An interview of Michael Altfield

Technology

Published on April 2, 2022, 8:05 a.m. by ksasidhar9305

The USB Buskill Cord: A whole new dimension of data privacy

Michael Altfield set another benchmark in information security with his invention which wipes/encodes the information of a PC when it's detached from it. The interview with Altfield gave more clarity about this.

In the end of december, a project called the ***'Buskill'*** pioneered by Michael Altfield and team, released a USB deadman switch conisting of a magnetic cable 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 and even self destruct with some minor tweaking.

I interviewed Michael Altfield on fourteenth of January and acquired a more profound knowledge about the journey behind the development of this gadget and furthermore got to know a great deal of new things about data privacy/protection. What makes this device a central fixture of discussion is the fact that it was specially designed keeping journalists and activists in oppressive regimes as the target audience after he observed the depressing plight of them in various oppressive regimes.

Before straightforwardly leaping to the Interview part, think about the following scenario:

You're someone whose work requires traveling frequently and you're deeply engrossed into the work which you're doing on your laptop or consider a situation where you're a journalist or a hacktivist based in an oppressive regimes, and suddenly out of the blue some unidentified men show up and they just snatch your laptop and run away. In both the aforementioned scenarios, one would face some serious loss of data, but the consequences would be much worse in the second scenario as it might mean some very serious legal consequences for the hacktivists/journalists and in some cases even execution! **Well, Buskill is the gadget one should be searching for if he/she belongs to one of the aforementioned group of professionals!**

The Interview

1: Was this invention of yours inspired by the arrest of the founder of the Silkroad in a public library? I asked this Because the scenario which you described in your blog sounds very similar to the situation in which the founder of the infamous ***drug website silk road*** was arrested.

Michael: I originally designed BusKill for myself as a traveller. I spent a lot of time working remotely out of hostels, coworking spaces, cafes, etc. I found myself feeling vulnerable when logging into financially sensitive accounts (eg online banking) in public spaces, and I wanted a way to prevent the possibility for a thief to drain my bank accounts if they snatched my laptop out of my hands when I was logged into such accounts. This is the example I provide in the article I originally punished that coined the name BusKill and that later flowered into an open-source project. After I published the above article, it got a lot of attention and users started asking me if it could be ported from Linux to other OperatingSystems. People started building their own BusKill cables, and I had one contributor write a program for Windows. To facilitate this, I createdan organization on GitHub for BusKill, and launched two websites: one showcasing the cable itself with a blog for news updates and another to document how to build and use BusKill:

* https://github.com/buskill/

* https://buskill.in/

* https://docs.buskill.in/

BusKill is currently designed primarily with the highest threat-model of Journalists operating in an oppressive regime. This is the primary example that we describe in the BusKill project's documentation. But we also think it will be useful for Activists, Travelers, Crypto Traders, Businesses, and members of the Intelligence Community.

2: Can you briefly describe the journey behind the invention of this device?

Michael: Right now it's January 2022. We're in the last couple weeks of a crowdfunding campaign to start manufacturing of the cables, which can be supported by visiting our website* https://buskill.in/buy. I built my first BusKill cable in 2017. I used it for years until, in 2020, I published a DIY guide describing how to build and use the cable in Linux using udev. That exploded.I spent a great deal of 2020 in COVID-19 lockdown writing a cross-platform GUI app for BusKill that works in Linux, Windows, and MacOS. The functional alpha release was published in October 2020.

* https://docs.buskill.in/buskill-app/en/stable/software_usr/download.html

The goal here was to make it accessible. I was no longer just writing a Linux hacker's CLI guide. My intention was to make it so that non-technical journalists working in oppressive regimes could easily &intuitively be able to use and benefit from this technology.Fortunately, in 2020 a lot of folks read my DIY guide and built BusKill cables. Unfortunately, so many did that the entire supply of USB-A magnetic breakaway adapters on Amazon went out-of-stock. I contacted the manufacturer and learned that they had EOL'd the product. At this point I had invested so much work into the project, yet I had folks asking me how they could build a cable when they couldn't buy the magnetic breakaway component (also, they were never available for sale in Europe).So I decided to fill the gap in the market. I decided to make the cables and sell them internationally. I ended-up spending much of 2021 reaching out to manufactures, researching market conditions, founding a company, and preparing for the crowdfunding campaign.As of now, we've raised almost $15,000 from folks on 5 continents who bought BusKill cables. The next big hurdle is to fulfill those orders. Then I hope to return to development so I can make the app even better. The next major feature is to permit the user to switch between having the cable trigger a lockscreen or having the cable trigger a shutdown (currently the alpha release only supports locking the screen).

3: Did you specifically keep journalists and activists in mind while designing this product?

Michael: Yeah, once I realized the demand for this technology, that became my target user group. Every decision I make, I consider the highest-risk group that, I think, needs this technology the most: journalists operating in oppressive regimes. It should never be dangerous to be a journalist, but unfortunately lots of journalists are at-risk. I cite Reporters Without Borders and the Committee to Protect Journalists here. They do great work documenting the threats that face journalists today.

