Supply Chain Security

S.Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

- Supply chain security is management of the supply chain that focuses on risk management of
  - external suppliers,
  - vendors,
  - logistics,
  - transportation.

- Supply chain security protects physical integrity and defends against cyber threats.

Secure Supply Chain

- Using accredited and certified suppliers
- Performing penetration and vulnerability tests [How much it is possible]
- Logging and tracking shipments
- Regularly auditing open source and vendor source codes. [How much it is possible]
- Authenticated data transmissions

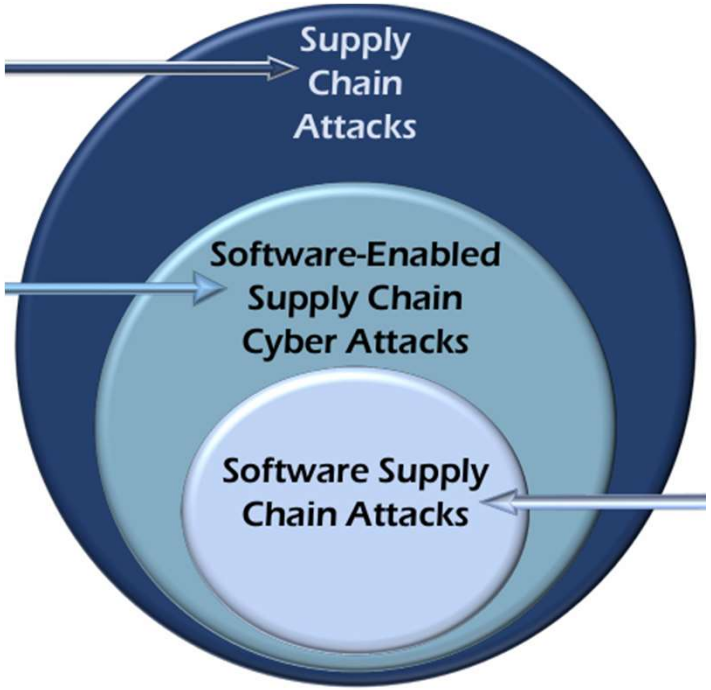
Basics

- Software supply chain security aims to secure the components and activities that go into developing and deploying an application, such as people, processes, dependencies, and tools.

- Software supply chain security differs from traditional application security, which focuses on
  - tools,
  - technologies,
  - automated processes
- used to identify, fix, and protect software against vulnerabilities that could impact the application at run-time.

Supply Chain Attack

- It combines two or more attacks
  - a malign actor first attacks at least one supplier within a supply chain
  - uses that attack as the means for attacking other suppliers or the final customer.
- Software-Enabled Attacks
  - Exploit software vulnerabilities (Log4j, for example) to disrupt, disable, or destroy supply chain resources, processes, or services.
- Software Supply Chain Attacks
  - Malign actors may attempt software supply chain attacks after infiltrating a software developer's networks, systems, personnel, or external resources.



Possibilities

- Modify the source code of genuine programs by illicitly accessing a developer's infrastructure, but may also exploit the legitimate access possessed by a malicious insider.
- May seek to exploit tools, dependencies, shared libraries, and third-party code or compromise the personnel or systems of associated developers or distributors.
- An attack against a supplier that then enables a subsequent attack against another supplier or the final target.
- Using software after it reaches end-of life exposes users to conventional cyber attacks.

Software Integrity

- For example, in 2020, security researchers discovered a backdoor dubbed GoldenSpy in tax software required by foreign companies doing business in China.

- In other cases, external attackers have hidden malware in unfinished software before developers added digital signatures, thereby imbuing compromised software with a presumption of trustworthiness.

- In other instances, attackers have injected malicious code through genuine updates and patches for software releases and upgrades, or have compromised servers used for delivering software updates, utilizing them to deliver malware to unsuspecting customers.

