A Review of Bluetooth Attacks and How to Secure Mobile Workforce Devices

Keep your people safe against Bluetooth hackers

Source: http://www.webroot.com/us/en/business/resources/articles/corporate-security/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices

Bluetooth is best known as the wireless technology that powers hands-free earpieces. Depending on your point of view, people who wear them either:
a) Look ridiculous (especially if shining a bright blue LED from their ear);
b) Appear mad (when apparently talking to themselves); or
c) Are sensible, law-abiding, safety-conscious drivers.

Whichever letter you pick, insidious security issues remain around Bluetooth attacks and mobile devices. While most of the problems identified five to 10 years ago have been straightened out by now, some still remain. And there's also good reason to be cautious about new, undiscovered problems.

Here are a few examples of the mobile security threats in which Bluetooth makes us vulnerable, along with tips to secure your mobile workforce devices.

General software vulnerabilities

Software in Bluetooth devices – especially those using the newer Bluetooth 4.0 specification – will not be perfect. It's unheard of to find software that has zero security vulnerabilities.

As Finnish security researchers Tommi Mäkilä, Jukka Taimisto and Miia Vuontisjärvi demonstrated in 2011, it's easy for attackers to discover new, previously unknown vulnerabilities in Bluetooth devices. Potential impacts could include charges for expensive premium-rate or international calls, theft of sensitive data or drive-by malware downloads.
To combat this threat: Switch off your Bluetooth when you're not using it.

Eavesdropping

Bluetooth – named after the Viking king, Harald Bluetooth Gormsson, thanks to his abilities to make 10th-century European factions communicate – is all about wireless communication. Just like with Wi-Fi, Bluetooth encryption is supposed to stop criminals listening in to your data or phone calls.

In other words, eavesdropping shouldn't be a problem. However, older Bluetooth devices use versions of the Bluetooth protocol that have more security holes than a tasty slice of Swiss. Even the latest specification (4.0) has a similar problem with its low-energy (LE) variant.

To combat this threat: Ban devices that use Bluetooth 1.x, 2.0 or 4.0-LE.

Denial of service

Malicious attackers can crash your devices, block them from receiving phone calls and drain your battery.

To combat this threat: Again, switch off your Bluetooth when you're not using it.

Bluetooth range is greater than you think

Bluetooth is designed to be a "personal area network." That is to say, devices that are more than a few feet away should not be accessible via Bluetooth.

However, you're not safe if you simply ensure there's distance between you and a potential attacker; hackers have been known to use directional, high-gain antennae to successfully communicate over much greater distances. For example, security researcher Joshua Wright demonstrated the use of such an antenna to hack a Bluetooth device in a Starbucks from across the street.

To combat this threat: Once again, switch off your Bluetooth!

Bluetooth headsets

Wright has also demonstrated serious flaws in many popular Bluetooth headsets. By exploiting these vulnerabilities, attackers can eavesdrop on your conversations with the people around you, not just your phone calls. Built-in hands-free car kits can also be vulnerable.

The device becomes, in effect, a mobile bugging device, transmitting everything it hears to an attacker.

To combat this threat: Make sure you change the default PIN code to something hard to guess. And yup… switch off the headset.

See the Bigger Picture

It's vital to develop and communicate company policies for mobile device security – including Bluetooth – so that your business's data aren't compromised and your users can work safely when mobile. While all mobile devices present risks that need to be addressed, Bluetooth security is one often-overlooked piece of the mobile security puzzle.

By Richi Jennings