BEYOND SOLARWINDS: PRINCIPLES FOR SECURING SOFTWARE SUPPLY CHAINS

by Christopher Nissen, Charles Clancy, Rick Ledgett, Chris Sledjeski

Executive Summary

Supply chain exploitations like the SolarWinds compromise should not be a surprise. Since 2015, there have been numerous supply chain attacks.[1] Billions of dollars are spent annually to protect against cybersecurity and software security incidents, yet the number and consequences of these types of incidents continue to increase. The recent SolarWinds[2] exploitation is likely the most damaging *known* software-enabled supply chain cyberattack to date.

Plugging individual vulnerabilities as they are identified is not a winning strategy against sophisticated nation-state actors. Although a variety of technical, policy, and regulatory actions are needed to begin to address obvious deficiencies, it is important to understand the larger causes of the susceptibilities that allow adversaries to so easily execute these types of asymmetric attacks at scale. To realize a true strategic roadmap, a new principles-based approach is needed that can be leveraged across short-, medium-, and long-term strategies.

This paper introduces a set of such principles and associated recommendations. Some of the key principles include the need to *reduce fragility* in our architecture designs through increased diversity; the need to *assume permeability* and layer security; and an acknowledgment of *where current practices produce a fallacy of trust in platforms and services*. Together these principles address critical shortcomings in existing approaches and provide a realistic foundation on which to gauge potential policy and strategy decisions.

PLUGGING INDIVIDUAL VULNERABILITIES AS THEY ARE IDENTIFIED IS NOT A WINNING STRATEGY AGAINST SOPHISTICATED NATION-STATE ACTORS.

These principles and recommendations also align with the Cyberspace Solarium Commission's call to deny the adversary undue benefits through increased resilience, more nimble information sharing structures, and the reduction of systemic vulnerabilities.

Lastly, we must seriously consider extending existing and future security frameworks and considerations to commercial-off-the-shelf providers, who are simply in too many critical applications to be mostly discounted across multiple cybersecurity frameworks.

Introduction

Software is the lifeblood of the digital age. It has enabled unprecedented creation and growth of previously unheard-of industries, and it feeds unlimited innovation with ever decreasing product development and evolution timelines.

In the corporate software sector alone, there are more than 20 million software developers; nearly all of them rely heavily on open source libraries—and nearly 90% of a typical software application is built on open source code.[3] The resulting assembled software products are continuously updated, with new versions pushed to users. Underpinning all this development is the need for speed—in development, modifications, and vulnerability patching.

The drive behind this entire ecosystem can be characterized by Adam Smith's "invisible hand" concept, wherein if each consumer can choose freely what to buy and each producer is allowed to choose freely what to sell and how to produce it, the market will settle on a product distribution and prices that are beneficial to the community as a whole.[4] In other words, the software development ecosystem is based on the common good and driven by value, efficiency, and ease of use.

WE LIVE IN AN ASYMMETRIC ERA IN WHICH DOMINANCE IS WON THROUGH NON-KINETIC EXPLOITATION OF OPEN SOCIETIES.

Yet we find ourselves in a global society in which some nation-states compete in ways antithetical to the common good, and in fact lay out as their objectives technological, economic, and even social dominance. We live in an asymmetric era in which dominance is won through non-kinetic exploitation of open societies. Our software supply chains are already in an invisible battle with malicious actors who seek to exploit the invisible hand concept to deliver observable impacts to our economy, society, and national security.

A Better Approach

By now it is apparent that a software-fueled innovation ecosystem that is based on trust, massive interconnectivity, increased interdependencies, and software reuse at scale exposes tremendous systemic vulnerabilities—vulnerabilities that facilitate major disruptive events.

Modern system interdependencies improve our ability to sustain random disruptions from events like hurricanes. However, in cyber compromises, this connectivity may increase the likelihood and potential scale of cascading failures (or systemic collapse)[5] in areas such as communications, energy transmission, and financial services.

