INDEFINITELY WILD (/2048321/WES-SILER)

Thieves Are Using Bluetooth to Target Vehicle Break-Ins

How to keep your devices safe when you park at a trailhead

By Wes Siler

Published
Dec 9, 2019

My friend Joe had his MacBook and iPad stolen from the back of a locked car over Thanksgiving. So far, so normal, right? Well, the thieves only broke the small window immediately adjacent to where his devices were hidden and only took the backpack containing them. Police told him it was likely they'd used a Bluetooth scanner to target his car and even located exactly where his devices were before breaking into it.

When he texted me about what happened, I turned to Google to see what a Bluetooth scanner was and immediately found dozens of smartphone apps. The first one I downloaded didn't just show me the signal strengths it detected, it also listed the specific types of devices and even displayed pictures of them—you know, for easy identification. Using signal strength as a distance meter, I found the phone my fiancée misplaced before she went to work. Another app displayed a live list of the devices commuters had in their cars while driving past my house. These apps are free and take no technical know-how or experience whatsoever to use. While they aren't designed specifically to aid thieves (developers need tools like these when designing Bluetooth accessories), it'd be hard to imagine a more powerful asset for criminals.

Bluetooth is a wireless transmission standard that a whole host of devices use to transmit data over short distances. It's what your phone uses to pair with your car stereo and what your AirPods use to connect with your phone. These days all manner of devices use it, including tablets, laptops, cameras, speakers, and phones—

basically, most things a thief may want to steal, except for your keys and cold hard cash. (Although if you use a Tile (https://www.thetileapp.com/en-us/products?utm_campaign=830750117&utm_source=google&utm_medium=cpc&utm_content=341425633155&utm_term=tile-e&adgroup=45437686794&&gclid=CjwKCAiA8qLvBRAbEiwAE_ZzPZTZy5r2UpYzcUQlall-Wc51X1FRp0_aUHz5SS68no-nUdQnUO9liB0CA0wQAvD_BwE&gclsrc=aw.ds) or similar locater dongle on your key chain or in your wallet, then those are discoverable using a Bluetooth scanner, too.) No pairing or security protocols are necessary; the scanners simply locate the signal a device emits and then evaluate its strength and frequency. Comparing that data against a database, they're able to identify exact devices using a digital fingerprint.

This isn't just some crazy theory Joe and I have. California, where he was visiting when his car was broken into, is currently experiencing an epidemic of vehicle break-ins, and police there report that thieves are using the technology.

"There are some people, auto burglars, who actually detect that signal and target your car for that," a San Jose Police Department representative told CBS (https://sanfrancisco.cbslocal.com/2019/11/26/thieves-really-can-use-bluetooth-to-find-hidden-devices-laptops-in-your-car/). San Francisco saw a 24 percent increase in vehicle break-ins between 2016 and 2017, and while 2018 saw a slight decrease, 2019 is on track to be a record year (https://www.latimes.com/california/story/2019-12-02/california-car-burglaries-lawmakers-loophole).

This vulnerability has the potential to impact people outside of major cities, too. Where I live in southwest Montana, local web communities around various outdoor activities often light up with reports of vehicle break-ins at popular trailheads. So far those break-ins seem to follow the usual pattern: smash-and-grabs targeting purses, wallets, or anything of value that might turn up. They're random acts with relatively low payoffs, but an ability to see exactly what your vehicle may be hiding, and calculating that value ahead of time, could encourage thieves to work harder to get into the more inaccessible areas of your vehicle when they know the reward for committing the crime. And because seeing what you're hiding only requires a smartphone app, those thieves have the ability to do their sleuthing undetected. One more person staring at their phone in a parking area isn't going to stand out.

So what can you do to keep your stuff safe? Putting a device in airplane mode or entirely powering it off will both work, according to a report in *Popular Mechanics (https://www.popularmechanics.com/technology/security/a29835980/technology-theft-rfid-bluetooth/)*. Some devices may still emit trace Bluetooth signals while sleeping, so closing the lid on your laptop isn't enough. For additional protection, you can place those devices in a Faraday fabric sleeve (https://www.amazon.com/dp/B07LCS41CN/?tag=outsideonlws-20) or wrap them in a blanket made from the same material (https://www.amazon.com/dp/B01LBFCJ7O/?tag=outsideonlws-20). Of course, the safest method remains the same as it always has: treat this as yet another reminder that you shouldn't leave valuables in your car at the trailhead or anywhere else.

Lead Photo: Duncan Rawlinson (https://www.flickr.com/photos/thelastminute/26382925854)/Creative Commons (https://creativecommons.org/licenses/by-nc/2.0/)