Kollaborative, Blackboard-basierte Verarbeitung von Netzwerk-Angriffen

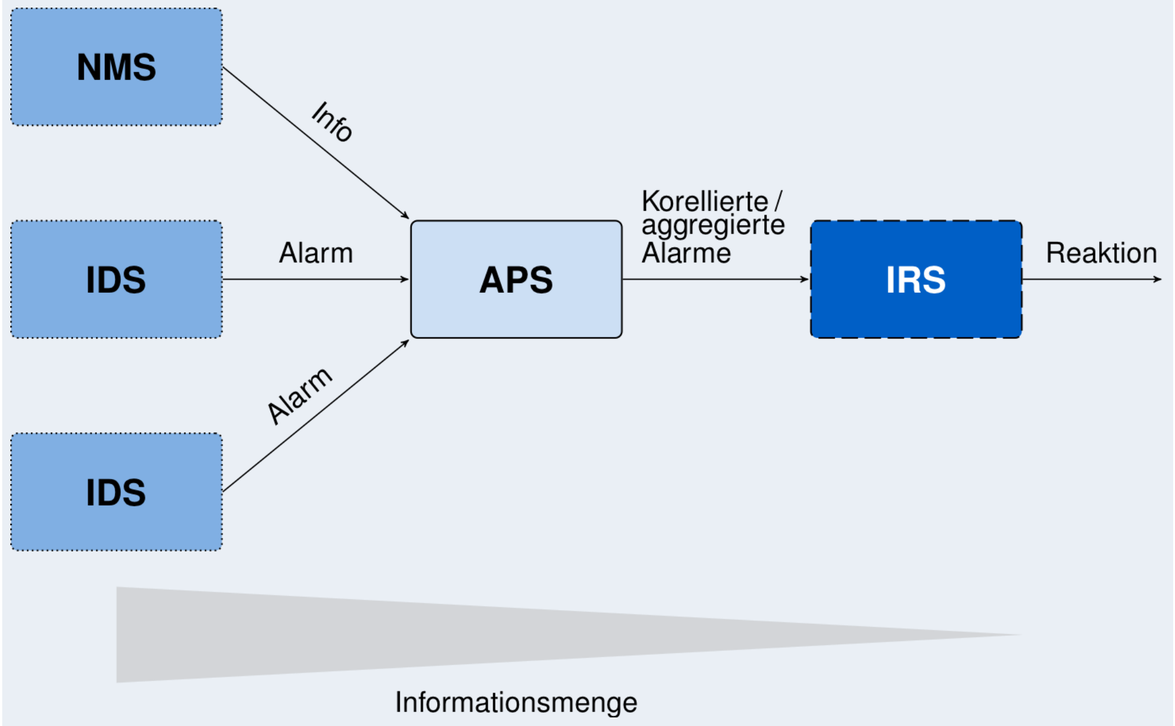
Typische Intrustion-Handling-Schritte

1) Informationsgewinnung durch
   - Netzwerk-Monitoring-Systeme (NMS): sammeln Informationen über Topologie, Infrastruktur, etc.
   - Intrusion-Detection-Systeme (IDS): lösen bei erkannten Sicherheitsvorfälle Alarme aus

2) Vorverarbeitung von Alarmen und Informationen durch Alert-Processing-Systeme (APS)

3) Automatische Ausführung von geeigneten Gegenreaktionen durch Intrusion-Response-Systeme (IRS)

Nachteile sequentieller Verarbeitung



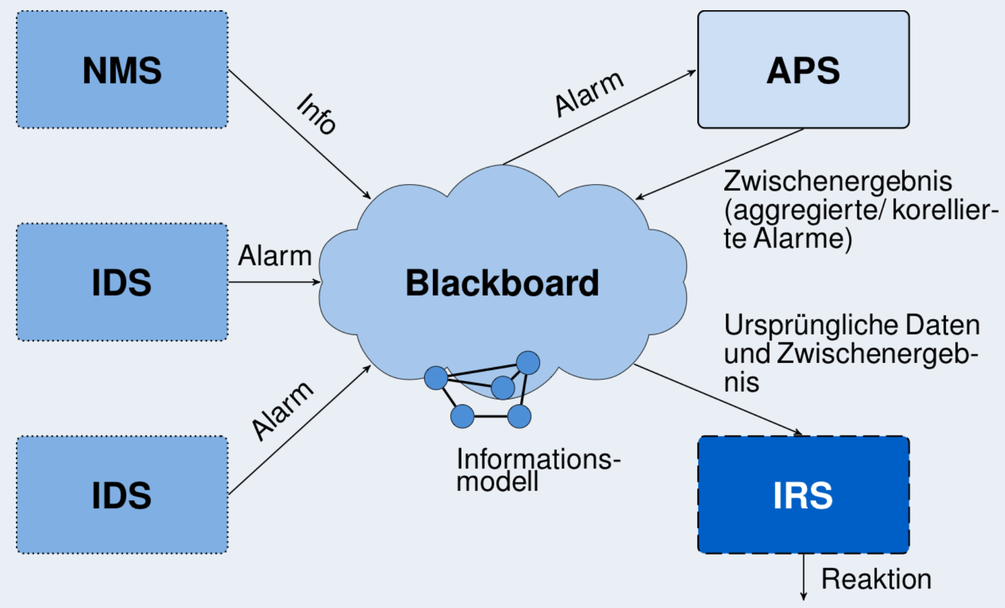
Probleme und Ziele

Informationsverlust bei sequentieller Verarbeitung:
- APS aggregieren/korrelieren Alarme und Informationen → Ursprüngliche Informationen gehen verloren
- Es gibt keine Möglichkeit Informationen über Komponenten hinweg zu teilen