The principles and recommendations described here can be applied to an enterprise, as well as to specific subsystems such as software development or update functions. Although a variety of technical, policy, and regulatory actions are needed to begin to address obvious deficiencies, it is important to understand the larger causes of the susceptibilities that allow adversaries to so easily execute these types of asymmetric attacks at scale, so that we can realize a true strategic roadmap.

This approach aligns with the Cyberspace Solarium Commission's call for layered cyber deterrence, promotion of national resilience, and reform of U.S. government (USG) structure and organization for cyberspace.[6] A key part of this deterrence is to deny the adversary undue benefits through increased resilience, more nimble information sharing structures, and reduced systemic vulnerabilities.

We can do this by building more diversity into system architectures, consolidating and enhancing our supply chain intelligence, and protecting the digital supply chain. These steps will add to our national resilience by increasing our capacity to withstand and quickly recover from attacks that could be leveraged to cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior.

Efficiency Increases Fragility

Modern system designs have resulted in increasing amounts of fragility in exchange for cost savings and speed. Perhaps even more concerning, some of these design changes have been initiated for *perceived* security. Resilience has been sacrificed, paving the adversary's path toward exploitations with massive economies of scale. Such fragile system designs tend to be some of the highest value adversary targets because of their self-evident return on investment.

The SolarWinds compromise is an excellent example. This attack confirmed well-known serious and systemic weaknesses in our approach to securing the software supply chains our nation depends on.

Network management software is one of many centralized software services that are prime targets of adversaries as they seek to exploit system fragility and realize tremendous asymmetric advantage. The concentration of a relatively small number of software suppliers that service many organizations, and the lack of effective material standards for securing the software supply chain, mean that high-end adversaries can effectively target a relatively small number of weak points to achieve outsized effects against many targets.[7]

The asymmetric approach our adversaries have chosen must be the lens from which an effective defense is developed and implemented.[8] From this perspective, it is possible to see the benefit from decisions that generate a higher degree of resiliency via solutions that frustrate and limit adversary actions. Resilience is essential as adversaries continuously adapt to protective measures; no one defensive approach will be sufficient to eliminate the realization of a threat now or into the future.

Diversity Decreases Fragility

To build an effective response foundation, we must recognize that diversity decreases fragility, while commonality increases it. Platforms like SolarWinds Orion consolidate network, infrastructure, and application performance management into a single platform, which also includes enterprise service management, information technology (IT) security, and database performance management.[9] On its own, this consolidation of an enterprise's core IT functions makes the platform a high-value adversary target.

The selling point of such a platform is integration and simplicity of use—however, the user takes on an unknown and non-zero degree of enterprise risk merely by accepting the consolidation of these core functions into a single commercial product. These risks come from inherent vulnerabilities in the vendor's product, product updates, and in how that product is configured and maintained on the user's premises. The opposite approach would execute these functions in a diverse manner, engineered in a way that could detect anomalous data exchange between the functions while distributing risk across several vendors.

Assume Permeability, Layer Security

Modern supply chains are incredibly complex and interconnected, and adversaries have multiple attack vectors available to them to realize their desired effects. If one vector is made significantly more secure than another, the exploitation will be realized via a more vulnerable approach. This is the reality of advanced persistent threats.

The objective of zero infiltration is unrealistic for a high-value target. Rather, world-class security designs assume permeability and are designed to contain damage (and hence risk) through infrastructure segregation and compartmentalization. However, these measures are insufficient unless combined with a robust threat-detection and hunting function, based on anomaly detection at the boundaries and within compartments, that is executed continuously.

> WE MUST RECOGNIZE THAT *DIVERSITY DECREASES FRAGILITY*, WHILE *COMMONALITY INCREASES IT.*

Layered security can serve as a buttress against exploitations that use different attack vectors within the supply chain. For example, the SolarWinds attack was executed under the guise of a legitimate update, with malicious code inserted into the original update with compromised log-in credentials. In other words, the malicious actor hijacked a trusted user's credentials and used their credibility for cover. The same effect could also have been realized by an insider either wittingly or unwittingly inserting the same code.

