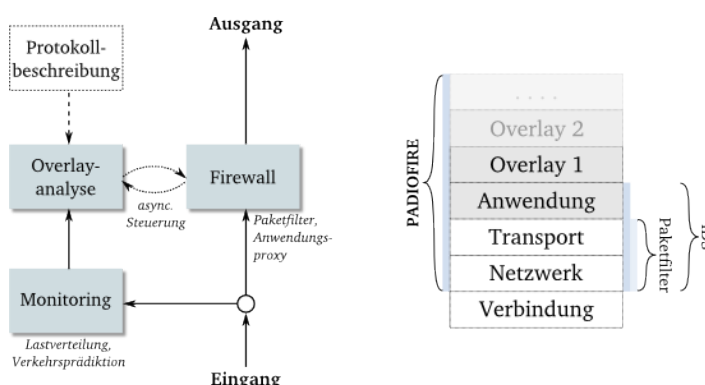


Master's Thesis

Monitoring Support for Efficient Web2.0 and Overlay Network Detection

Beschreibung:

Ziel des Projekts PADIOFIRE ist es, ein neuartiges Firewallsystem zu entwickeln, welches eine semantische Analyse von mehrfach geschichteten Anwendungsprotokollen am Beispiel von Web 2.0-Diensten durchführen kann. Die Ergebnisse der Analyse stellen die Grundlage für die Entscheidung dar, ob zugehörige Datenströme weitergeleitet oder verworfen werden. Konkret ist es geplant, ein Intrusion Detection System (IDS) als Basis zu nutzen, welches auf die Erkennung von bestimmten Strukturen, vorrangig Angriffen, im Netzwerkverkehr spezialisiert ist und somit gut geeignet für die Anwendungs- und Protokollerkennung ist. Da aktuelle IDS-Ansätze nicht auf die semantische Analyse von Overlaystrukturen spezialisiert sind, welche für eine genaue Analyse auf Anwendungsebene nötig ist, soll eine neuartige Regelsprache entwickelt werden, welche mehrfach geschichtete Anwendungsprotokolle detailliert analysiert. Die semantische Analyse von Anwendungsdaten ist sehr aufwändig, daher sind architektonische Optimierungen geplant. Zum einen spielt die verteilte Analyse auf mehreren Prozessorkernen eine essentielle Rolle und zum anderen ist die Entwicklung einer losen Kopplung von Analyse und Firewall geplant.



Aufgabenstellung:

Im Rahmen der Arbeit soll eine dynamische Erkennung von Web 2.0 Anwendungen am Beispiel von Google Maps realisiert werden. Vermont soll so erweitert werden, dass nicht nur Flows auf Transportebene, sondern auf Anwendungsebene unter Berücksichtigung der Web 2.0 Erkennung erkannt und statistisch ausgewertet werden können. Ebenfalls ist das IPFIX Protokoll so zu erweitern, dass neue Floweigenschaften für Web 2.0 Flows exportiert und weiterverarbeitet werden können. Abschließend soll eine umfangreiche Experimentserie zur Bewertung der erreichten Leistungsfähigkeit durchgeführt werden.

Vorraussetzungen:

Grundkenntnisse von Datennetzen, speziell IP, und Statistik sind wünschenswert

Ansprechpartner:

Falko Dressler <falko.dressler@uibk.ac.at>