Some/IP Intrusion Detection System

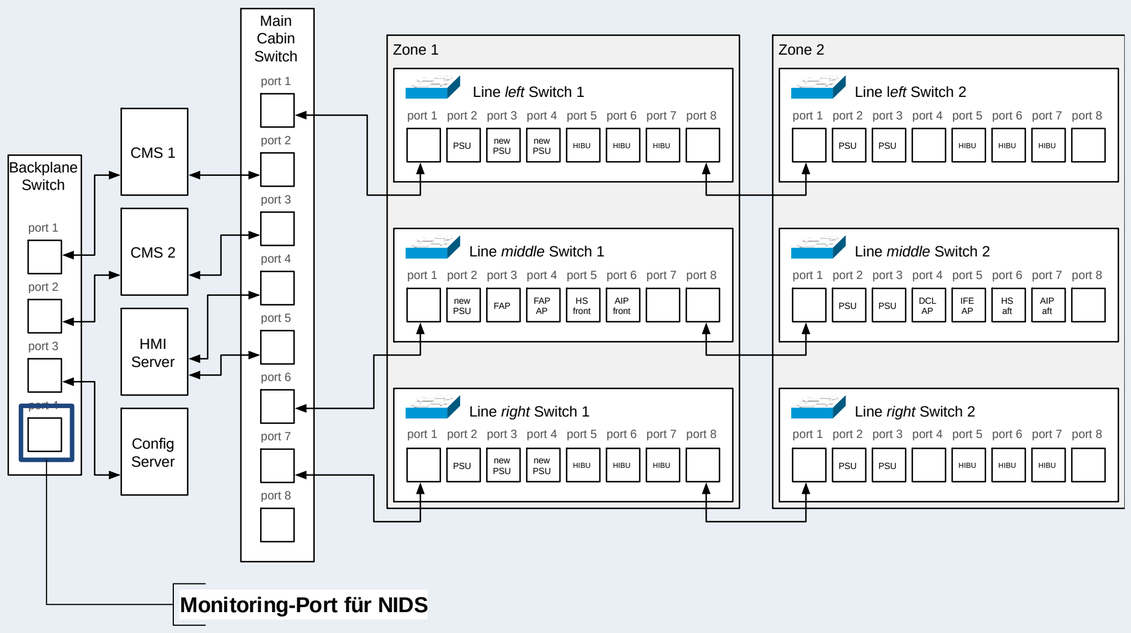
SURF – Systemic Security for Critical Infrastructures

Abschlussmeeting und Demoday für das Projekt SURF
08.12.2016, Infineon Technologies AG, Am Campeon 1-12, Neubiberg

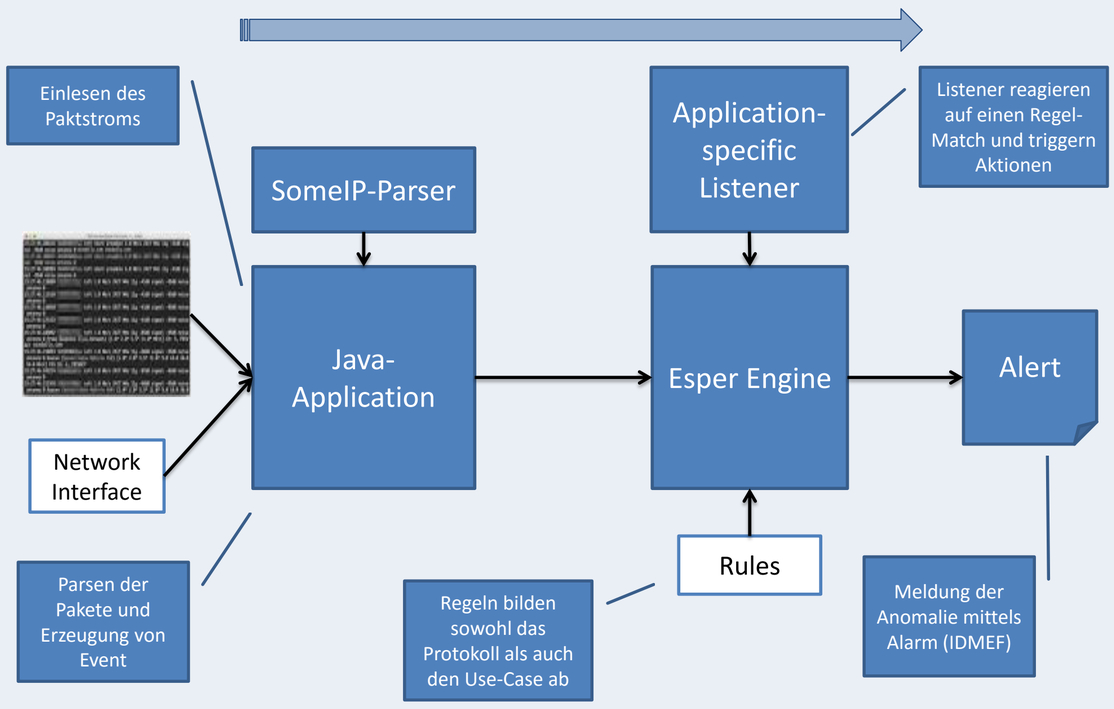
Some/IP-IDS - Übersicht

- Netzwerkbasiertes Anomalieerkennungssystem
- Regeln bilden das Soll-Verhalten der Komponenten ab.
- Grundlage für diese Regeln ist der Some/IP Standard.
- Verwendung von Complex-Event-Processing (CEP) zur Prüfung des Paketstroms.
- Implementierung mittels der CEP-Engine Esper und EPL (Event Processing Language) für die Regeldefinition.

