How 4 Microsoft engineers proved that the "darknet" would defeat DRM

Peter Biddle speaks at the ETech conference in 2007.

Can digital rights management technology stop the unauthorized spread of copyrighted content? Ten years ago this month, four engineers argued that it can't, forever changing how the world thinks about piracy. Their paper, «The Darknet and the Future of Content Distribution» (available as a .doc here) was presented at a security conference in Washington, DC, on November 18, 2002.

By itself, the paper's clever and provocative argument likely would have earned it a broad readership. But the really remarkable thing about the paper is who wrote it: four engineers at Microsoft whose work many expected to be at the foundation of Microsoft's future DRM schemes. The paper's lead author told Ars that the paper's pessimistic view of Hollywood's beloved copy protection schemes almost got him fired. But ten years later, its predictions have proved impressively accurate.

The paper predicted that as information technology gets more powerful, it will grow easier and easier for people to share information with each other. Over time, people will assemble themselves into what the authors called the «darknet.» The term encompasses formal peer-to-peer networks such as Napster and BitTorrent, but it also includes other modes of sharing, such as swapping files over a local area network or exchanging USB thumb drives loaded with files.

Once a popular piece of information—say, a movie, a song, or a software title—»leaks» into the darknet, stopping its spread becomes practically impossible. This, the engineers realized, had an important implication: to prevent piracy, digital rights management had to work not just against average users, but against the most tech-savvy users on the planet. It only takes a single user to find a vulnerability in a DRM scheme, strip the protection from the content, and release the unencrypted version to the darknet. Then millions of other users merely need to know how to use ordinary tools such as BitTorrent to get their own copies.

Trusted computing or treacherous computing?

Ars Technica talked to Peter Biddle, the paper's lead author, last week. The basic premise of the paper came from an e-mail Biddle circulated within Microsoft in the late 1990s. The term «darknet» was coined by co-author Bryan Willman, another Microsoft engineer. Two other Microsoft engineers, Paul England and Marcus Peinado, contributed to it.

At the time they wrote the paper, Biddle and his co-authors were working on Microsoft's «Trusted Windows» project, an effort to provide hardware-level authentication features that could make PCs

How 4 Microsoft engineers proved that the "darknet" would defeat DRM

resistant to tampering even by those who have physical access and control. The initiative would go under a variety of names, including Palladium, TCPA, and the Next-Generation Secure Computing Base.

Biddle, who now works at Intel but stressed that he was speaking only for himself in our interview, told us that it was a project fraught with political challenges. Inside Microsoft, people bristled at the implication that vanilla Windows was untrustworthy. Outside Microsoft, critics charged that Biddle's project represented the beginning of the end for the PC as an open platform. They feared that Microsoft would use the technology to exert control over which software could be executed on Windows PCs, freezing out open source operating systems and reducing users' freedom to run the software of their choice.

One widely discussed application for Biddle's technology was digital rights management. Building DRM atop an open, general-purpose computing platform is an inherently difficult problem. Every DRM scheme requires distributing encryption keys or other secrets to users' devices without the users themselves having access to them. But on an open PC, the user has the ability to inspect and modify essentially all data stored on the device, so DRM schemes are inherently insecure.

It was «very challenging for the PC industry to make the same kinds of statements around how secure data could be on the PC compared to closed devices like CE boxes,» Biddle told us. Many hoped (or feared) that a «trusted» computing platform could dramatically improve a DRM scheme's tamper-resistance by preventing a machine's owner from inspecting sensitive encryption keys or modifying DRM code. But preventing users from modifying DRM schemes also inherently meant reducing users' control over the devices they owned. The risk of Microsoft locking down everyone's PC provoked an online backlash, with critics calling the technology «treacherous computing.»

Biddle says that backlash «took us completely by surprise.» He told us that his team didn't «realize the level of entrenchment and fear» about the ways Microsoft might misuse the technology. In his view, the public overreacted to what was designed to be an application-agnostic security technology. «A lot of the things that were said about trustworthy computing being treacherous were actually impossible,» he told us.

