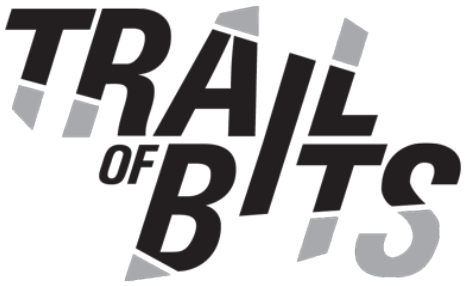

Kubernetes Working Group

Assessment Proposal and RFP Response

Sanitized version for limited distribution

Prepared For:
Kubernetes Working Group, Cloud Native Computing Foundation

Prepared By:
Dan Guido | *Trail of Bits*
dan@trailofbits.com

Shawn Moyer | *Atredis Partners*
shawn@atredis.com

Stefan Edwards | *Trail of Bits*
stefan@trailofbits.com

Nathan Keltner | *Atredis Partners*
nathan@atredis.com

Date of Proposal: 11/30/2018
Quote Valid Until: 12/30/2018
Version: 1.0

About this Version

At the request of the Kubernetes Security Audit Working Group, Trail of Bits and Atredis Partners have created this sanitized version of our RFP response, for limited distribution among the Kubernetes community. In this version, client references have been removed out of respect for our clients' privacy, and the pricing table has been omitted, since it did not reflect the final, negotiated engagement cost.

Executive Summary

Wide adoption of Kubernetes by service providers and their clients has resulted in the containerization system rapidly becoming a key part of cloud infrastructure. Kubernetes is a common and growing pattern in infrastructure management for cloud-scale deployments. It is deeply integrated into multiple cloud providers, and represents a common architecture that clients can design their applications and systems around, and compose common tasks into Kubernetes-specific design patterns. The quality of these patterns and the penetration of Kubernetes into many organizations' infrastructure belies the hard work and research that went into its design.

As part of this commitment to quality, the Kubernetes Working group released a Request For Proposals, seeking vendors to holistically review the state of security in Kubernetes, to source code analysis, configuration review, and dynamic runtime testing of a running Kubernetes environment. The Kubernetes team also stated a need for a threat model of the containerization system itself, including items such as flow diagram and control family weaknesses, in order to better understand the nature and location of risks to the Kubernetes system.

The Engagement Team

In order to best accomplish this review, Atredis Partners, a firm with industry-leading capabilities in penetration testing and exploitation of complex targets and cloud infrastructure, has partnered with Trail of Bits, a firm with industry-leading capabilities in low-level system security, cryptography, exploitation, and reverse engineering. The review will take a multi-phased approach, with multiple teams completing tasks across the Kubernetes threat landscape, source code, and live running environment.

Trail of Bits and Atredis Partners (collectively, "the engagement team" or the "the assessment team") also have a past history of successful collaborations, working on long-term complex security engineering and assessment projects. Our two organizations will work as a single team, with communications and project management tasks shared between both firms. For clear delineation of responsibilities, each firm will be assigned to specific objectives of the RFP as individual work streams in the project, such as cryptography, network isolation, etc.

We believe the combined skill sets and reputations of our two firms will provide the working group with the best assessment and research capabilities in our industry, bar none, and that the respect our two teams have will garner support for the ultimate outcome for the project of public, referenceable documents on the security of the Kubernetes platform.

Background

Kubernetes is a cloud orchestration system focused on “deploying, scaling, and operating application containers across clusters of hosts.” This has led Kubernetes to have a large surface area across multiple facets of the system, including networking, authentication, authorization, cryptography, secret management, and isolation. Kubernetes has seen adoption by large cloud providers as both an exposed orchestration framework for client use, as well as cloud providers’ clients deploying their own Kubernetes infrastructure to the cloud. As such, the Kubernetes Third-Party Audit Working Group (working group, henceforth) was created to select a vendor or vendors to provide a comprehensive review of the Kubernetes system as a whole.