The actors behind the SolarWinds compromise also exploited trust in victim computer systems by accessing global system administrator accounts and/or trusted Security Assertion Markup Language token-signing certificates; they then forged those tokens, which allowed them to impersonate highly privileged accounts to bypass multi-factor authentication for critical applications such as the Microsoft Office 365 suite.[10] Layered security is and will continue to be necessary to effectively close the gaps between individual security initiatives and to provide an opportunity to observe and contain malicious activity across an enterprise. Abuse of trust relationships will continue to drive successful adversary operations in the asymmetric era.

Beware of the Fallacy of "Trust"

The opposite of assuming permeability is the concept of trust. Most public declarations of trusted systems or components, on their own, are an invitation to adversary attacks. More concerning, these labels may give users a false sense of security.

Specifically, "trust" signals to an adversary the availability of cover under which they can more easily hide and maneuver. This is because, in most cases, the processes used to declare something as trusted or certified are not (and likely never will be) comprehensive enough across the major attack vectors, nor applied frequently enough in enough places. In most enterprises, there are significant gaps in the continuous monitoring needed to rapidly detect a compromise. In addition, well-hidden exploits may lie dormant for long periods of time and survive the trust certification process, or be inserted after the trust label has been applied.

Once a system is in use and declared trusted, the end user's guard is typically down and the exploit can be activated. By declaring something trusted, all the responsibility for trust lies with the few individuals involved in the process. Even worse, such certifications of trust often discourage third parties in the supply chain to verify that trust.

The means by which FireEye discovered the SolarWinds exploitation is an illustration of the value of not trusting one's enterprise and investigating subtle anomalous actions. It also points to the potential power of expanded continuous monitoring in IT and operational technology (OT) environments.

Related to trust, we must seriously consider extending existing and future security frameworks and considerations to commercial-off-the-shelf (COTS) providers, who are simply in too many critical applications to be mostly discounted across multiple cybersecurity frameworks. For example, the DoD Cybersecurity Maturity Model Certification includes "every supplier/vendor with the exception of those providing solely COTS."[11]

In the case of SolarWinds, COTS exclusions may have inadvertently contributed to untold damage to Defense Industrial Base (DIB) and other critical federal government systems. COTS exclusions exist in other major security frameworks too, such as the Defense and Federal Acquisition Regulations, and the Federal Information Security Modernization Act, which furthermore does not consider software vendors.[12, 13, 14] We must cautiously label trust in our products and security approaches to avoid certifying and scaling a false sense of security.

Recommendations

An immediate focus on defensive mechanisms is essential and understandable. However, the principles above strongly argue for more fundamental changes in our approach, especially since the risk of attacks through the software supply chain remains significant and potentially severe. Below we suggest six specific recommendations, each of which falls into one or more of the following classes of defense: situational awareness; defensive protective measures; and engineering and technical emphasis.

1. **Create a National Common Operating Picture of Cyber Domain Adversary Actions**

   Despite open source reports of massive cyber-IT and software supply chain breaches over the past several years, the U.S. still does not have a coherent, integrated common operating picture (COP) of adversary movement against private and public sector companies within the U.S. We are in a non-kinetic, asymmetric conflict, yet we lack robust technical event collection, rapid and effective information sharing both inter- and intra-government, and sufficient legal authorities to proactively defend the private sector at large.

   As an example, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 directs the Secretary of Defense to establish a comprehensive capability to enhance cybersecurity for the Defense Industrial Base.[15] But SolarWinds was not a formal member of the DIB—nor are most commercial companies and critical service providers. The NDAA is an excellent start, but it should be expanded beyond the DIB to focus on centralized leadership, command and control, and seamless integration of joint authorities.[16, 17]

   To date, private and even public sector entities have largely been left on their own to defend against top tier nation-state foreign intelligence services. In many instances, when the USG becomes aware of an attack, there can be significant delays before the victim is located and informed.

