Sachbericht zum Verwendungsnachweis
Teil I
2024

Verbundvorhaben

5G-FORAN

5G-FORAN - IT-Forensik und Behandlung von IT-Sicherheitsvorfällen im Open RAN

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Konsortialführung: **PROCYDE GmbH** Wiesenstraße 2 57539 Breitscheidt	Förderkennzeichen: **01MO23020A**
Laufzeit des Vorhabens: von: **01.01.2023** bis: **31.12.2024**	
Berichtszeitraum: von**: 01.01.2023** bis: **31.12.2024**	Datum: **17.04.2025**

Projektpartner:

1. PROCYDE GmbH
2. TH Köln

Teil I:

Kurzbericht (max. 2 Seiten)

Im Rahmen des Verbundvorhabens 5G-FORAN ist eine Methode entwickelt, konzipiert und praktisch simuliert worden, wie IT-Sicherheitsvorfälle im Bereich Open RAN analysiert, behandelt und behoben werden können. Grundlage für diese Entwicklung sollten nachvollziehbare Angriffsspuren auf den Komponenten bilden, die ebenfalls im Rahmen dieses Gesamtvorhabens durch eine Angriffssimulation zu berücksichtigen sind. Das Gesamtvorhaben wurde in zwei Teilprojekte untergliedert:

1. **5G-FORAN-ATTACK** „Aktive Angriffssimulation (Offensive Attack) auf Open RAN Komponenten“ (Teilvorhaben durch TH Köln verantwortet)
2. **5G-FORAN-DFIR** „Digital Forensics und Incident Response (DFIR) im Open RAN“ (Teilvorhaben durch PROCYDE GmbH verantwortet)

Es wurden geeignete Open RAN Implementierungen identifiziert und im Ergebnis die Referenzimplementierung der O-RAN Software Community (SC) ausgewählt. Zum einen verfolgt die O-RAN SC mit der Referenzimplementierung das Ziel sich an die offene Architektur und die vorhandenen Spezifikationen der O-RAN Alliance zu halten, zum anderen sind große RAN-/ und Technologie-Hersteller in der Community und O-RAN Alliance vertreten, was die Wiederverwendung von Bausteinen in kommerziellen Produkten wahrscheinlich macht.

Die Referenzimplementierung der SC ist in kontinuierlicher Weiterentwicklung. Teilweise sind O-RAN Funktionen, die in den Spezifikationen beschrieben sind, unvollständig implementiert oder erst für zukünftige Releases vorgesehen. Aufgrund des noch geringen Reifegrads waren Skripte zur Implementierung anzupassen und interne Funktionen zu rekonstruieren, um ein Deployment und eine rudimentäre Interoperabilität zu gewährleisten. Im Projekt wurde auf das G-Release (2022) und das I-Release (2023) der Software Community zurückgegriffen.

Die O-RAN SC Referenzimplementierung basiert auf Container-basierten Microservices. Mit Kubernetes als de-facto Standard für die Orchestrierung von Container-Lösungen in Kommunikationsnetzen bietet sich eine erweiterte Angriffsflächen im Vergleich zu monolithischen, proprietären Softwarelösungen. Die Evaluation der Angriffssimulation fokussiert auf eine detaillierte Analyse der in der O-RAN SC Referenzimplementierung eingesetzten Infrastruktur- und Softwarekomponenten und der Auswertung wissenschaftlicher Studien zur Bedrohungslage. Eine der Haupterkenntnisse ist die potentielle Bedrohung durch interne Angreifer, weshalb Angriffe von legitimen Nutzern mit Privilegien und Zugang zu Teilen der Infrastruktur bis hin zu Administratoren des RAN-Betreibers priorisiert behandelt werden. Die Angriffsanalyse ergibt zudem, dass Virtualisierung, Containerisierung und Orchestrierung der Infrastruktur den Großteil der Angriffsfläche darstellt. Es wird auf bekannte Angriffsdatenbanken und Frameworks wie MITRE ATT&CK zurückgegriffen. Details zu den Ergebnissen der Analyse sind der Veröffentlichung “Open RAN Threat Analysis of the O-RAN SC Reference Implementation“ zu entnehmen[1].

Für die digitale Forensik und die Reaktionsmöglichkeiten auf IT-Sicherheitsvorfälle ist, als ein Ergebnis der Evaluationsphase, ein Infrastruktur-naher Ansatz vorteilhaft. Isolierte Maßnahmen, die ausschließlich auf der O-RAN Applikationsschicht anzusiedeln sind (z.B. auf Basis dedizierter xApps oder rApps), zeigen für die Forensik und Reaktionsfähigkeit Schwächen, da Angriffsvektoren auf der Infrastruktur-Ebene unberücksichtigt bleiben.