The working group has selected five areas that the assessment should focus on:

- Networking
- Cryptography
- Authentication & Authorization
- Secrets management
- Multi-tenancy isolation

Due to the scale that Kubernetes seeks to achieve, as well as the environments in which it is used, each of these areas comes with various risks that the working group is seeking to expound upon. Additionally, the working group is seeking reference implementation guidelines, in the form of YAML files, and a formal threat model including system flows and threat actors, to better understand the risk presented and the inherited controls from Kubernetes itself in order to mitigate those same.

Kubernetes’ design presents new sets of risks and controls to be evaluated by the assessment team. For example, containers and nodes have a unified network architecture that allows a container to have a consistent IP address within the Kubernetes network and does not rely on Network Address Translation (NAT). At the same time, Kubernetes includes strong Network Policies which network plugins can utilize to filter and control communications between pods within a Kubernetes cluster. Our engagement team is uniquely positioned to assess the security of these new protocols, threat surfaces, and mitigations, including a cryptography practice that engineers secure protocols of this nature, as well as some of the most well-respected vulnerability researchers in our industry.

Project Goals

The phases and objectives of this project are designed to give the working group the information necessary to make informed decisions about risk to the Kubernetes platform, and an evaluation of the security posture of the platform as it exists today. This philosophy dictates the following goals, at a high level, for the proposed project described in the Working Group's RFP:

- Provide an estimate of the overall security posture of the system.
- Evaluate the difficulty of system compromise from an attacker.
- Identify design-level risks to the security of the system.
- Identify implementation flaws that illustrate systemic or extrinsic risks.
- Provide recommendations on best practices that could improve resistance to attack.
- Educate the project team on common security flaws and testing techniques.
- Where possible, deliver system-specific security tools to reduce future risks.
- Where appropriate, provide alternatives to implementations and components in use.
- Uncover, discuss, and document architectural risks to the system in the form of a threat model and data flow of the selected system components.
- Provide a reference architecture that the client may use, both to evaluate the coverage of the security assessment, as well as to provide as a baseline of a secure reference implementation of the system.

The assessment team will conduct a detailed security analysis from the perspective of an attacker with access to all available source code and documentation, in a live, representative example of a typical Kubernetes deployment. The assessment team will collaborate with the working group extensively, reporting findings as soon as they are confirmed and helping the working group identify ideal paths toward mitigation.

This engagement will culminate in a report detailing any findings from threat modeling, source code review, or live assessment, a reference implementation of a Kubernetes configuration, and a white paper detailing observations about Kubernetes, its code base, live environment, and notes on the security of the same. Findings within the report will include a justification as to the content of the finding, a proof of concept exploit (if relevant), an attack scenario including relevant threat actor, and recommendation guidance.

Project Scope

Security Assessment and Component Scope

The RFP outlines requests for specific outputs, such as the documented Threat Model or White Paper, as well as areas of review that broadly encompass various components within the Kubernetes architecture. The in-scope components that may come under review include, at a high level, those components at the Master level (or cluster control plane) and those at the Node level. Specifically, these include:

Master / Cluster Control Plane

- kube-apiserver
- etcd
- kube-scheduler
- kube-controller-manager
- cloud-controller-manager

Node

- kubelet
- kube-proxy
- Container Runtime

The scope of review for each component will be constrained to the guidelines outlined in the RFP and the referenced Bug Bounty scope documentation, as described in the RFP. Specifically, the Container Runtime component is generally out of scope, with exceptions for any areas of Kubernetes that may introduce vulnerabilities into the Container Runtime. Likewise, components outside of Kubernetes direct responsibility, such as addons implementing CNI to provide Kubernetes networking, are out of scope for the purposes of the assessment review.

For each in-scope component, the assessment will perform source review and dynamic testing to provide coverage across each of the requested Focus Areas as described below.

Threat Modeling

The assessment team will conduct a threat model of the Kubernetes system, in the style of NIST 800-154 (“Guide to Data-Centric System Threat Modeling”) and Adam Shostack’s “Threat Modeling: Designing for Security.”

