Dark Net Daily

Your Clearnet source for Darknet news.

Interview with Michael Altfield, The Mind Behind BusKill – The World's First USB Kill Cord

Interviews News Privacy

Interview with Michael Altfield, The Mind Behind BusKill – The World's First USB Kill Cord

December 16, 2021 Admin

0:00 / 1:35

Imagine you're in a San Francisco public library. You're accessing sensitive data on your laptop when you get distracted by a couple's tiff. Next thing you know, someone has swooped in and snatched your laptop right out from in front of you. Now, your privacy has now been compromised and your data is in serious danger – all in a matter of seconds. Depending on what programs you had open you could have lost access to personal emails, banking documents, cryptocurrency wallets, private keys and other sensitive data.

Michael Altfield saw this problem and created a solution.

Introducing BusKill, the USB kill cord for your laptop that lets you lock, shutdown, or self-destruct when it's physically separated from you. BusKill has been featured in Forbes, PCMag, CoinDesk and ZDNet just to name a few. Keep reading to learn about Michael's journey to bring BusKill to life and how you can get your hands on one of your very own.

For those who may not yet know, who is Michael Altfield?

I'm the Founder of the BusKill open-source project.

I've been building computers since I was 14. First quake game servers. Then LAMP web servers. Mostly I'm a Linux SysAdmin by trade, with a passion for security and privacy.

At some point in 2008, I started playing with smtp and ettercap and realized emails and web traffic could be spoofed and read by third parties, so I picked-up gpg and https.

These days I train journalists and activists on OpSec. I tell them to protect their computer and accounts by using strong passwords, TOTP 2FA, FDE, etc. But there's always been this, like, glaring physical security hole: what do you do if someone physically steals your laptop after you've authenticated?

Say I'm training a journalist that's going to be embedding themselves in a very dangerous situation in an oppressive regime. Sure, they have FDE and protonmail with 2FA or whatever, but how does that help them if the secret police bust-down their door and snatch the laptop right out of their hands when they're reading their emails? How can they protect their accounts and the data on their computer in this situation?

That's why I invented BusKill; it's like a physical trip wire that will trigger your computer to lock or shutdown if your laptop is physically taken away from you while you're using it.

What is Buskill?

BusKill is a laptop kill cord — it's a hardware Dead Man's Switch that executes some user-configurable trigger when your machine is physically separated from you.

No video with supported format and MIME type found.

It's a USB cable (with a magnetic breakaway in-line) that runs from your laptop to a carabiner clipped to your belt. If your laptop is snatched off the table (or you're tackled to the ground), then the cable's connection will be severed and your laptop's screen will lock.

Why the name BusKill?

USB stands for Universal Serial BUS. BusKill is a Kill cable that uses the usB.

It's very, very simple. And it works in Linux, Windows, and MacOS.

You insert the cable, double-click the app, and click the "arm" button in the app. Disconnect the cable, and your screen locks.

Where did the idea and inspiration for your product come from?

Actually, though I design BusKill for journalists — the original use-case was for personal use.

I spent a lot of time working remotely while traveling around America and Asia — sleeping in crowded hostels at night and working out of cafes and co-working spaces by day (the internet in hostels is terrible).

I always felt super vulnerable in public spaces whenever I logged-into my online banking. Once I had to file my taxes in Brazil and I just felt so unsafe handling those documents in a public space in Rio — even with my back against a wall.

Of course I'm confident that my data is safe when my laptop is off and encrypted, but I needed a solution to trigger my computer to shutdown if it was grabbed by a snatch-and-run thief.

I used BusKill for years before I ever published the idea in 2020.

Nothing hardware-based that's designed for folks operating in a high threat model.

There's one guy who made a cool lazer tripwire, but it was designed more as a joke to minimize a video game when your boss walks into your office.

Most of the "auto lock" apps are radio-based And most of these apps are designed more for convenience than security. For example, they unlock your machine when you walk back to your laptop — no auth required.

There's nothing on the market like BusKill, and that's why I'm so compelled to make this tech accessible.

Why use BusKill over a radio-based dead man switch?

Most of these "auto lock" apps are radio-based. Not only are radio/heartbeat solutions full of false-positives (and therefore tuned to be exceedingly slow), any radio-based solution just opens the floodgates for potential attack like radio jamming, replay attacks, etc.

These radio-based apps are designed for convenience — not security.

What was the process like bringing this product to life?

It's been a long journey.

If you're just a TAILS user, then you'll probably just use the hardware cable (since ejecting the TAILS USB drive triggers the auto-shutdown sequence). But for Linux, Windows, and MacOS users, I wrote a cross-platform GUI app. It's all open-source and available on GitHub.

BusKill has been available for a long time for DIY hackers, but I specifically wanted to bring something to market that non-techie journalists could benefit from. And that's what I'm selling: it's a super-simple UX that "just works" in Linux, Windows, and MacOS.

This is not a half-assed effort: I also spent quite some time documenting the project, which can be found here.

and accept anonymous cryptocurrency like Monero.

It's been a very long journey to get to here.

BusKill has been featured in Forbes, PCMag, CoinDesk and ZDNet to name a few. How did those features come about and how have they helped the project?

