

Review: Pen Tester Sets Sights on the IronKey

After more than 10 years in the information security industry and a significant amount of time running a lab that tests products, I'm a pretty difficult guy to impress with technology. And I'm NEVER nice to vendors. They hate me. As an example, when running said test lab, we once had a vendor give a client six-figures worth of software when the client told them that we'd be testing it before they purchased. The client was happy, so we did our jobs even though we never tested a thing.

The only product I have ever had a net positive review of was the Safeboot disk encryption product, and even then, it was a case of being damned with faint praise. I believe that the entire positive part of our assessment was: "the product works as advertised."

So, when Don approached me to do a review of the IronKey Personal, I knew I was going to rip it apart. I was going to write a scathing review of how terrible their product is and why these "gimmicky" pieces of hardware don't work. Because they usually don't.

del.icio.us

Discuss in Forums {mos_smf_discuss:Murray}

As Exhibit A, I approached another vendor of a "secure" USB stick at RSA last year and inquired about who they were having do code review. "Oh, we don't actually do that," the vendor (shamelessly) admitted. "We don't expect these products to stand up to attack."

This is what I expected of the IronKey product review. I figured the technical analysis would take all of about 10 minutes — I'd toss the unlocker into Olly, figure out how to circumvent the password routine, unlock my supposedly "safe" data, and that would be that. Then I'd write my "this product sucks" diatribe, and be finished.

That I'm telling you this story should tell you that this will not be that diatribe.

I did all of that technical research. And I found the password routine and circumvented. And the key didn't unlock. In fact, it just errored out.

So, I booted it up in linux, figuring that their linux software couldn't be as mature as their Windows software. Same thing.

The protection is really baked in to the hardware. And I already knew I couldn't do anything to the hardware. In fact, the hardware is so tightly compressed in epoxy and metal that I (accidentally) put it through the washing machine twice. And the key still works.

But I was committed. I knew that there had to be something wrong. Clearly, the people behind IronKey are a bunch of shady, fly-by night shysters who don't know anything about security. So, I asked the PR person that I was working with if I could talk with the CEO. I figured I'd write this review talking about how they had a decent enough product, but no strategy or business focus to speak of.

Dave Jevans, the CEO spent nearly an hour on the phone talking threat models, business justification and strategy with me. And, when I finished the conversation, I not only believed in the quality of their team (mostly sourced with product people from Apple and various professionals from the InfoSec world), but we spent a bunch of time talking about all of the threat scenarios that they had focused on in designing the product.

This is the CEO I was talking with. Not the CTO or some product manager. This guy got it.

Beyond that, Dave made sure that I understood their strategy and how they planned to focus on both the prosumer (i.e. power user) market and the enterprise/government identity management space. He even took the time to tell me about the new features that they had developed for the product, and got me to agree to be a beta tester.

Surely, the beta product had to be crap.

By now, I'm sure you know what I found. Bulletproof product design and implementation. And some incredibly cool features, including a secure web-browser that uses Tor to protect anonymity. As well as encrypted backup and the ability to host your own portable apps in a secure (i.e. non-writable) environment.

I sound like a commercial for IronKey. This is disturbing. But I actually like the product.

I like it so much that all of my data for all of my clients is now stored on the IronKey that they sent me for the beta program. That's probably the most telling statement I can make — usually, when someone sends me a product for a review, I rip it apart and then toss it in a drawer. For me to trust it to house my clients' data is not normal. And as many of you fellow pen testers know, the data we keep could bring down their organizations. (As an aside, I'm even pondering whether or not to buy one of the 8GB ones to house the entirety of my business docs — it's that useful).

Of course, I've been dragging my feet on writing this review. Because I know that I'm going to lose some of my rep as a hard-ass. Some vendors might even think I've gone soft. But, in the process, I've gained a new tool to protect myself and my clients' information. At the end of the day, it's probably not a bad trade.