ConversationalGeek®

Conversational
Supply Chain Security

Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)

Learn about:

- Why supply chain attacks are so successful
- How cryptographic key management can help prevent attacks

Sponsored by Unbound Security

Unbound Security is the global leader in cryptography and empowers enterprise customers worldwide to confidently secure, manage, and authenticate all critical business transactions, information, identity, and digital assets – anywhere, anytime. Unbound Security CORE is the enterprise platform of choice for secure key management, trusted by many of the world's largest banks and Fortune 500 companies. Unbound Security is a recent recipient of the Deloitte Fast 500 award and is headquartered in New York, with research and development facilities in Tel Aviv.

For more information visit
www.unboundsecurity.com

Conversational Supply Chain Security (Mini Edition)

by Brien Posey

ConversationalGeek®

Conversational Supply Chain Security (Mini Edition)

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at www.ConversationalGeek.com.

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Brien Posey
Project and Copy Editor:	Pete Roythorne
Content Reviewer(s):	Marcella Arthur
	Lucy Temprano
	Yehuda Lindell

Note from the Author

Hi, I'm Brien. For those of you who don't know me (or know my work), I am a long-time Conversational Geek author, and 19-time Microsoft MVP.

In this book, I wanted to write about supply chain attacks. Supply chain attacks come in different forms, but they generally refer to breaches that occur as a result of a vulnerability in a vendor's software. One of the best things that an organization can do to fend off these attacks is to put a solid key management plan in place to guard against stolen or misused encryption keys. I will be talking all about that in this book.

Brien M. Posey

The “Conversational” Method

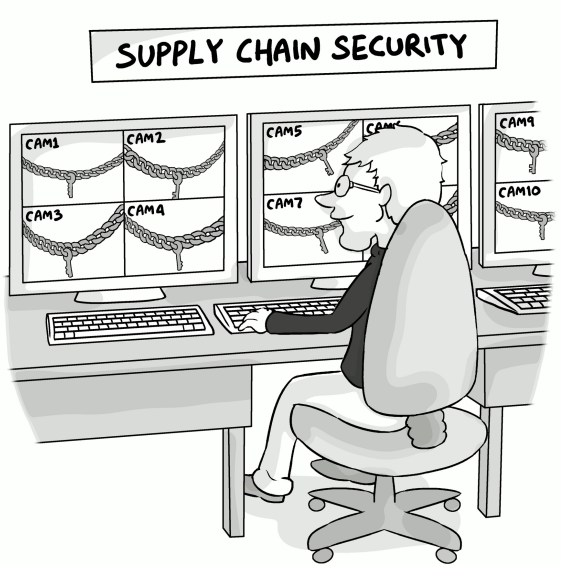
We have two objectives when we create a “Conversational” book. First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

The Cryptographic Fallout from Supply Chain Attacks



Before I get too far into this book, I want to start by giving you a really simple explanation of what a supply chain attack is, and why supply chain attacks can potentially be so devastating.

Every business, no matter how large or small, relies on software that has been created by another company. Your desktop computer for example, probably runs an operating system that was created by Microsoft or Apple. Similarly, you might use an online service such as Microsoft 365 to handle your email and cloud storage.

The point is that it is nearly impossible for an organization to create all of its own software. Even a software company will likely use tools, utilities, or online services that were created by another company.

When an organization licenses software that was created by another company or subscribes to another company's online services, there is an expectation of security. The organization trusts the software provider to take all reasonable steps to keep their software secure so that the organization will not suffer a security breach as a result of using that software.

This is the very essence of a supply chain attack. In a supply chain attack, a hacker uncovers a vulnerability in a particular piece of commercially

available software. The hacker knows that this vulnerability will impact anyone who is using the software, and therefore begins attacking the software company's customers. An organization that suffers from such an attack might not have done anything wrong itself, but was left exposed as a direct result of a vulnerability that existed in software that was created by someone else. In other words, the attack stemmed directly from a vendor's security failure, hence it is extremely important to use vendors that take the proper security precautions, and implement technologies that will compliment your current infrastructure, as well as mitigate risks to your most critical data and assets.

From a vendor standpoint, it is incredibly important to make sure that you do not become the source of a supply chain attack. After all, such an attack can do irreparable harm to your brand's reputation, and possibly also open you up to legal action.

The number one thing that you must do in order to avoid being the source of a supply chain attack is to protect your code signing keys. While that alone will not stop vulnerabilities within your software from being exploited, it will prevent attackers from being

able to create malicious code that they sign with your key and then pass off as having been created by you.

Of course, the flip side to this is that organizations that use software that has been created by someone else must also ensure that they do not become victims of supply chain attacks. The remainder of this book focuses on supply chain attacks from the perspective of an organization that seeks to do whatever it can to mitigate the ever-present threat of a supply chain attack.

