WIKIPEDIA - LAURAPOITRAS

SNOWDEN'S SECURITY SECRETS

YOU ALREADY KNOW THAT YOU'VE CROSSED A LINE AND IT'S IMPOSSIBLE TO GO BACK.

BY **DR. BRANDEN R. WILLIAMS**

You have information, in the form of digital evidence that you need to get into the hands of someone else. It could be a loved one, a government contact or someone from the press. Simply possessing this information means that bad things can happen to you. Even though people will be hunting for the person who created and transported this digital copy, getting it safely to your confidant is worth the risk of being in harm's way.

Stories like this play out in thriller novels and movies every year, as well as in the real world. The continuum ranges from the most innocent versions (I'm trying to surprise someone with a gift) to the most criminal (I'm stealing digital copies of secrets). Moving this information from one place to the next uses the same tactics and techniques that have been used for millennia, even in a digital form. There is still some kind of physical medium required to transport it.

Two prominent examples in recent history include the leaks provided by Chelsea

(Bradley) Manning and Edward Snowden. In both cases, an individual made digital copies of a large number of files and smuggled them through some kind of security checkpoint to leak them to someone else. While these stories started from a relatively similar spot, they had dramatically different outcomes. Manning spent nearly seven years in various prisons, while Snowden is trapped in Russia after being granted asylum.

In both cases, there were multiple opportunities to catch the data as it was copied or being transported out of the facility. In the case of Manning, digital storage devices brought in and out of a secure facility in any form (specifically, a CD labeled "Lady Gaga") should never be allowed. I've personally witnessed much better security at data centers and payment card production facilities that would have stopped something like this from happening. Complacency had evidently set in within the security structure at his location.

For Snowden, all we have is the dramatization in the Oliver Stone biopic. Snowden himself came up with the idea, but never went public with exactly how he smuggled a flash drive through metal detectors and X-Ray scanners similar to what you find at an airport. All indicators point to physical theft as the networks in question were air-gapped from the Internet—meaning, that they operated on their own network with no physical connection to the public Internet. The only way to take that information is physically, and flash drives are fairly easy to conceal.

But if you had a cache of digital documents that you needed to transport, how would you move them in a way that protects the data, yourself and your interests?

FUNCTIONALITY VS. SECURITY

Defeating both physical and digital countermeasures to information theft remain high on the list of hackers and espionage organizations globally. Every year, thousands of hackers descend on the Las Vegas Strip to showcase their new methods and techniques, often times to great fanfare. "Hacker Summer Camp" as it is known in the community is a combination of three security events: B-Sides Las Vegas, Blackhat and DEFCON. Attendees learn about practical and theoretical ways around security systems—including shattering common knowledge security controls.

Firms spend millions of dollars to keep digital secrets protected and as a security practitioner, I can tell you it is incredibly complex. Security professionals joke that we play on this continuum of total security on one end and total functionality on the other. If systems are totally secure, they are not usable (think a computer encased in feet of concrete buried deep in the earth's crust). If they are completely and freely usable with tons of functionality and no controls, they are not secure. This is where risk management comes into play. We need to define the functionality requirements and design security controls that enable them while keeping the system and data secure.

IF YOU HAD A CACHE OF DIGITAL DOCUMENTS THAT YOU NEEDED TO TRANSPORT, HOW WOULD YOU MOVE THEM IN A WAY THAT PROTECTS THE DATA, YOURSELF AND YOUR INTERESTS?

Here's a simple example. Banks want to provide better service to their customers, so they allow for more self-service actions. It started with the ATM, first deployed in 1969. Today it takes the form of feature-rich mobile and web applications. For many of us, visiting a bank branch and talking to a teller is just not in our daily planner.

For fans of Western action-adventure game Red Dead Redemption II, think about how banks worked in the Old West. Physical cash, precious metals, gems and bonds were all secured in vaults (either built into the banks or into the Old West equivalent to an armored car). If you wanted to get access to this, you had to go into the bank to get it. Today, you can perform nearly all the services your bank offers through a mobile or web application that uses public networks to enable. Banks can only ensure the security of their systems and networks, they can't (directly) secure the Internet or the device accessing those networks.

Where security used to be done 100 percent on the bank's terms, it's now a shared responsibility between banks and their customers, all leveraging public systems they don't control.

PHYSICAL TRANSMISSION

Digital content can be stored or transmitted in a number of ways, all of which have varying levels of effectiveness, speed and stealth. Physical media can often times be one of the most effective ways to transmit information because the carrier controls his copy. If it's the only copy, then the carrier can either ensure it makes it to its destination or ensure its destruction if that is necessary.

Physical transportation also carries risk. You could lose the information or have it taken from you. The physical media could be accidentally destroyed by being crushed, dropped or even submerged in liquid. If it is encrypted, you could be compelled to reveal how to access the information by basic inquiry or aggressive interrogation. If you can somehow prove it is the only copy, however, that does give you options with both leverage and personal safety. For this reason, Snowden likely did not move his stolen documents to a cloud service before meeting reporters in Hong Kong.