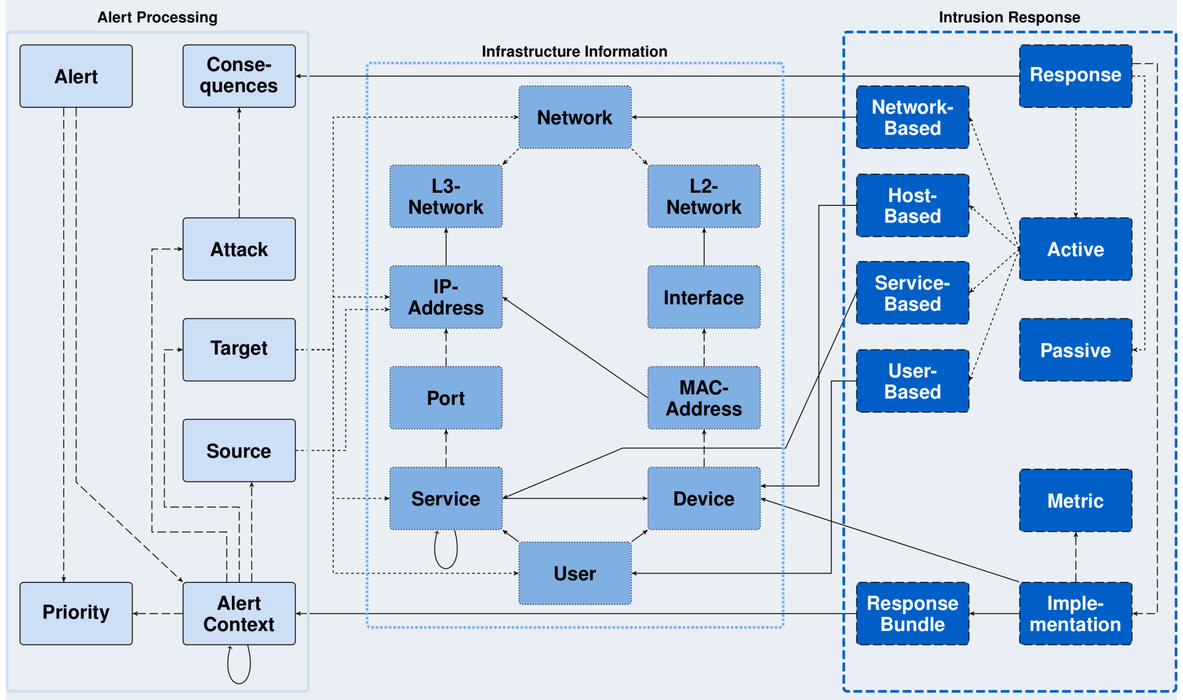
Problem: IRSe benötigen aber oftmals diese Informationen, um korrekte und wirksame Gegenreaktionen bestimmen und auslösen zu können.

Ziel: Entwicklung eines gemeinsam nutzbaren Informationsspeichers

Kollaborative Angriffsverarbeitung



Informationsmodell des Blackboards



Ausblick

Informationen im Blackboard müssen geschützt werden:
- Einschleusen gefälschter Informationen löst unerwünschte Gegenreaktion aus.
- Angreifer können Daten aus Blackboard zur Vorbereitung von Angriffen nutzen
- Daten im Blackboard sind teilweise personenbezogen

Lösungsmöglichkeiten
- Authentisierung aller Module
- Verschlüsselung aller Informationskanäle
- Zugriffskontrolle gemäß dem Minimalitätsprinzip

SURF und DecADe werden gefördert vom

Bundesministerium für Bildung und Forschung

Weitere Informationen

SURF:
- https://www.net.in.tum.de/html/surf/

DecADe:
- https://www.net.in.tum.de/sites/decade/

Veröffentlichung:
- N. Herold, H.Kinkelin, G. Carle “Collaborative Incident Handling Based on the Blackboard-Pattern,” in Proc. of the 3rd ACM Workshop on Information Sharing and Collaborative Security, Vienna, Austria, 2016.

Kontakt

Dr. Holger Kinkelin, Prof. Dr.-Ing. Georg Carle
<lastname>@net.in.tum.de

Technische Universität München
Lehrstuhl für Netzwerkarchitekturen und Dienste
Boltzmann Str. 3
85748 Garching