The outputs of this threat modeling exercise will serve to define and inform the team’s focus throughout the engagement, and take place first in the project timeline to help direct the testing, analysis and deliverables for this project. Specific tasks may include:

- Conversations with stakeholders and developers to understand the components within the system, and the data processed therein.
- Discussions surrounding the sensitivity of any data processed by a component, which actors may have access to it, and the risk of exposure or theft from malicious actors who had compromised or abused legitimate access.

- Identification of “boundaries of trust” in order to trace passing of security sensitive information.
- Dialog surrounding the communication protocols, protections, and the various controls (logging, sensitive data protection, &c.) used to connect components of the various areas of the system.
- Diagramming the control flow, documenting control location, trust boundaries, and any weaknesses noted about the same.
- Identification of common failure modes that inform areas of focus within the overall scope.
- Identification of components requiring inclusion of specifically requested tasks from the RFP. This will note specific usage of cryptography and secrets management, as well as note areas potentially susceptible to AuthN/AuthZ or multi-tenancy issues.

Reference Implementation

The working group’s RFP describes a reference implementation of Kubernetes. The test environment will be generated in collaboration with the working group, documented, and submitted for review. This documented reference implementation will provide the baseline of the assessment, and will be used for proof of concept generation, runtime testing, and as a source for generating technical documentation such as the whitepaper or any findings resulting from the engagement team’s analysis.

Drawing from knowledge gained throughout this engagement, the assessment team will use this reference architecture to help define and provide a best-practice configuration from a security perspective for Kubernetes, reified in a set of YAML configuration files that can be consumed by others for securing a default Kubernetes implementation.

White Paper

The working group also requested one or more white papers providing a public-facing retrospective of observations of the engagement team during the assessment as a whole. This will take the form of one or more white papers that include knowledge gained, tips and tricks, tooling, configurational concerns, and the like for building a secure Kubernetes infrastructure.

The objective of these public-facing documents, as our team understands it, is to provide an useful reference on securing Kubernetes, defining the key aspects of the Kubernetes attack surface and security architecture, ultimately enabling end users make sound design and implementation decisions.

Engagement Focus Areas

Secrets Management

The assessment team will review the management of secrets within the system, including the strength of any storage algorithms, which actors may have access to those same secrets, and ways in which they may be exposed to various threat actors. Tasks within this phase may include:

- Review of storage locations for secrets.
- Review of mechanisms to share secrets within various components of a system, including transmission within the cluster itself.
- Evaluation of the strength of all algorithms used in the storage and transmission of secrets.
- Discussion and documentation of risks impacting the repudiation, integrity, and secrecy of any secrets within the system.

Networking

The assessment team will perform source review and dynamic testing of relevant Kubernetes components for introduction of network-based vulnerabilities. Much of Kubernetes practical networking exposure relates to out-of-scope networking plugins, guiding the assessment focus to the Kubernetes components implementing or interacting with CNI plugins.

Tasks within this phase may include:

- Review of the Kubernetes side of the CNI specification
- Identification of design-level issues that impact downstream networking plugins
- Highlighting areas where Kubernetes configuration or implementation produce invalid security assumptions relevant to Kubernetes deployments or plugin developers
- Review of internal networking design and implementation, protocol usage, and transport

Cryptography

The assessment team will review the cryptographic algorithms within the Kubernetes system, from both an implementational as well as theoretical strength perspective. Specific tasks may include:

- Discovery of implementation defects that impact the security guarantees of the selected algorithms.

- Discussion of the security profile for the selected algorithms and any modes or associated accoutrements, vis-a-vis their usage within specific locations of the Kubernetes codebase.
- Recommend algorithms, libraries, and implementations to replace any weak, outdated, or incorrect implementations discovered during the assessment.

Authentication and Authorization

The assessment team will review the authentication and authorization mechanisms within the system for items such as repudiation of actors, the strength of that repudiation, and the granularity to which they may be repudiated. Sample tasks may include:

- Assessing the authentication mechanisms for theft, replay, and information disclosure potential.
- Reviewing the strength of claims, their location, and how they intersect the authorization schema within the system.
- Discovering ways in which authentication or authorization may be bypassed.
- Uncovering information that may be leaked by users who are authenticated but not authorized for a particular action.