I wrote a simple article on my tech blog describing how to build the BusKill cable and posted it to hacker news. It went viral.

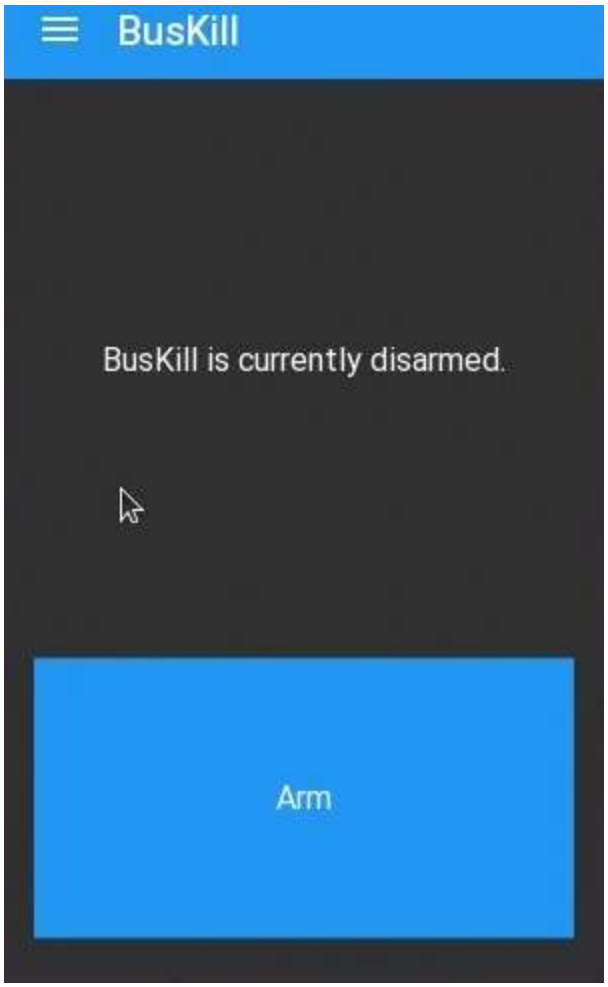
I think Catalin Cimpanu at ZDNet picked it up first, and then it spread like wildfire internationally. Even the CERT of Tunisia tweeted about it; I was pretty blown away by the interest.

After that wave I had 3 contributors approach me and help-out with various tasks. BusKill is entirely open-source, and you too can help us 😉

I see there is also a supporting app. Can you tell us about that and it's features?

Yeah, the app is where the magic lives. If the cable gets disconnected, then your screen locks. Simple.

The app UI is just a giant on/off button so you can pause (disarm) the trigger before manually locking your screen to use the restroom.


BusKill
BusKill is currently disarmed.
Arm

Currently, when armed, the app will lock your screen if the cable disconnects. This works in Linux, Windows, and MacOS. Soon we'll be adding another trigger to immediately shutdown the device when the cable disconnects.

Who would benefit most from using BusKill?

TAILS users, journalists, travelers, etc.

First, if you use TAILS, you'll immediately see the benefit of using the BusKill cable. If you've ever physically removed your TAILS disk when booted you know this will

your TAILS disk, and you have a very improved mechanical mechanism to trigger emergency shutdowns in TAILS.

That said, BusKill is designed for the threat model of a journalist operating in an oppressive regime. People have been able to build DIY BusKill cables for years, but my primary goal in selling the cables is to lower the barrier of usability. I want to make it easy to use this tech, even for folks who don't understand tech at all.

But, in fact, I actually designed it for myself. I spent years traveling around America and Asia working remotely out of coworking spaces and cafes. Every time I had to login to online banking or file my taxes, I felt super vulnerable. That's why I originally designed BusKill: to keep my funds, private keys, and tax records safe in crowded public spaces.

I've also imagined it being useful for large-sum/in-person bitcoin transactions, activists, and various businesses with sensitive data.

Is this project open source?

Yes, radically. And I wouldn't buy any security-related devices that are closed-source.

All of our code is licensed GPLv3. Everything else is CC-BY-SA.

We put our sources on GitHub. PRs are welcome 🙂 https://github.com/buskill/

I'm sold! Where and when can I purchase BusKill?

Clearnet: https://buskill.in/buy

Darknet:
http://buskillvampfih2iucxhit3qp36i2zzql3u6pmkeafvlxs3tlmot5yad.onion/buy

Will customers have the option to pay using crypto?

What would you say to anyone who is on the fence about purchasing BusKill?

Think about the data on your laptop. Think about the accounts that you log-into on your laptop. Now think of your adversaries.

If you have a legitimate concern that your adversaries may steal your laptop to gain access to your data or the accounts that you authenticate into on your laptop, then you should probably buy it. In some cases, it
can be an invaluable life-saving investment.

Is there anything else you would like to add? Where can people find you?

The best thing is to signup for the BusKill email newsletter. But you can also follow us on various platforms:

You can also follow me @MichaelAltfield on twitter and @MichaelAltfield on Mastodon.

buskill, dead man switch, michael altfield, privacy, usb kill cord

SHARE

Facebook Twitter Pinterest Linkedin

« Crypto Exchange Bitmart Hacked With Estimated Losses at Nearly $200 Million – SafeMoon, BabyDoge and BNB Included