Anwendungsfall – Kabinennetz der AGI



Some/IP-IDS – Architektur



Some/IP-Protokoll – Angriffsanalyse

„Malformed Packets“ beschreiben Pakete deren Struktur nicht dem Standard entspricht, d.h. beispielsweise können einzelne Headerfelder oder auch Kombinationen nicht korrekt sein. Hierbei muss nur ein einzelnes Paket betrachtet werden.

Protokollverletzungen sind alle Abweichungen vom standardisierten Verhalten bezüglich der Kommunikation zwischen Geräten. Hierbei müssen mehrere Pakete zusammen betrachtet werden.

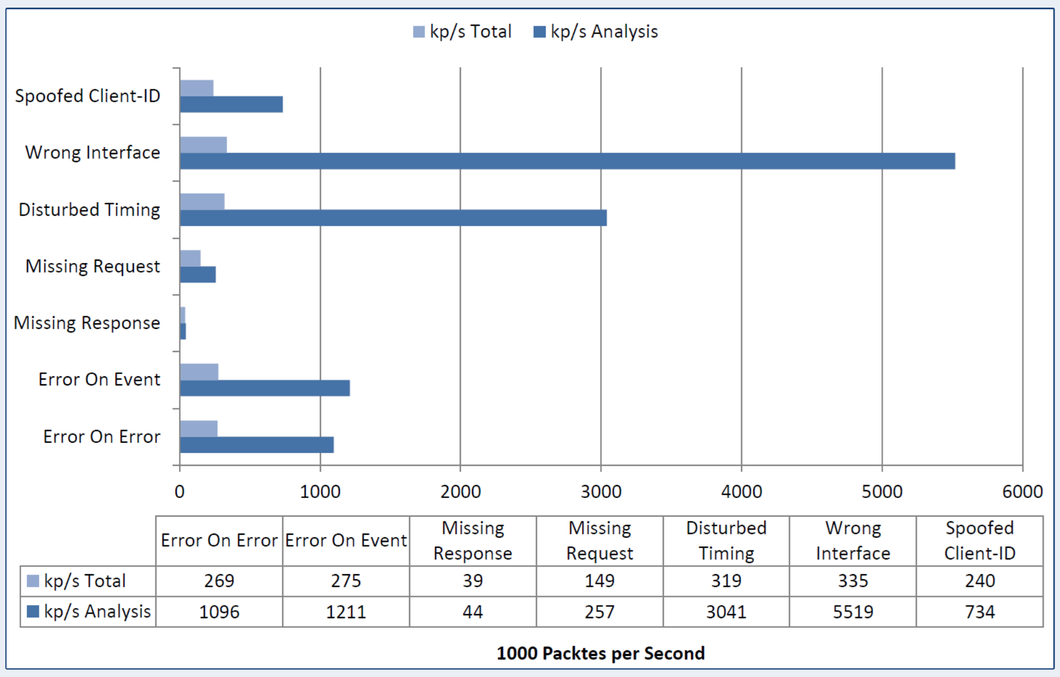
System-Spezifische Verletzungen beschreiben alle zusätzlichen Einschränkungen, die durch einen spezifischen Anwendungsfall vorgegeben werden.

Zeitbasierte Probleme sind meist eine Sonderform der system-spezifischen Verletzungen und beschreiben meist Abweichungen von erwarteten Intervallen für den Eingang von Paketen

EPL-Regel – Fehlermeldung auf Fehler

```
SELECT *
FROM SomeIPPacket(type=ERROR).win:length(1) s1
WHERE NOT EXISTS
       (SELECT *
       FROM SomeIPPacket(type=REQUEST OR type=NOTIFICATION
            OR type=REQUEST_NO_RETURN).win:length(100) s2
              WHERE s1.serviceID = s2.serviceID
              AND s1.methodID = s2.methodID
              AND s1.request ID = s2.request ID
              AND s1.srcIP = s2.dstIP
              AND s1.dst IP = s2.srcIP
              AND s1.srcMAC = s2.dstMAC
              AND s1.dstMAC = s2.srcMAC
              AND s1.srcPor t = s2.dstPor t
              AND s1.dstPor t = s2.srcPor t
              AND s1.timestamp > s2.timestamp
              AND s2.timestamp < s1.timestamp + d )
```

Evaluation



	Error On Error	Error On Event	Missing Response	Missing Request	Disturbed Timing	Wrong Interface	Spoofed Client-ID
kp/s Total	269	275	39	149	319	335	240
kp/s Analysis	1096	1211	44	257	3041	5519	734

1000 Packtes per Second

Projekteckdaten

Gefördert vom BmBF

Bundesministerium für Bildung und Forschung

Laufzeit 09/2014 – 08/2016 (12/2016)

Bereich IT-Sicherheit – Kritische Infrastrukturen

Ziel Entwicklung einer Ganzheitlichen Lösung zur Verbesserung der Schutzsysteme für KRITIS

Weitere Informationen

GitHub:
https://github.com/Egomania/Some/IP_Generator
https://github.com/Egomania/Some/IP_Analyzer

Veröffentlichung:
N. Herold, S. A. Posselt, O. Hanka and G. Carle, "Anomaly Detection for SOME/IP Using Complex Event Processing," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, 2016, pp. 1221-1226.

Kontaktinformationen – TUM

Webseite https://www.net.in.tum.de/html/surf/

Verbundkoordination Infineon Technologies AG

Kontaktadressen – TUM

Prof. Dr.-Ing. Georg Carle
+49 89 289 18030
carle@Net.in.tum.de

Dr. Holger Kinkelin
+49 89 289 18006
kinkelin@net.in.tum.de