Innerhalb der digitalen Forensik sind die Identifizierung, Sicherung, Sammlung und Analyse von Beweismaterial relevant. Neben den Applikations-Logs der O-RAN Microservices, sind

[1] H. Wittemeier, A.J. Dieterich, T. Karl, A. Grebe: „Open RAN Threat Analysis of the O-RAN SC Reference Implementation“, in Cologne Contributions to Computer Engineering, 2024, ISSN 2193-570X

Security- und Infrastruktur-Logs ebenso von Interesse, wie Ereignisse auf den Kubernetes-Knoten selbst. Diese Logs werden zentralisiert in einer abgesicherten Umgebung vorgehalten, um anschließend Ereignisse korrelieren und auswerten zu können. Daneben zeigt sich während der Evaluierung, dass der „extended Berkeley Packet Filter“ (eBPF) eine äußerst hilfreiche Technologie bietet, um Sichtbarkeit von sicherheitsrelevanten Ereignissen in Open RAN Implementierungen zu schaffen, ohne O-RAN Microservices zu beeinflussen. Bei gegebenem Anfangsverdacht lässt sich über das kürzlich veröffentlichte „Forensic Container Checkpointing“[2] in Kubernetes eine zustandsorientierte Kopie eines O-RAN Microservices erstellen und anschließend offline forensisch analysieren. Zur Eindämmung eines Sicherheitsvorfalls wurde auf Isolationsmechanismen der Container-Runtime zurückgegriffen, sowie auf die automatische Löschung von infizierten O-RAN Microservices (z.B. maliziöse xApp). Weitere Details sind der Veröffentlichung “Digital Forensics and Incident Response (DFIR) in O-RAN Implementations” zu entnehmen[3].

Bei der Realisierung der O-RAN Referenzimplementierung, der 5G-FORAN-DFIR- und 5G-FORAN-ATTACK-Komponenten, ist die nahtlose Integration in eine Kubernetes-basierte Infrastruktur, unter Verwendung von DevOps-Prinzipien, berücksichtigt. Basierend auf der Schwachstellenanalyse wurde das Angriffstool „ClusterForce“ entwickelt, das Open Source Angriffstools mit unterschiedlicher Zielsetzung integriert (z.B. kdigger für Kubernetes-Discovery oder Flightsim zur Erzeugung von maliziösem Netzwerkverkehr) und über eine Implementierung der Angriffe aus der Microsoft Kubernetes Threat Matrix verfügt. Es werden Angriffsszenarien simuliert, Angriffsabläufe automatisiert und Metadaten der Angriffe persistent gespeichert. Das Angriffstool ist modular erweiterbar, bietet eine Visualisierung mittels Dashboard zur detaillierten Analyse der Metadaten und implementiert eine Korrelation zu bekannten Angriffsframeworks. Als eigenständiges O-RAN-spezifisches Angriffstool kommt eine neu entwickelte Near-RT-RIC xApp zum Einsatz. Dort sind zum einen Angriffstechniken in die Go-basierte Anwendung eingebettet, zum anderen bietet eine Integration mit der Angriffssimulationsplattform Caldera vielfältige Möglichkeiten, Angriffsoperationen durchzuführen und auf Angriffstechniken von MITRE zurückzugreifen.

Für DFIR ergibt sich eine Aufteilung in zwei Applikationsbausteine. Zum einen die Entwicklung einer Applikation, die auf den Open RAN Kubernetes-Clustern ausgeführt wird und dort sowohl relevante Artefakte einsammelt und aufbereitet als auch Gegenmaßnahmen zur Eindämmung und Beseitigung von Angriffen einleitet. Zum anderen wurde eine zentrale Instanz entwickelt, die der Vorhaltung und Auswertung von forensischen Artefakten dient. Details zum Tool-Stack, dem Aufbau und der genauen Funktionsweise sind den Repositories[4] zu entnehmen.

Die Integration der beiden Teilprojekte 5G-FORAN-ATTACK und 5G-FORAN-DFIR erlaubt die Automatisierung aller Deployments in eine durch Kubernetes gemanagte Open RAN Referenzumgebung. Diverse Tests zur Simulation von Angriffen und Beobachtung mit Hilfe der eingesetzten DFIR-Tools zeigen die Möglichkeiten und Grenzen der Nachvollziehbarkeit der simulierten Angriffe. Voraussetzung ist eine Feinjustierung („Baselining“) der eingesetzten ATTACK- und DFIR-Tools für spezifische Open RAN-Implementierungen (Releases).

---

[2] Vgl.: https://github.com/kubernetes/enhancements/tree/master/keps/sig-node/2008-forensic-container-checkpointing

[3] H. Wittemeier, T. Karl, A.J. Dieterich, A. Grebe: „Digital Forensics and Incident Response (DFIR) in O-RAN Implementations“, Mobile Communication - Technologies and Applications; 28th ITG-Symposium, Osnabrück, VDE Verlag, 2024, ISBN 978-3-8007-6382-5

[4] Siehe https://codeberg.org/PROCYDE/5g-foran-dfir und https://codeberg.org/PROCYDE/charts