"I almost got fired"

Biddle says that he and his team realized early on that DRM technology would never succeed in shutting down piracy. He hoped that writing a paper saying so would reassure Microsoft's critics in the technical community that Redmond wasn't planning to lock down the PC in order to satisfy Hollywood. And by making it clear that the people behind Microsoft's «trusted computing» push were not fans of DRM, Biddle hoped he could persuade the technical community to consider other, more benign applications of the technology he was building.

Biddle couldn't be *too* candid about the link between his paper and the technology he was building. Explicitly admitting that DRM schemes built on «Trusted Windows» wouldn't stop piracy might make it harder for Microsoft to persuade content providers to license its products for Microsoft's technology platforms. Biddle hoped that releasing his paper at a technical security conference would allow him to send a «dog whistle» to the technology community without raising the ire of Hollywood.

It didn't work out that way. «I almost got fired over the paper,» Biddle told Ars. «It was extremely controversial.» Biddle tried to get buy-in from senior Microsoft executives prior to releasing the paper. But he says they didn't really understand the paper's

implications—and particularly how it could strain relationships with content companies—until after it was released. Once the paper was released, Microsoft's got stuck in bureaucratic paralysis. Redmond neither repudiated Biddle's paper nor allowed him to publicly defend it.

At the same time, «the community we thought would draw a connection never drew the connection,» Biddle said, referring to anti-DRM activists. «Microsoft was taking so much heat around security and trustworthy computing, that I was not allowed to go out and talk about any of this stuff publicly. I couldn't explain 'guys, we're totally on your side. What we want is a program that's open.'»

A losing battle

While Biddle and his colleagues didn't succeed in allaying the fears of Palladium's critics, the paper's central arguments have held up well. The authors predicted that the emergence of the darknet would produce a technological and legal arms race. They thought content companies and law enforcement would attack those aspects of the darknet that were most centralized, but that the darknet would adapt through greater decentralization. And they predicted that efforts to build secure DRM schemes would continue to fail. All of their predictions have continued to hold true over the last decade.

Both content companies and the US government have pursued increasingly aggressive anti-piracy strategies. The Recording Industry Association of America sued thousands of alleged file-sharers during the last decade, and content companies have sued numerous file-sharing startups out of existence. In 2010, the federal government got into the act, using the powers of the recently passed PRO-IP Act to seize domains and other assets of alleged pirate sites. And they have even begun to arrest key figures in file-sharing networks.

Yet these increased enforcement efforts have barely slowed down the darknet's momentum. A key development has been the emergence of «locker sites» that host infringing files and «link sites» that provide pointers to those files.

«The thing about the locker and link sites is that they can be very lightweight,» Biddle told us. They are «not that hard to replicate because they are basically a database.» That makes the network as a whole much more robust to law enforcement efforts to shut it down: close down one site and two more pop up in its place.

And while BitTorrent and Megaupload get all the attention, Biddle notes that there are other file-sharing techniques that the government is never going to stop. «Teenagers and twenty-somethings I know routinely will go over to a friend's house with a terabyte drive to swap stuff,» he said. They choose the «sneakernet» approach less out of fear of liability than because it's so convenient. «You can have a ton of content on a terabyte drive,» he noted.

Yet the content industry continues to try, and fail, to produce secure DRM schemes. Biddle believes this strategy has proved counterproductive because it inconveniences legitimate customers without stopping piracy.

«I'm now finding that for some kinds of content, the illegal is clearly outperforming legal,» Biddle said. «That blows me away. I pay for premium cable. It's easier to use BitTorrent to watch *Game of Thrones*. HBO Go is trying very hard to do a good job,» he said, but the user experience just isn't as good. Because HBO Go is a streaming service, he said, it's more vulnerable to network congestion than simply downloading the entire episode from the darknet.