Nephio Project
MINUTES OF THE TECHNICAL STEERING COMMITTEE
June 8, 2023
10:00 am Pacific Time

Voting Representatives
Please add + after your name if you are attending
Google
-Kandan Kathirvel (Chair) +

Wind River
-Seshu Kumar Mudiganti

Nokia
-Timo Perala +
Wim Henderickx (Nokia) for Timo

Deutsche Telekom
-Bernard Tsai

Vodafone
-Iain Wilkinson +
-Riccardo Gasparetto Stori

Equinix
-Oleg Berzin

Intel
-Sundar Nadathur +

TIM
-Fabrizio Moggio

Ericsson
-Ciaran Johnston +
-Peter Woerndle

Casa Systems
-Eric Gaudet

Mavenir
-Jane Shen +

Bell Canada
-Daniel Bernier
-Marc-Alexandre Choquette

TELUS

-Sana Tariq

Aarna Networks
-Sandeep Sharma

Orange
-Eric Debeau +

VMware
-Hunor Demeter: present +
-Padma Sudarsan

Argela
-Erhan Lokman

Capgemini
-Sandip Sarkar
-Chandra +

F5
-Sanju Abraham
-Ravi Ravindran +

Kubermatic
-Sebastian Scheele +

Verizon
-Gene Bagwell

Attending
Please add yourself here if you are not a voting representative

Lucy Hyde (LF) +
Julian Suarez (LF) +
Sunny Cai (LF) +
Balaji Varadaraju +
Charles Eckel
John Belamaric +
Alexis de Talhouet
Ranny Haiby
Vishwanath Jayaraman (Red Hat) +
Tal Liron
Reden Martinez
Liam Fallon
Radoslaw Chmiel
Anh Thu Vo
Stephen Wong +

Keguang He
Refael Hamo
Selcuk Duman
David Bainbridge (Ciena)
Wajeeha Hamid
Mike Woster
Vance Shipley (SigScale)
Olivier Smith (MATRIXX)
Borislav Glozman
Kaushik Bhandankar
Philippe Jeurissen
Senthil Kumar Ganesan
Subhash Kumar Singh
Byung Woo-Jun
John Mechling
Phil Porras +
Victor Morales (Samsung) ++
Girish Kumar
Rahul Jadhav +(AccuKnox) +
Raj Panchapakesan +
Shekhar C
Gaurav

Call to Order
Kandan Kathirvel (KK) called the meeting to order at 10:03 am. Lucy Hyde (LH) and Julian Suarez (JS) assisted in recording the minutes. LH reviewed the antitrust policy notice.

Agenda/Action Items
Kandan Kathirvel (KK) reviewed the agenda for the meeting. There were no changes or additional topics added.
Timo P. provides update on D&TF. Overall Nephio presentations were delivered nicely.
John B. walks through release readiness checklist

Release Readiness Checklist:
John B. goes through presentation of what is planned to be discussed next week.
Kandan K asks for others input to be added to checklist and if there is any questions on what will be presented.
John B. explains the status, meetings, and current state of where they are at. An extra week is needed but still expected to deliver what was requested.
TSC Members, there is a special TSC meeting on June 15th at 10am PT/1pm ET to approve Release 1

Versioning Scheme for Nephio:
Bala presents versioning scheme options. Bala provides and presents three options (Semantic version, Increasing release numbers, and Numbers plus names)
Key components to consider regarding versioning are external releae name/number, Github tags/branches, and API versioning and compatibility.

John B. emphasizes the need to set expectations appropriately and the versioning reflects that. John B. continues to explain API versioning and kubernetes.
Victor M. explains a year and month alternative option possibility.
Kandan K. to put together a pros and cons list and request input from TSC to capture all possible suggestions.

R1 - Target Dates:
Bala asking for input and finalized version from John B. for next Thursday.
Bala, Kandan and John B. to discuss internally.

Rahul Jadhav: Nephio Security in the context of kubernetes security automation:
Nephio security consideration - a big part is the design aspect.
-Kubernetes-native design where pods are execution units
-Co-located worklods from multiple vendors increase various security risks, where the broad application could compromise the control plane
-This assumes basic security practices are in place (code/secrets/image vulnerability/cloud account configuration scanning)

Intent Driven Security Automation:
Intent Drive Security Automation is designed to use kubernetes effectively through specificing the intent of resource models and deploying the appropriate resources to enforce that intent

Use Case: Securing RIC
In Non-Realtime Intelligent Controller, multiple vendors may be performing specialized task. Chance of whole platform compromise. Container/pod isolation would assist in limiting compromisation. If framework allows, identifying issues early in the lifecycle (change in app code which would result in clear security gap- should be highlighted in CI/CD) - how do you secure problems already in pipeline?

Static vs. admission vs. runtime security
Takes time for tooling to mature
How to check whether workload satisfies benchmarks prior to deployment
How to ensure security against exploits once deployed

KubeArmor Runtime Security:
Observability to application actions (contains module to understand workload actions)
Preventing attacks: Linux Security Modules (LSMs) for policy enforcement and remediation; Kubearmor strives to solve LSM userability in containerized/orchestrated workloads

Inline Mitigation vs Post-Attack Mitigation:
Multiple approaches for runtime security; most existing tooling concentrates on understanding events in kernel space; if malicious, will take action.
Intention of KubeArmor is observability events of app behavior; passed on as a policy.

KubeArmor: Abstracting LSMs
Makes LSMs easier to consume
Provides consistent alerting
Will be converted to apparmor;selinux;bpf-lsm. Handles consistent alerting.

Use-Cases: Continuous Compliance, Network Segmentation:
Workload hardening; multiple policy templates (MITRE ATT&CKm NIST, CIS etc)
Network segmentation; visibility into network handling of containers/pods

Use-case: Zero Trust Policies:
Zero trust policies allow specific behavior and deny/audit untrusted behavior (process whitelisting (volume mount point etc)

Hildegard attack: k8s based TTPs:
Rahul provided a comprehensive overview of the Hildegard attack and KubeArmor protective stances. When working with open horizon, need to use KubeArmour on arm platform. Deploys as a daemonset, operates across any kubernetes provider or on prem; supposed CRIs (docker, containerd, crio)
Sundar: how to go to binary level within container? Rahul: can specify apparmor policy natively. even after apparmor policy in place, may change in a few weeks (change management is issue). Sundar: how to translate binary name to apparmour level? Rahul: can specify to apparmor. Can essentially insert byte code to match certain policy.

5G security Work in progress context to KubeArmor
Intent to secure control plane; work from D&TF conf - 5G SBP; LF Edge Open Horizon POC

Phil Porras discussed white paper (5G security-enhanced radio access network)
Project SE-RAN: an ORAN compliant 5G native platform

John Belamaric: come talk to SIG1/2 after R1; number of ways in which this can integrate (may fall into best practices of building workload packages)

Kandan Kathirvel (KK) adjourned the meeting at 11:02am PT.