   This model must be reversed to pivot the U.S. to a unified defensive and offensive posture in which information is shared across government with little or no friction, along with established and continuous bi-directional sharing with industry. The creation of a national COP must be backed by adequate resources, technical capabilities, and legal authorities for effective information sharing and the production of actionable intelligence.

PRIVATE AND EVEN PUBLIC SECTOR ENTITIES HAVE LARGELY BEEN LEFT ON THEIR OWN TO DEFEND AGAINST TOP TIER NATION-STATE FOREIGN INTELLIGENCE SERVICES.

2. **Create a National Supply Chain Intelligence Center**

   In MITRE's "Deliver Uncompromised" report, one of our main recommendations was to create a National Supply Chain Intelligence Center (NSIC) like the basic information sharing model used in the war against terrorism—the National Counterintelligence Terrorism Center (NCTC).[18] The NCTC information construct was formed after the 9/11 Commission determined that obstacles to information sharing within the law enforcement, intelligence, and defense communities was a root cause of the failure to consolidate and disseminate *actionable intelligence in a timely fashion*.

We need the same type of approach today to combat supply chain attacks: an organization staffed jointly from those agencies with the necessary legal authorities, working as a team against the common threat against public and private sector U.S. homeland interests. The COP described in Recommendation 1 would be a valuable information feed into an NSIC, which would have responsibility for information sharing, production of actionable intelligence, and unified collection and mission management functions.

It is interesting to note that our primary adversaries have sought many of these unified approaches while they exploit seams between our privacy protections and associated legal authorities. Even so, the U.S. has addressed this problem before through the careful construction of the NCTC model, much of which we believe can be leveraged for supply chain security.

3. **Require Recorded Data for Critical Entities**

The SolarWinds exploit was detected relatively quickly—less than a year after it was inserted. Typically, large-scale sophisticated exploitations go undetected for much longer. Data storage has never been cheaper, and having full packet capture and system logs can help tremendously in forensic analysis within and across organizations to increase understanding and characterization of adversary tactics, techniques, and procedures. This information is even more valuable when coupled with machine learning and artificial intelligence analytics at scale to help generate a comprehensive picture of the span and impact of an attack.

Early detection is especially important for Industrial Control Systems (ICS). ICS such as energy systems or factory automation have real-time information feeds that if unmet or delayed, manipulated, or lost can result in catastrophic failures. After-the-fact forensics on such systems is incredibly difficult without extensive packet capture logs. The good news is that real-time and near real-time monitoring of OT systems is beginning to be addressed by the commercial market space—these early detection technologies should be incentivized and encouraged, and their use mandated in critical applications.

4. **Require Due Diligence and Transparency in Commercial Software Use**

Due diligence, and the transparency required to enable meaningful due diligence, are necessary to make informed risk-based decisions on software vendor use. Even basic due diligence can inform and guide the overall security posture for a company that chooses to use a product with suspicious linkages. For example, some media reports claim that U.S. investigators suspect JetBrains may have been an attack vector into SolarWinds through its deployment within TeamCity, which SolarWinds used in its software build process.[19] This discovery should have increased SolarWinds' attention, as JetBrains is developed by a company founded in Russia and based in the Czech Republic.

Separately, we have seen multiple occasions over the years where software vendors were chosen to provide critical elements of Department of Defense (DoD) or USG software that used developers based in adversarial nations such as Russia and China. Some of these vendors operated over local cloud infrastructure and networks, with all the attendant security risks that should be apparent from publicly posted national security laws.

Due diligence is vital for software used within our key national and defense critical infrastructure systems. The integrity of software means a great deal, particularly since a supply chain compromise provides the means for adversary exploitation, intelligence gathering, or disruption of a critical function, mission or enterprise.