What Happens When a Software Vendor is Hacked?

Although I want to focus my attention on helping businesses to avoid supply chain attacks, I want to first discuss what happens when an attacker targets a software vendor. After all, it's tough to defend yourself against a supply chain attack unless you first understand how a supply chain attack works.

A supply chain attack against a software vendor starts out much like any other hack. An attacker will begin by gaining entry into a network and will then make a series of lateral moves in an effort to gain elevated privileges.

The thing that makes a supply chain attack different from other attacks is that compromising resources on the victim's network is not the ultimate goal. Instead, the attacker's main goal is to steal the company's signing key. This is the certificate that the software vendor uses to digitally sign the software that it publishes. The signing key ties the software vendor's identity to the software, thus proving that the software was created by that particular vendor.

Let me give you a real-world example of why this matters.

In the early days of Windows, Microsoft didn't digitally sign the files that it included with its Windows operating system. As Windows began to gain mainstream popularity, hackers quickly realized that they could replace files associated with the print spooler with malicious files of the same name. This not only helped the malicious files to blend in

and evade detection, it also allowed them to run with privileged access. Eventually Microsoft realized what was going on and began digitally signing operating system files so that hackers could no longer delete an operating system file and replace it with a similarly named file of their own choosing.

This is why signing keys are so important. Signing keys allow an organization to positively prove (through a digital signature) that anything signed with the signing key truly did originate with them and is not a counterfeit.

So, with all of that in mind, just imagine what would happen if an attacker managed to gain access to a publisher's signing keys. At that point, they could use the keys to sign their own code, making it appear as though the code originated from the publisher whose keys they stole. The publisher's customers have no reason to believe that signed files are illegitimate and therefore deem them to be trustworthy. This inevitably leads to the customer suffering a breach, much like what happened following the now infamous SolarWinds hack.

Why Supply Chain Attacks are Successful

If an organization is to prevent supply chain attacks, it must understand the reason why supply chain attacks are so often successful.

A successful supply chain attack ultimately comes down to a matter of trust. The victim of the attack trusts the software that they are using and the publisher who produced that software. As such, the organization has little reason to question the code that is deployed. This is especially true if the code is digitally signed and has passed all of the usual security checks, such as anti-malware scans. Of course, the case could also be made that attacks are successful because of vulnerabilities that exist with regard to the way that encryption is currently performed and with the way that enterprise-class organizations structure their security.

Vulnerabilities with Current Encryption Methods

Vulnerabilities dealing with encryption methods often come down to adherence to key management best practices. Assuming that an organization is

security conscious, it probably takes at least some measures to keep its keys from falling into the wrong hands. Even so, there is a lot more to key management than just keeping hackers away from your keys.

Ideally, an organization should have some sort of process in place for monitoring key access and key usage. Suppose for instance that someone uses a key to sign a piece of code. Was that signing function a part of a workflow? Was it an expected operation? Was the user who signed the code authorized to do so?

These questions can be difficult, if not impossible, to answer if an organization has not adopted an effective key management strategy. Additionally, there needs to be an immutable logging mechanism put into place so that the organization has an irrefutable record of every time that a given key has been used, by whom and to perform what cryptographic operation.

Vulnerabilities with Enterprise Security Layers

One of the best known and most widely used IT security strategies is to practice defense-in-depth. The idea behind defense-in-depth is to take a multilayer approach to security so that if one security mechanism fails, there is another mechanism available to thwart an attack.

While the defense-in-depth approach to security has its merits, it is sometimes used as a Band-Aid. In other words, some organizations simply purchase a bunch of security products, install them all, and refer to it as defense-in-depth. There are two problems with using this approach.

The first problem is that it can lead to overlapping protection in some areas and security gaps in others. In some instances, security products can actually interfere with one another.

The second problem is that the approach is not based on any sort of strategic initiative. In order for defense-in-depth to be effective, an organization must establish a comprehensive security strategy

and then work to integrate a defense-in-depth solution in a way that aligns closely with that strategy.

One of the most important things that must be understood with regard to defense-in-depth and supply chain attacks is that many organizations have gone well beyond practicing simple defense-in-depth and have moved to a zero trust model. Zero trust is based around the idea that nothing is trusted by default and that everything needs to be proven. Most zero trust architectures for example, require both internal and external network traffic to be encrypted, because the organization's own internal network cannot be assumed to be trustworthy

Although there are undeniable security benefits associated with zero trust, there is at least one downside to adopting a zero trust architecture. A zero trust architecture can lead to a false sense of security. Imagine for a moment that a software vendor that your organization uses has suffered a breach and that their cryptographic keys have been compromised. Just to make things interesting, let's also assume that the attacker somehow manages to deliver malicious code that has been signed with the

attacker's keys, making that code look like a legitimate software update.

