Crossing the Digital Divide (v41)

“Leaky Faucets”

By Joseph Feigon for the Observer

Being aware of one’s surroundings isn’t a given – we train our children to look both ways before crossing a street, we’re taught to come to a full stop at an intersection and look both ways before proceeding. Learning to be aware of those things around us is somewhat straight forward in a physical world, but what of the digital universe?

Software patches, antivirus and anti-malware signature updates, frequent scanning of your PC, and judicious backups (and an occasional verification) will go a long way in keeping your digital footprint controlled. You’ve been good about updating your passwords and making them complex? You’ve got your wifi network setup for WPA or WPA2 encryption, right?

I’ve been talking about IoT, the Internet of Things. Computers (and computational devices) are getting smaller and smaller, and these devices are often equipped with radios (wifi, Bluetooth, etc.) that can (sometimes) be configured for added security. But wait, I hear you, finding the settings, let alone changing them, is often an exercise in frustration. Bluetooth enabled devices are becoming commonplace, we see them in cars, in our phones, our computers, appliances and more.

Bluetooth is a radio frequency designed for really short “hauls”, e.g., from a headset to your Smartphone. Bluetooth is the magic that was designed to reduce wires and cables between speakers, and sound systems.

You’ve installed WhatsApp or Signal, and your friends have done the same, and you’re now assuming end-to-end encryption is in place, right? Or is it?

If you use a Bluetooth device, your conversations could be recorded, without decryption, even if your communication channel is secure (Signal/WhatsApp/etc.).

The following text was written by Richi Jennings of Webroot:

> #### *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 brands of headset. 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.

Keep control of those things you can control.