In some cases, establishing the level of transparency needed to provide a reasonable level of confidence in systems may require C-suite attestation to the software supply chain used for key USG, DoD, and critical infrastructure functions, and the introduction of controls that provide the visibility necessary to make that attestation meaningful. We may also need to better define specific cybersecurity controls, and both incentivize compliance and penalize those who fail to act. Actions like these would need to be phased in to allow companies time to comply, and those in regulated areas like energy must be allowed to charge off the necessary compliance costs.

5. **Protect the “Digital Supply Chain”**

   While there is a plethora of opinions and advice on how to technically prevent enterprise or software penetrations, an important but often overlooked area is robust protection of the “digital supply chain”—protecting data during aggregation, processing, storage, dissemination, and access.

   For example, there are multiple examples of China targeting academia that are often reported as a means of stealing intellectual property (IP). However, just as valuable, yet not technically IP, are vast data stores or even metadata from which social or business interactions can be gleaned. China has declared its interest in medical techniques and information, yet available information often includes biological identification markers such as DNA samples from COVID or ancestry tests, or eye, fingerprint, or voice scans used in multifactor or other identity authentication services, which pose significant security risks if not managed and protected. *The U.S. should extend privacy protection regulations to include robust protection of the digital supply chain and impose penalties for gross negligence in their application.* Such “duty of care” is an essential element of software supply chain security, since the digital supply chain also contains the building blocks of software and other end products, platforms, and services.

AN IMPORTANT BUT OFTEN OVERLOOKED AREA IS ROBUST PROTECTION OF THE “DIGITAL SUPPLY CHAIN.”

6. **Build Diversity into System Architectures to Distribute Risk**

   Security against nation-state adversaries is often traded for lower upfront development, purchase, maintenance, or lifecycle costs, with little consideration of the costs of a breach or, in military applications, a failed mission or loss of intelligence information. Unfortunately, there are many examples where government requirements dictate the use of a software suite or architecture for cost or uniformity advantages, while unknowingly making those systems or users targets.

The largest single example in the USG is probably the Intelligence Community IT Enterprise (ICITE) based on Amazon Web Services. ICITE consolidates classified computing enterprises into one cloud-based service, a primary motivation for which was cost savings.[20, 21] Regardless of the vendor selected, this consolidation made ICITE and the many supply chains needed to build it the top targeting priority of nation-state adversaries. The concentrated risk in using one provider for a nationally critical function is extremely high, as the consequence of a successful exploitation is too rewarding and convenient for an adversary to pass over.

Likewise, private sector entities must consider the fragility of their architecture designs, given the many now public exploitations that have occurred in recent years. The concepts of fault tolerant computer and network architectures developed at the dawn of the computing age used diversity and redundancy as a means of increasing mean time between failure (MTBF), mostly to guard against component failure. Approaches based on concepts such as MTBF should be re-explored, with an eye toward system resiliency for select high-consequence infrastructure at the subsystem, system, and enterprise levels, and for some national USG systems.

Conclusions

This paper is not meant to be a detailed review of the SolarWinds campaign and associated technical mitigations.[22] Rather, its intent is to lay out fundamental asymmetries in adversary behavior, our overall national software supply chain security posture, and available opportunities to better align our decision making to account for the actual threat environment.

When viewed from this perspective, both immediate and longer term actions point toward a need for a robust, diverse, and layered security posture. This approach will limit and contain realized threats and reduce their impact and consequences. Such an approach will also drive up the cost for adversaries to execute an operation and disrupt the risk/reward asymmetry currently tipped in their favor.

Although a variety of technology, policy, and legislative actions are underway to begin to address obvious deficiencies in our software supply chain security posture, we have illustrated the larger causes of the susceptibilities that, if continually discounted or left wholly unaddressed, will endure to allow adversaries undue benefits to conduct asymmetric supply chain attacks at an even larger scale.

We hope this paper spurs constructive discussions among decision makers, engineering and security specialists, policy makers, and leaders in all facets of the software supply chain in the public and private sectors, and that going forward, these principles inform the development of a more effective strategic roadmap for software supply chain security.

