Microsoft AES (Advance Encryption Standard) technical factsheet

In today's mobile world, wireless technology is everywhere. We use it to get online on the go, connect mobile accessories to our PCs, listen to music from our phone—and the list goes on. Because wireless technology is so common, we often assume it's safe. Many of us use it to enter passwords, send personal data, and share confidential work information. The reality is that every point in a wireless communication system is a potential vulnerability, and without the proper security measures in place, your private information could be at risk.

To protect our data, we typically create difficult passwords, keep our operating systems up to date, and use the latest anti-spyware software. But many business are unaware that choosing the wrong wireless keyboard can also expose their confidential information. Wireless keyboards transmit keystrokes over the air to our PCs, making them a point of attack for cyber-thieves.

That's why Microsoft offers a line of keyboards and desktop accessories that use the 128-bit Advanced Encryption Standard (AES) cipher to encrypt the transmission of keystrokes. These products can help prevent hackers from intercepting usernames, passwords, and other sensitive information during wireless transmission.

AES is a specification for the encryption of electronic data established by the National Institute of Standards and Technology (NIST). Considered one of the most secure encryption standards in use today, it has been adopted by the United States government and other countries around the world to protect confidential data and information.

Below you can find some key facts about the implementation of AES in Microsoft keyboards:

Advanced cryptography
Microsoft AES keyboards use Microsoft Windows CryptoAPI, which is the same cryptographic resource found in Microsoft Windows Server products in government and corporate datacenters worldwide.

Secure key transmission
No AES encryption key information is ever transmitted via radio, even in the factory. Instead, the keys are programmed into each accessory and receiver using a direct physical connection.

Encryption key protection
Once the AES encryption key information is programmed in the factory, firmware prevents access to it from the outside. The firmware contains no test modes or backdoors that could expose or change it.

Session identifiers, sequence numbers and random data
An attack methodology known as a "session replay" could allow intruders to mimic a device or computer without decrypting a transmission. In such an attack, the attacker records an entire encrypted session, such as a login, and replays it later to repeat the login while the user is away. Microsoft AES devices prevent this by using a unique identifier for each session. As a result, a transmission will only work once within its own session, and a replay will not trick the system into believing it is legitimate.

A related methodology could allow intruders to modify a session in progress. In this form of attack, the attacker captures and inserts repetitions of valid messages within a session, or blocks messages within a session to modify the session. For example, an attacker might try to block the decimal point in a financial transaction by interfering with the radio at the right time. Microsoft AES transmissions contain sequencing information to protect the integrity of the transmission sequence—thus preventing such attacks.

Inclusion of random data prevents attackers from using “frequency analysis” to compromise security. In a frequency analysis attack, the attacker captures data over a period of time and measures the frequency of identical messages. The attacker then matches those packets with the frequency of typical expected messages, such as typing the letter ‘e’ on the keyboard. In doing so, the attacker hopes to identify the ‘e’ message, even though it is encrypted, based on how often the message is seen. By adding random data to each message, each message is unique even if the same letters are typed over and over. This prevents frequency analysis from finding identical messages to track.