A StenoCast White Paper

3949 Ruffin Road, Suite E
San Diego, CA 92123
858.279.5700
www.StenoCast.com

StenoCast's Wireless Bluetooth Security

Michael Appelman, President

Contents

Introduction

It was brought to our attention that, due to a potential security breach of a Wi-Fi wireless system, the court has undertaken a review of all wireless technology utilized in courtrooms within its jurisdiction. We will not endeavor to comment on the merits or demerits of Wi-Fi wireless systems. Our observations and analysis will be limited to Bluetooth in general, and StenoCast's Bluetooth wireless realtime systems in particular, limited further to wireless communications within the confines of the walls of each individual courtroom.

Much of the technical data regarding Bluetooth is provided by the Information Technology Laboratory. The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems.

The Dilemma

Modern courtrooms require the transfer of data (realtime) from court reporters to judges, attorneys and clerks. Prior to 2004 all such transfers were handled by hard-wiring the court reporter's computer to each client (judge/attorney/clerk). The actual wires handling the transfer of data were serial cables (RS232). The industry as a whole adopted serial technology. All steno machines, all court reporting software and all litigation-support software are designed to transmit and receive data via serial communications over COM ports. This legacy technology has proved to be a blessing in disguise.

The three current options available to the courts are:

1) Serial cables.
2) Wi-Fi router.
3) StenoCast's Bluetooth wireless system.

Option 1 is problematic in that modern computers no longer utilize serial ports. To connect to a court reporter's realtime system would require utilizing RJ45 adapters, plus USB-to-serial adapters. The primary reason court reporters were looking for an alternative to the serial cables/adapters problem was because of the incompatibility issue of USB-to-serial adapters with certain computers and, in addition, court reporter and litigation-support software. The combinations of incompatibility were significant.

Option 2 is considerably more reliable than utilizing serial cables, but most courts have been reluctant to allow a judge to connect a courthouse's secure networked computer to a court reporter's Wi-Fi router that all other parties connect to.

The Solution

Option 3: To provide a secure wireless transmission from Point A to Point B requires one thing: hardware-level security at Point A and Point B. StenoCast manufactures Point A and Point B.

StenoCast's Bluetooth wireless realtime systems were designed to meet and exceed any courtroom security concerns. The system is designed to allow only a one-way transmission of data from the court reporter to a judge and/or one-way transmissions to attorneys. The hardware does not allow transmission of data back to the court reporter or between the parties.

Pairing of transmitters and receivers is done by StenoCast, not in the field by our customers. Each transmitter (plugged into the court reporter's computer) is programmed to transmit to receivers (plugged into client computers) specifically paired to it. Each receiver is paired to receive data from a single, specific transmitter. The transmitter will not send data to any other Bluetooth device that has not been specifically paired to it. In addition, other Bluetooth devices not specifically paired to a StenoCast transmitter would not be able to detect the wireless transmission. The StenoCast wireless transmissions are set to "non-discovery mode."

As previously mentioned, all StenoCast products are designed and built with hardware-level security. They are designed to provide a level of security that is in addition to the software and firmware solutions provided by the Bluetooth SIG, which includes:

- **Authentication:** verifying the identity of communicating devices.
- **Confidentiality:** preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.
- **Authorization:** allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

In addition, StenoCast wireless realtime employs Security Mode 3, a link level-enforced security mode, where our Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandates authentication and encryption for all connections to and from the device. This mode supports authentication (unidirectional or mutual) and encryption. The authentication and encryption features are based on a separate secret link key that is shared by paired devices, once the pairing has been established.

Bluetooth authentication is handled as follows:

1) The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.

2) The claimant uses the E_1 algorithm9 to compute an authentication response using his unique 48-bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E_1 output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later to create the Bluetooth encryption key.

3) The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier.

4) The verifier compares the SRES from the claimant with the value that it computed.

5) If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication has failed.

Performing these steps once accomplishes one-way authentication. The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated with the verifier and claimant switching roles.

Confidentiality is maintained as follows:

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. StenoCast employs Encryption Mode 3.

Encryption Mode 1—No encryption is performed on any traffic.

Encryption Mode 2—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.

Encryption Mode 3—All traffic is encrypted using an encryption key based on the master link key.

The encryption key provided to the encryption algorithm is produced using an internal key generator (KG). The KG produces stream cipher keys based on the 128-bit link key, which is a secret that is held in the Bluetooth devices, a 128-bit random number (EN_RAND), and the 96-bit ACO value. The ACO is produced during the authentication procedure, as shown in Figure 3-4.

The Bluetooth encryption procedure is based on a stream cipher, E_0. A key stream output is exclusive-OR-ed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR).10 The encryption function takes the following as inputs: the master identity (BD_ADDR), the 128-bit random number (EN_RAND), a slot number, and an encryption key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet; the ciphering engine is also reinitialized with each packet while the other variables remain static.

Bluetooth Authorization:

In addition to the four security modes, Bluetooth allows two levels of trust and three levels of service security. The two Bluetooth levels of trust are trusted and untrusted. A *trusted device* has a fixed relationship with another device and has full access to all services. StenoCast transmitters and receivers are configured as trusted devices. An *untrusted device* does not have an established relationship with another Bluetooth device, which results in the untrusted device receiving restricted access to services. Three levels of security have been defined for Bluetooth services. These levels allow the requirements for authorization, authentication, and encryption to be configured and altered independently. The service security levels are as follows:

Service Level 1—Requires authorization and authentication. Automatic access is granted only to trusted devices; untrusted devices need manual authorization.

Service Level 2—Requires authentication only; authorization is not necessary. Access to an application is allowed only after an authentication procedure.

Service Level 3—Open to all devices, with no authentication required. Access is granted automatically.

StenoCast Wireless realtime systems employ Service Level 1 security features.

Summary

StenoCast wireless realtime systems are deployed in hundreds of courtrooms around the world, providing an unparalleled level of secure, yet simple-to-use wireless technology that has transformed and streamlined the administration of justice. A court reporter's realtime transcription is invaluable, prompting many judges to "refuse" to take the bench unless there is a reporter providing realtime. Some law firms consider it malpractice on their part to go to trial without receiving realtime from the court reporter.

We would suggest it is a mistake to, in a sense, throw the baby out with the bath water. StenoCast manufactures unique wireless realtime equipment that is uniquely secure and reliable. You may have issues with other forms of wireless technology, but we do not believe, after a thorough examination, that you have issue with our products.