In such a situation, a zero trust architecture would not necessarily stop the organization from deploying the counterfeit update. After all, the update appears to be authentic based on its digital signature.

Keep in mind, however, that zero trust architectures are tightly intertwined with the concept of defense-in-depth. As such, the organization's other defenses should ideally be able to keep the counterfeit code from doing significant harm. Even so, this example serves to illustrate just how damaging a supply chain attack can be if the proper defenses are not in place.

Crypto Strategies for the Digital Business

So what can a digital business do to help ensure the safety of its cryptographic keys? As discussed in the previous section, the first step is to develop an enterprise cryptographic strategy. Specifically, this means having documented policies, procedures, and safety mechanisms in place to guard things like transactions, assets, identities, infrastructure components, clouds, users, and related applications.

As you create these policies and procedures it is important to enable encryption across your entire digital value chain. This includes all of your critical business applications and any other related assets.

It's also extremely important to put mechanisms in place to prevent keys from being misused. Keep in mind that preventing key misuse is different from preventing key theft. Both are important, but there is a difference between the two. Key theft implies that someone manages to steal a copy of your key.

Key misuse, on the other hand, happens when someone infiltrates your organization and uses your key to sign or decrypt something without your knowledge or consent. As previously discussed, one way of preventing key misuse is to integrate the cryptographic process into a workflow. The idea here is to make it so that it is impossible for just any cryptographic operation like signing or decryption to be carried out arbitrarily. Every such operation should be logged, and should correspond to a business workflow that can easily be traced back to a legitimate business activity.

Another goal within your key management strategy should be to eliminate any potential single points of failure. The concept of removing single points of failure is often thought of in terms of system resiliency. For example, organizations host workloads on failover clusters in order to prevent an individual server from becoming a single point of failure. However, resiliency is not the only time that the concept of having a single point of failure comes into play. You can also have a single point of failure in a security strategy. This would be one barrier that if breached, would give an attacker access to the assets that they seek.

One potential single point of failure with regard to key management is storing all of the keys in one place. Ideally, no key should reside on any single machine at any point, not even when it is being used. This can go a long way toward preventing an organization's keys from being misused or stolen.

Consider for example, what happened in the SolarWinds breach. SolarWinds customers who installed the malicious code (which appeared to have come from SolarWinds) gave the attackers the ability to steal their Active Directory Federation

Services (AD FS) token-signing certificate. This made it possible for the attacker to log into a federated resource (such as Microsoft 365) using any of the organization's user accounts, without a password.

Another best practice is to understand what a Hardware Security Module (HSM) is and is not designed to do. An HSM is a hardware-based solution that performs cryptographic operations like signing, decryption, and encryption.

HSMs are one of the most widely used options available for preventing key theft. Even so, it is critically important to understand that while an HSM might be able to stop your keys from being stolen, these devices are not designed to prevent keys from being misused.

There is nothing wrong with using an HSM, but it is important to know their limitations.

Another best practice is to have a way of monitoring (or even auditing) the key management process. While most, if not all systems do provide auditing capabilities, the audit logs can vary widely in scope each having its own logging format that somehow needs to be normalized in order to report and alert on suspicious behavior. To be effective, your key management process needs to be transparent.

Another thing to consider with regard to visibility is the importance of having a single pane of glass by which you can manage your keys across a hybrid/multi-cloud environment. Imagine for a moment that an organization uses one key management solution on premises and another in the cloud. In a situation like that, the organization would have to manage both key management platforms separately.

It's usually going to be better from a manageability standpoint to bring those and any other key management solutions together under a single management tool. This makes it a lot easier to gain a comprehensive picture of how an organization's key management assets are being used.

Finally, as you are establishing your key management strategy it's really important to engage a trusted cryptography expert. Effective key management is rarely easy, and the difficulties are compounded when key management must be performed at enterprise scale. Engaging with a trusted key management expert can help you to avoid making mistakes that could end up compromising your organization's security later on.

The Big Takeaways

Supply chain attacks can be absolutely devastating for an organization. One of the best things that any organization can do to avoid falling victim to such an attack is to adopt solid enterprise cryptography management practices in order to help ensure that its keys are not stolen or misused.

Defend your enterprise from supply chain attacks

Unbound Security's CORE Code Signing ensures that all code is scanned using malware-detection tools, before being signed.

unbound security

unboundsecurity.com

Supply chain attacks can have a devastating impact on an organization. In this book I'll discuss the best things that organizations can do to avoid falling victim to supply chain attack and why ensuring your business is adopting good cryptography management best practices is crucial.

About Brien Posey

Brien Posey is a 19-time Microsoft MVP, a published author and conference speaker with 20+ years of IT experience, and a Commercial Scientist Astronaut candidate.