Sandia National Labs Response re: Position Statement 4

A Novel Approach to Assessing the Software Supply Chain Risk of Software Binaries

In this white paper is a response to position statement 4 that involves leveraging a methodology developed by Sandia Labs and the resulting HECATE[1] (High-density Evaluator of COTS Applications for Trust and Efficacy) platform, to help inform needed requirements to actionably reduce risk in commercial software. We contend that source code analysis is only part of the approach to securing the software supply chain as binaries (such as those distributed in commercial of the shelf software) are a critical part of the equation. HECATE automates testing and assurance of software from a dynamic, holistic view because end-to-end security is a dire need in today's world of opaque software.

Background

Many of today's source code solutions (such as code signing, software bill of materials) address only part of the puzzle. Current supply chain attacks show that advanced persistent threats, such as those seen in the SolarWinds[2] attack, can have legitimate access and credentials to commit code to the repositories of commercial companies, subverting many of the systems that are or can be put in place.

Much of the current effort focuses on securing the development pipeline; however, this presupposes that there is (1) the ability to influence the development lifecycle and (2) that companies audit and address concerns found within the pipeline. The customer has limited optics into that correction process and as a result, owns residual risk.

While products for threat detection and protection exist, such as malware identification, there are currently few products that offer a solution for preventing, detecting and mitigating software supply chain attacks. Government agencies cannot escape the reality that critical functions will be driven by COTS on our networks and **we must** include software binaries as part of the attack surface and have associated standards and mitigations.

Gap

An exigent gap exists in the market today because of the lack of omniscient visibility and transparency into the application code, software libraries, supply chains, and upgrade platforms. Application users must assume the risk of all applications (particularly those without source available), and trust that the vendor:

- Has a robust cyber security posture with secure development practices
- Does due diligence when inspecting their software code commits
- Does due diligence when importing and updating packages that are part of their product

Approach

We propose a radically different approach for software supply chain assurance. We must combine multiple dimensions of data (static, dynamic binary and supplier information) to better understand and evaluate COTS applications in an automated and consistent fashion. The empirical and artifact driven methodology may be used to uncover software subversion in addition to providing supply chain insights. This supports a move toward an evidence-based approach to assuming risk when software is introduced into computing environments.

With HECATE, we showed that it is possible to have an analysis platform that can identify software supply chain risks and provide heuristics on suspect software behaviors. This information can be used to accumulate trust in compiled commercial and open source software.

[1] https://www.rdworldonline.com/rd-100-2020-winner/high-density-evaluator-of-cots-applications-for-trust-and-efficacy-hecate/

[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Sandia National Labs Response re: Position Statement 4

Outcome

HECATE gets to the root of software risk by not just viewing the code (when available), but by taking a holistic view of how that code came to be (foreignness, developer information, provenance), with emphasis on how the software behaves in an operational environment. The platform is driven by the inclusion of:

- Automated vendor assessment through open-source intelligence
- Static analysis of code via a plug-in architecture
- Dynamic excitation of software in a virtual environment
- Deep introspection of software execution
  - Host level (memory access, disk access, security subversion, …)
  - Network level (scanning, command and control, …)
- Automated extraction of raw data and derivation of:
  - Risk indicators
  - Maliciousness
- Object-based database for collection of artifacts for:
  - Historical and trending data points and analysis
  - Cross-correlation (with other versions/software/vendors)
  - Sharing of risk assessments and raw data
- Tailored reports to express supply chain threats
- Risk assessment for software

Figure 1 shows the tools and workflow. Analysis begins with an automated determination of the provenance and trustworthiness of linked libraries in the COTS applications. HECATE then provides automated heuristics and dashboards on potential risks introduced by the software as it is executed in a virtual environment - leveraging conventional supply chain tools, public information on software providers, and overlays of known vulnerability information to form a risk profile for the application under study. The risk profile brings factors for consideration to the forefront so decision-makers can make informed choices based on the risk tolerances of the networks under their purview.

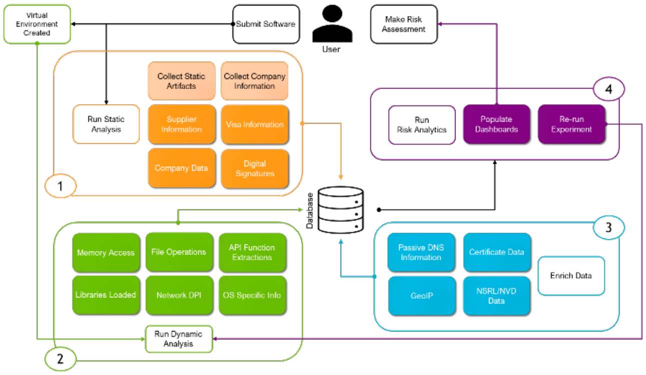

Figure 1: COTS Application Workflow

Proposed Path Forward

Underlaying these techniques are a set of principles and standards:

- a common, repeatable way to exercise software prior to being installed on systems
- a common data model that can drive standards in interoperability
- a method for embedding SME knowledge into analytics
- a method for analyzing the entire system in a holistic fashion
- tools to enable mission to execute in a risk-informed fashion **without significantly impacting** operations
- automated, scalable, and extensible tools/methods to measure risk and provide usable, actionable data
- enable better prioritization of analyst efforts

We hypothesize that the approaches leveraged in HECATE may provide new techniques and avenues to assure software deployed in various environments and welcome further discussion.