipping in volume. Like any integrated wireless technology, Bluetooth introduces potential network security risks into government and military communications computing devices.

The security problems related to Bluetooth technology are widely known in the security community and a number of terms have been adopted to describe various Bluetooth attacks:

"***Blueprinting***" is a method to remotely fingerprint Bluetooth-enabled devices.

"***BlueStumbling***" allows an adversary to locate and identify users based on their Bluetooth device addresses.

"***BlueSmack***" performs a denial of service attack over the Bluetooth connection making the device unavailable.

The use of Bluetooth-enabled keyboards and mice introduces an avenue of attack for an adversary to capture keystrokes and spoof a user to gain access to a host machine. It has been shown that a Bluetooth connection can be made from distances of up to one mile.

To mitigate the risk of compromise of these devices, it is important to utilize both authentication and encryption capabilities on Bluetooth communication ports. Enable the connection only when needed and make devices discoverable only when necessary. Be sure to require pairing (PIN exchange) for each new connection even if it has previously been authenticated. Although these guidelines will not guarantee protection, they will provide several additional layers of defense.

The goal of the network security designer is to reduce the risk to acceptable levels. Note that the owners of the networks are the only ones that can determine what level of risk is acceptable once they have evaluated the threat, the vulnerabilities, and the value of their information.

For more details on securing Bluetooth technology, and other security information, visit the NSA IAD library on SIPRNET.

SNAC DoD, 9800 Savage Rd Ft. Meade, MD 20755-6704 410-854-6294 DSN 244-6294 FAX: 410-854-7321 www.nsa.gov/snac

DC6M6-06-12946