Authenticating Software Integrity

- Code Signing
- Hashing

Open-Source Software (OSS)

- Open-Source Software (OSS) is widely available under licensing terms that ease its use and distribution.
- Source code for OSS must remain freely available, OSS projects promote transparency and facilitate modifications.
- In 2021, developers of the Linux kernel determined proposed updates provided by University of Minnesota (UMN) researchers deliberately included security flaws.
  - In response, the Linux kernel development team banned UMN in its entirety from future contributions outright
- The number of public repositories hosted by popular software development and source code management platform GitHub exploded from 46,000 in February 2009 to more than 200,000,000 by February 2022.

Attribution

- The complexity of software supply chain attacks and the resources necessary to accomplish them often implicate state actors. However, assigning culpability to specific national intelligence services can be challenging.

- In July 2020, a federal grand jury indicted two hackers working with China's Ministry of State Security (MSS) for a global computer intrusion campaign targeting intellectual property and confidential business information.

- In April 2021, the United States announced new economic sanctions directed against Russian technology companies for their role in Russian malicious cyber activities, including the SolarWinds Orion software supply chain attack.
  - Publicly disclosed in December 2020, the source code compromise of the SolarWinds Orion infrastructure monitoring platform is among the most significant software supply chain attacks impacting the United States to date.

- In March 2022, the Department of Justice unsealed two indictments charging four Russian nationals who worked for the Russian government with orchestrating hacking campaigns that included hiding Havex malware inside legitimate software updates for industrial control systems used by the energy sector.

Requirement

- As C. Paulsen [5] indicated that there are most cyber security issues originates in the supply chain, there is a need to identify policy to buy, build, deliver, and dispose of technology goods and services.

- The software bill of material provided by the developer makes the user aware of various technologies used.

- However, a tool that helps the users to analyze the software bill of material increases the confidence.

Materials

- File Extension
- Software Version
- IP and URL
- Back End Packages

Statistics

- 80%: Applications that contain at least one security vulnerability
- 42%: Apps with flaws left unaddressed for more than a year
- 71%: Pros who perceive their software attack surface as unmanageable
- 95%: Teams using 20 or more tools to manage application security
- 72%: Pros who said software supply chain security was their biggest blind spot
- 60%: Organizations demanding software bill of materials (SBOM) by 2026
- 1300%: The increase in threats via OSS package repositories
- 70%: Applications that have flaws in third-party code
- 96%: Applications with OSS vulnerabilities that are completely avoidable
- 54%: Major code changes that goes through a formal security review process

https://www.reversinglabs.com/blog/software-supply-chain-security-by-the-numbers-30-key-stats-that-matter

SBOM

- Supply chain attacks have become more frequent, sophisticated and devastating, as evidenced by high-profile incidents such as SUNBURST, Kaseya and Apache Log4j.

- SBOMs are a standardized inventory of software components used in a particular product or system, including
  - their versions,
  - dependencies
  - sources.

- SBOMs provide transparency and visibility into the software supply chain.

- U.S. National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), have been advocating for SBOMs as a best practice for software supply chain security.