In addition to laying out these fundamental principles, we have articulated six specific recommendations that address defensive protective measures, much-needed broader situational awareness of the real and potential supply chain threat, and an improved application of technical engineering measures:

1. Create a National Common Operating Picture of Cyber Domain Adversary Actions
2. Create a National Supply Chain Intelligence Center
3. Require Recorded Data for Critical Entities
4. Require Due Diligence and Transparency in Commercial Software Use
5. Protect the “Digital Supply Chain”
6. Build Diversity into System Architectures to Distribute Risk

Endnotes

1. Office of the Director of National Intelligence (ODNI), "Software Supply Chain Attack Graphic." Available at: https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Software-Supply-Chain-Attacks02.pdf [Accessed December 18, 2020].
2. U.S. Department of Homeland Security (DHS), Cyber Security and Infrastructure Security Agency (CISA), Alert (AA20-352A), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," December 17, 2020. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-352a [Accessed December 18, 2020].
3. D. Weeks et al., "2020 State of the Software Supply Chain Report," available at https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report.
4. A. Smith (1723-1790), An Inquiry into the Nature and Causes of the Wealth of Nations. New York, NY: Modern Library, 1994.
5. A.-L. Barabasi, Linked: How Everything is Connected to Everything Else and What it Means. New York, NY: Basic Books, Perseus Press, 2014.
6. Cyberspace Solarium Commission, March 2020, available at: https://www.solarium.gov.
7. D. Geer, E. Jardine, and E. Leverett, "On market concentration and cybersecurity risk." Journal of Cyber Policy 5, no. 1 (2020): 9-29.
8. C. Nissen et al., "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," The MITRE Corporation, 2018. Available at: https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.
9. SolarWinds Orion, accessed on 17 Feb 2021 at https://www.solarwinds.com/orion-platform.
10. CISCO Talos Threat Advisory: Solar Winds Supply Chain Attack, December 14, 2020, accessed at https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html.
11. U.S. Department of Defense, "Cybersecurity Maturity Model Certification," January 2020. Available at: https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf.
12. General Services Administration, "Federal Acquisition Regulations," January 2021. Available at: https://www.acquisition.gov/browse/index/far.
13. The Federal Acquisition Regulation is a set of federal government acquisition rules for both vendors and the government.
14. DHS CISA, "Federal Information Security Modernization Act," accessed January 2021 at https://www.cisa.gov/federal-information-security-modernization-act.
15. Public Law 116-92—Dec. 20, 2019. § 1648 (a).
16. The NDAA recommended integration of cybersecurity with traditional counterintelligence (CI) capabilities to support proactive operations to thwart adversary actions through the integration of cyberspace operations, technology, and offensive operations; operations to thwart malicious cyber activities that integrate cyberspace operations, technological means, and offensive CI operations; and the leveraging of technology to monitor and protect contractor information systems.
17. Public Law 116-92—Dec. 20, 2019. § 1648 (c).
18. C. Nissen et al., "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," The MITRE Corporation, 2018. Available at: https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.
19. E. Kovacs, 7 Jan 2021, "Investigation Launched into Role of Jetbrains Product in SolarWinds Hack: Reports," Security Week, https://www.securityweek.com/investigation-launched-role-jetbrains-product-solarwinds-hack-reports.
20. R. Berliner, "Unclassified ICITE on the Horizon," 15 Aug 2017, Federal Computer Weekly, https://fcw.com/articles/2017/08/15/icite-unclassified-odni-cio.aspx.
21. "Intel Agencies ready to start deploying shared IT systems," 16 April 2014, Federal News Network, https://federalnewsnetwork.com/defense/2014/04/intel-agencies-ready-to-start-deploying-shared-it-systems/.
22. For a detailed discussion, see C. Clancy et al., "Deliver Uncompromised: Securing Critical Software Supply Chains," The MITRE Corporation, 2021. Available at: Deliver Uncompromised: Securing Critical Software Supply Chains | The MITRE Corporation.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™