Finally, perhaps one of the more interesting reasons why physical transport is desirable is that it can be moved from person to person or location to location without leaving a trace. The only way security professionals can reliably detect the data movement is by catching it when it is transferred from the source system (and clearly both companies and governments struggle with doing this). Once it is on the transport media, it is up to physical controls to detect it moving (there are exceptions; for example, if the media is designed to phone home). To put the problem into perspective, imagine operating a firm with thousands of contractors and trying to track a single USB drive. At best, you could capture it (if you know to look for it and conduct sufficiently invasive searches 100 percent of the time) at main egress points. In reality, once it slips past your facility, it is untraceable.

Cloud-Based storage systems such as Dropbox or Amazon S3 allow anyone to store and share files as long as they have an internet

connection and access to a basic browser—which describes virtually every network-enabled device on the market. More discrete file sharing options such as anonymous file drops or Tor services allow for safer file transfers without records, but have various limitations that may affect your decision to use them.

Leveraging something like Dropbox or an Amazon S3 bucket is easy and user friendly, but Dropbox and Amazon will have records of the file transfer (the evidentiary value of which remains to be tested) that can link you to the upload. It will also do the same for anyone downloading the content. In both cases, certain steps can be taken to hide or mask your identity, but these services do not have the features required to really be anonymous. Just knowing the address to the file could mean that anyone can download it multiple times—definitely not ideal if you are trying to get information to one individual only.

This is where specially designed services such as Onionshare and anonymous file drops come into play. With something like Onionshare, only the person knowing the address (and potentially a secret if you use the stealth mode) will be able to download the file. The true source and destination addresses are hidden by being routed through the Tor network such that people capturing internet traffic near your computer will only know that you are connected to a Tor node. One drawback with Onionshare is that you must be online for the recipient to receive the file.

For a dead drop option, choose one of many anonymous file sharing services. I've used file.io in the past with decent results, but there are many alternatives. These services work by uploading a file to their servers and giving someone the URL to access it. The file is deleted upon download (or within a time limit you set irrespective of download) to ensure only one person receives it from the service. There is nothing for you to maintain or keep connected to the internet, but anyone with the URL will be able to download that file. Do not depend on any file protections provided by the service. It is foolish not to use your own encryption on top.

There could be some perfectly valid reasons for choosing digital vs physical transport. For example, if you were physically unable or prohibited from traveling to meet this person or doing so puts you in danger. If you do select digitally transporting the information, consider taking some of the following additional countermeasures to improve the probability of success. Always encrypt your files using strong encryption methods. Consider splitting the file into multiple parts, or hiding it using steganography (hiding the secret file inside another file like an image). You could even hide decoys among the split file segments to further complicate reassembly. Finally, consider using a combination of physical and digital methods to communicate with your receiver (place key elements for retrieval or decoding in a physical dead drop for someone to get).

Make it as complex as you like, but don't forget that these methods must be communicated to the receiving party. Otherwise, they will not be able to reassemble and use the files.

PHYSICALLY POSSESSING AND MOVING FILES HAS THE ADVANTAGE OF CONTROLLING THE INFORMATION AT ALL TIMES, BUT IT WILL ALSO BE SUBJECT TO LOSS, DAMAGE OR THEFT.

Discreetly sending sensitive information to a third party without detection is absolutely possible, and still a very real threat to defenders globally. The attention from high-profile cases in recent years encouraged leaders to counter the threat of data leaks through more digital walls and detection methods. Sending data undetected used to be extremely easy to do, and now to be successful you need finesse and tradecraft.

The original cyber kill chain (modification of the F2T2EA kill chain concept for cyber warfare) as documented by Lockheed-Martin listed its last link as exfiltration—or the act of moving data outside of its controlled environment. It's the last opportunity for defenders to prevent a data breach, so there is serious attention and investment in trying to detect unauthorized traffic from leaving a network.

Attackers take a huge risk of being discovered when they transfer data from a watched network to somewhere on the Internet. Common exfiltration methods are monitored, and most sophisticated security programs will block things like file sharing services and Tor. Those countermeasures are not foolproof, but often times without an insider's help, you may reveal yourself and your intentions by testing what is allowed through. Detecting exfiltration is difficult if the attackers are skilled and patient; but remember, any exchange leaves a trace. The evidence of exfiltration is ever-present; it is up to the defender to capture it.

No matter your situation or need, there are a number of ways to safely get digital information from one place to another. Physically possessing it and moving it has the advantage of controlling the information at all times, but it also means that it is subject to loss, damage or theft. Always encrypt data you carry with you so those threats are minimized. Placing it somewhere digitally frees you from the responsibility of maintaining its security, but it could be leaked to someone other than your intended contact. Ultimately, each situation comes with its own risk/reward equation.

ADDITIONAL RESOURCES

Do you want to leverage the same anonymous OS that Edward Snowden uses? Check out Tails: https://tails.boum.org/.

There are plenty of anonymous file sharing options, but check out Onionshare (https://onionshare.org/) and www.file.io for some examples.

Don't forget that you need to encrypt your files. You can use something like GnuPG (https://www.gnupg.org/) or VeraCrypt (https://www.veracrypt.fr/). ✓

BIO

*Branden R. Williams (**www.brandenwilliams.com**), DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow and technology executive sought after by global companies to consult on their digital business initiatives. His latest book on PCI DSS v3.2 Compliance is available via Amazon.*