Software Supply Chain

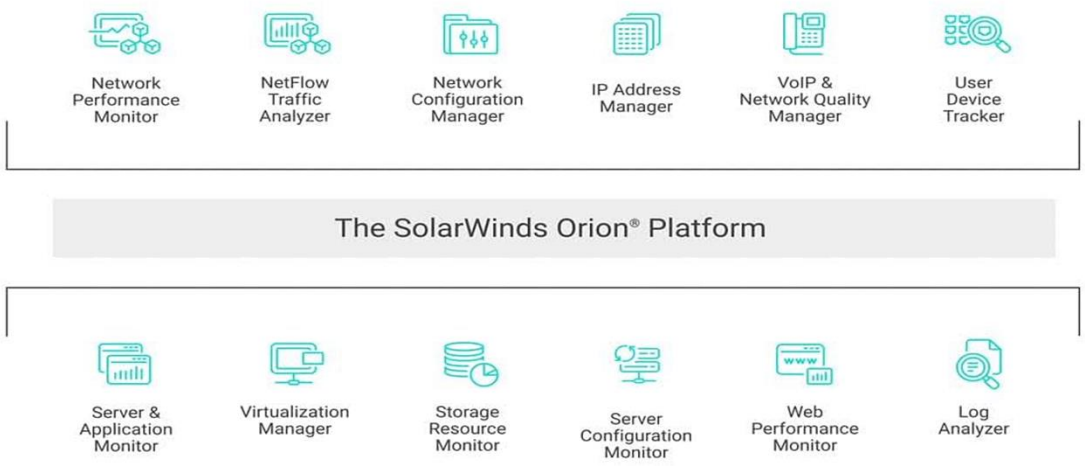
- The software supply chain is made up of everything and everyone that touches your code in the software development lifecycle (SDLC), from application development to the CI/CD [Continuous Integration and Delivery] pipeline and deployment.

- The supply chain includes networks of information about the software,
  - like the components (e.g. infrastructure, hardware, operating systems (OS), cloud services, etc.),
  - the people who wrote them,
  - and the sources they come from, like registries, GitHub repositories, codebases, or other open source projects.

- It also includes any vulnerabilities that may negatively impact software security – and that's where software supply chain security comes in.

SolarWinds Attack

- SolarWinds offers an IT performance management and monitoring system called Orion.
- To enhance its effectiveness, Orion has access to customer system performance logs and data, making it a lucrative target for hackers.



https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack

Attack

- The hackers used a supply chain attack to insert malicious pieces of code into the Orion framework.
- In the Orion hack, a backdoor was created which could be accessed by the hackers to impersonate accounts and users of victim organizations.
- This backdoor allowed the hackers to access system files and hide their tracks by blending into the Orion activity, masking the malicious code from antivirus packages.

Attacks

- By late 2019, the SolarWinds network had already been breached by malicious actors. The update containing the backdoor was a remote access trojan (RAT).

- This particular malicious update was named the Sunburst update.

- Come Spring 2020, and this harmful update was already being pushed out to users.

- Customers had no reason to doubt the update considering it came directly from the SolarWinds servers.

Detection

- FireEye, a cybersecurity company, detected the malware spreading to their customers and was able to identify the Sunburst update package responsible for the breach.

- Once detected, several customers could detect similar behavior in their systems and their customers, indicating a rapid spread of the malware package.

- First detected in late 2020, the Sunburst update had infected thousands of systems worldwide by then.

Affected Users

- 18,000 customers of SolarWinds had applied the Sunburst update, which then allowed the remote access trojan to infect all their customer systems and networks.

- Notable victims, the US departments of health, treasury, and state were affected by this attack.

- FireEye, Intel, Cisco, and Microsoft are affected by this malware.

Vulnerability Exploitability eXchange (VEX)

- A VEX document is a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities.

- Minimum Data Elements
  - VEX metadata (Identifier string for the VEX
  - document, Author, Author role, Timestamp)
  - Product Details
  - Vulnerability Details (CVE or other vulnerabilities)
  - Product Status Details (Affected, Not Affected, Fixed, Under Investigation)

SBOM vs VEX

- Inventory described in a SBOM will typically remain static until such time the inventory changes.
- However, vulnerability information is much more dynamic and subject to change.
- Therefore, it is recommended to decouple the VEX from the BOM.
- This allows VEX information to be updated without having to create and track additional BOMs.

Bugs/Issues

- Developer Ignorance
- Intentional
- Updates

References

- Software Supply Chain Attacks, National Counter Intelligence and Security Centre (NCS), US
- https://devops.com/the-role-of-sboms-in-software-supply-chain-security/
- https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security
- https://www.hpe.com/in/en/what-is/supply-chain-security.html
- https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf
- https://cyclonedx.org/capabilities/vex/