Multi-tenancy

The assessment team will uncover the edges and information disclosed to users within the same Kubernetes infrastructure, but of potentially-different organizational sensitivity. Sample tasks may include:

- Identification of vulnerabilities related to or exacerbated by malicious control of user code executing within Kubernetes pods.
- Cross-host communication to simulate post-exploitation scenarios.
- Bypass of intended isolation boundaries between Kubernetes components.
- Exfiltration of secrets that may be available to a compromised container.
- Resource exhaustion or other host-level denial of service attacks.

Operational Approach

Collaboration and Client Focus

A key aspect of our team's engagement style is collaboration, flexibility, and client focus. We assign a project manager, as a non-billable resource, to every engagement to serve as a single point of contact from kickoff to outbrief, managing the day-to-day operational and reporting goals for the project.

In an overwhelming majority of our projects, our engagement team also collaborates in real time with our clients via services like Slack, Chime, Hangouts, and Signal, giving us a direct feedback loop throughout the project and helping our team rapidly confirm vulnerabilities and address any blockers to the project's success.

Project Inception

As described in the RFP, our team expects to being the engagement with an initial one-hour kickoff call with the key principals for the project. The kick-off meeting will review the goals of the project, the project risks and mitigations, and the proposed approach. At the kick-off meeting we'll work with the users to refine the tasks and milestones for each phase of the project.

After the kickoff, the team will schedule regular status meetings with the working group during the project, of either daily or weekly frequency, at the client's discretion. Our team will report findings in real-time as soon as they are confirmed, via secure communication channels.

Testing and Acceptance

Our team follows an iterative approach to security research and software engineering. We recommend reviewing weekly project milestones for approval instead of waiting for a large, final review. This helps us to continuously identify problem points and deal with them proactively.

Throughout the engagement, we communicate findings as they are identified and validated, and schedule ongoing engagement meetings and touchpoints, keeping our process open and transparent and working closely with our clients to focus testing efforts where they provide the most value.

This approach catches defects early and helps us lead engineering and research into a direction that solves well-defined problems.

Risks to the Engagement

Although the duration of each project will be selected to provide a balance between coverage and timeliness, detection of all potential vulnerabilities without the ability to formally prove correctness is impossible. The assessment team will mitigate this risk by following a systematic approach to ensure high coverage and provide a best-effort assessment in the time allotted.

Assessment scope is constrained to Kubernetes-provided code, although issues that impact the overall security of Kubernetes may be discovered, or even more prevalent, in third-party code. In real-world scenarios, attackers will not be constrained to this distinction and may target code that is out-of-scope for this assessment. As a results, the findings from this security review could provide a false sense of security for Kubernetes. These concerns will be addressed by documenting areas of third-party risk in the threat model.

For example, specific vulnerabilities in Kubernetes may only be present within specific environments or configurations that are out of scope for this assessment. For example, a theoretical edge within Google Kubernetes Engine may not be exposed in the reference implementation of the assessment team. It will be critical to the engagement's success that the team focus on the core codebase, while still taking into consideration that integrations with other components constitute a significant part of Kubernetes' attack surface.

Requirements for a Successful Engagement

In order to carry out a successful engagement and mitigate project risk, the assessment team will require access to the following:

- Access to a designated project sponsor and appropriate technical resources.
- Meetings with all stakeholders at the appointed time during Threat Modeling activities.
- Access to all in-scope source code and any documentation for it, preferably via a source code repository.
- Detailed build instructions, configuration files, a VM that can build the software (e.g., VMware, QEMU, etc.), or access to a build cluster for repeated rebuilds.
- Documentation discussing potential future directions, design intent, and that may influence the recommendations made by the assessment team.
- Access to a technical point of contact at the project under review.

Project Deliverables

After each week of the engagement, the assessment team will report on actions taken, confirmed vulnerabilities found, and guidance on next steps.

The assessment team can provide a readout of the weekly report, typically lasting one hour, with one or more technical representatives from the working group. This meeting will cover flaws identified during the assessment, offer guidance on structuring remediation efforts, and more effective security testing.