* https://rsf.org/en/ranking

* https://cpj.org/data/imprisoned/2021/

4: What are your favourite ways to help non-security-aware people about the issue of data privacy?

Michael: *This depends, but I think — for a lot of people — it's good to start by teaching compassion, empathy, and consent. The first step to establish a need for privacy. People often say "I have nothing to hide." But whether or not that's true (and it's almost never true; you probably want to hide your credit card number), it's a disgustingly ignorant & privileged statement that's oblivious of the impact that your poor data hygiene has on others. The data that you have isn't just your data. In almost all cases, your data includes other people's data: names, phone numbers, addresses, conversations, etc. There's a plethora of metadata on your devices that paints a picture of your daily activities and also the activities of your contacts. If someone says they don't care about privacy, then they should consider also the privacy of the refugee from Central America who sent them an email 2 years ago with their home address. They got asylum because their life was at-risk at home. When you hand your phone to someone else, you may be handing over their life. That's an intentionally extreme example, but think about it: I mean actually take a minute and think about it. Can you write down a list of everyone whose data you have on your device? It's more than a few dozen names. Likely it's a few thousand. Do you know all of them? Do you know all of their adversaries? Do you know the risks they face? If not, then it's your moral obligation to figure that out before you hand-over your device. And you must get their consent to hand-over their data to a third party. If you don't get that consent, don't do it. Privacy matters. It's an act of solidarity and respecting others' consent.*

4: I am not a very tech savvy person, so could you please explain me how using buskill in tails can be more beneficial than using it on windows?

Michael: Microsoft is a company. Windows is an Operating System. Microsoft makes Windows. Windows is a popular Operating System, but it's full of bugs and security vulnerabilities. You probably don't want to use Windows in security-critical situations. TAILS is another Operating System. It's widely accepted as the most secure Operating System available today. TAILS stands for The Amnesic Incognito Live System. It's designed with security from the ground-up. Think journalists operating in oppressive regimes.

* https://tails.boum.org

By Incognito, TAILS means that it's designed such that all of your internet activity is censorship and tracking resistant. This is achieved by forcing all internet traffic to use the TOR network. By Amnesic, TAILS means that when you shutdown, it leaves no trace of the fact that you've run TAILS on your system. And by default, the USB drive itself doesn't record your activity. Everything is forgotten when you shutdown. By Live, TAILS means that it runs on a USB drive. Destroy the USB drive, and all the data is destroyed. Another really cool feature of TAILS is the Emergency Shutdown. If you yank out the USB drive when TAILS is running, it triggers a well-tested Emergency Shutdown sequence. BusKill improves this a bit by adding a magnetic-breakaway, hardware kill-cord that attaches your body to your computer. The magnetic breakaway can make it much easier to trigger the TAILS Emergency Shutdown if you're being physically assaulted and need to trigger it fast.

5: ***What other apps or softwares would you recommend in combination with Buskill in order to make our data more secure?***

Michael: For highest-risk individuals, you should use TAILS. We have a guide for how you can use BusKill with TAILS:

* https://buskill.in/tails/

But amnesia is hard and annoying. If you can accept a bit more risk, I recommend using QubesOS. It's what I use and what Ed Snowden uses.

* https://buskill.in/qubes-os/

BusKill does basically nothing for you if you don’t use Full Disk. Encryption. In Linux that’s LUKS. In MacOS, probably turn-on FileVault. If you must use Windows, I recommend VeraCrypt instead of BitLocker

0:00 / 0:05

A quick demo of the working of the ***'Buskill Cord'***

Share This Post On

Twitter Facebook Share Email Reddit WhatsApp Telegram

Tags: Technology Data privacy Hacking Cybersecurity

0 comments

Leave a comment

You need to login to leave a comment. Log-in

TheSocialTalks was founded in **2020** as an alternative to mainstream media which is fraught with misinformation, disinformation and propaganda. We have a strong dedication to publishing authentic news that abides by the principles and ethics of journalism. We are a not-for-profit organisation driven by a passion for truth and justice in society.

Our team of journalists and editors from all over the world work relentlessly to deliver real stories affecting our society. To keep our operations running, we depend on support in the form of donations. Kindly spare a minute to donate to support our writers and our cause. Your financial support goes a long way in running our operations and publishing real news and stories about issues affecting us. It also helps us to expand our organisation, making our news accessible to more everyone and deepening our impact on the media.

Support fearless and fair journalism today.

₹100.00

₹500.00

₹1,000.00

Related

Technology

An interview of Jack Rhysider, a cybersecurity Veteran and the host of the darknet diaries

Technology

The Erosion of Online Privacy As A Threat To Freedom

Technology

A Short History On The Rise and Crash of Cable Television

Follow us

Useful Links

Home

About

Privacy

Contact

Subscribe

Email Address