The assessment team will provide a final assessment report. Typical final reports follow the outline below:

1. Executive Summary
    - Short description of the project and what was tested
    - Analysis of overall security risk based on the findings
    - Brief summary of the recommendations
    - Review of project goals and estimate of coverage
2. Comprehensive List of Vulnerabilities
    - Detailed explanations sufficient to identify and/or reproduce the vulnerability
    - Attack and exploit scenario to provide context for the vulnerability
    - Recommended short and long term mitigation steps
3. Appendices, if applicable
    - Reference material used to support findings
    - Additional detail or context for larger security issues
    - Code used to reproduce or exploit a specific finding
    - Any tools created during the assessment to aid future regression testing
    - Trail of Bits will provide any artifacts developed during the assessment

The assessment team will provide a final readout of the assessment component deliverable, typically lasting one to two hours, with one or more technical representatives from Customer. This meeting will cover flaws identified during the assessment in depth and offer guidance on structuring remediation efforts and more effective security testing.

Example reports from Trail of Bits can be found in their ‘publications’ repository on Github, and example reports from Atredis Partners are available on their website.

The assessment team will provide a set of YAML files detailing a reference implementation, a collection of any tools or notes that come out of the assessment, and one or more white papers detailing observations uncovered by the assessment itself, as described in the Project Scope section of this document.

Project Schedule and Location

Services are expected to start upon mutual agreement with the engagement team and the working group. As described in the RFP, testing phases are expected to occur over approximately 8 weeks of calendar time, with the final white paper delivered 3 weeks after testing concludes.

Services are expected to be performed from Trail of Bits and Atredis Partners office locations, with site visits conducted on an as-needed basis.

If applicable, travel and expenses are billed as incurred, after client approval. Travel meals and expenditures will be billed under US GSA (domestic) or US State Department (international) per diem guidelines. Other typical travel costs may include airfare, mileage, and automobile rental, where applicable.

About Trail of Bits

Since 2012, Trail of Bits has helped secure some of the world's most targeted organizations and products. We combine high-end security research with a real world attacker mentality to reduce risk and fortify code.

Our clientele -ranging from Facebook to DARPA- lead their industries. Their dedicated security teams come to us for our foundational tools and deep expertise in reverse engineering, cryptography, virtualization, malware, and software exploits. According to their needs we may audit their products or networks, consult on the modifications necessary for a secure deployment, or develop the features that close their security gaps.

After solving the problem at hand, we continue to refine our work in service to the deeper issues. The knowledge we gain from each engagement and research project further hones our tools and processes, and extends our software engineers' abilities. We believe the most meaningful security gains hide at the intersection of human intellect and computational power.

About Atredis Partners

Atredis Partners was created in 2013 by a team of security industry veterans who wanted to prioritize offering quality and client needs over the pressure to grow rapidly at the expense of delivery and execution. We wanted to build something better, for the long haul. Since 2013, Atredis Partners has doubled in size annually, and has been twice named to the Saint Louis Business Journal's "Fifty Fastest Growing Companies" and "Ten Fastest Growing Tech Companies". In 2018, Atredis Partners joined the ranks of the Inc. 5,000 list of fastest growing private companies in the United States.

The Atredis team has built a reputation for delivering deeper, more advanced assessments than any other firm in our industry. Atredis Partners team members have presented research over fifty times at the BlackHat Briefings conference in Europe, Japan, and the United States, as well as many other notable security conferences, including RSA, ShmooCon, DerbyCon, BSides, and PacSec/CanSec. Atredis team members have authored and co-authored several notable books, including The Android Hacker's Handbook, the iOS Hacker's Handbook, Wicked Cool Shell Scripts, Gray Hat C#, and Black Hat Go.

In 2015, we expanded our services portfolio to include a wide range of advanced risk and security program management consulting, expanding our services reach to extend from the technical trenches into the boardroom. The Atredis Risk team has extensive experience building mature security programs, performing risk and readiness assessments, and serving as trusted partners to our clients to ensure the right people are making informed decisions about risk and risk management.