Technische Universität München
Lehrstuhl für Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

21.07.2009

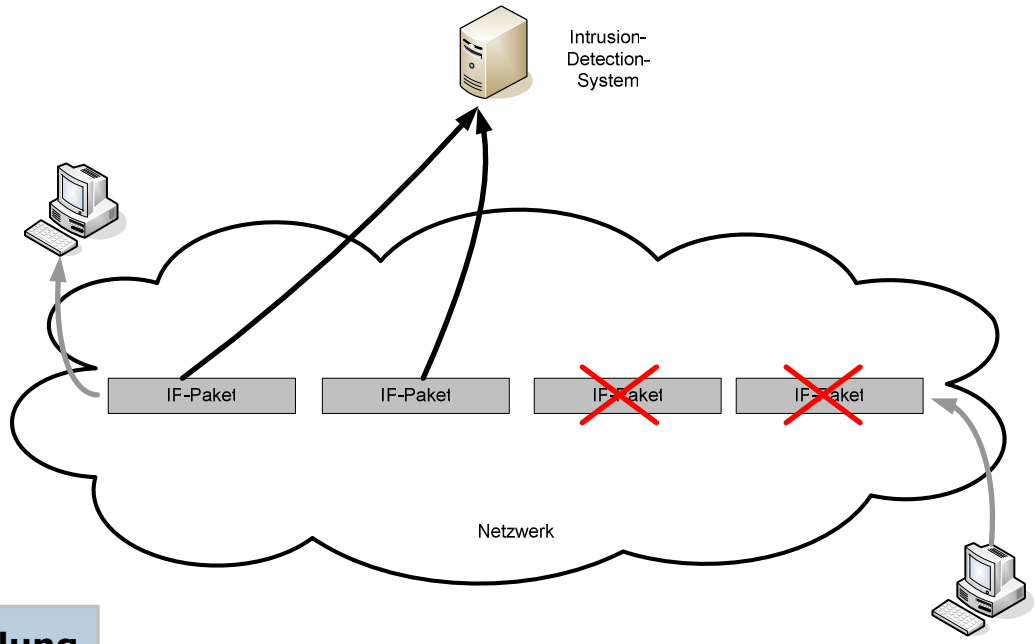
Diplom-/ Bachelor-/ Masterarbeit/SEP

Performance-Optimierung von Intrusion-Detection-Systemen durch Paket-Sampling

Beschreibung

Intrusion-Detection-Systeme wie *Snort* oder *Bro* untersuchen den Netzwerkverkehr auf Angriffe und unerwünschte Pakete. In Netzwerken mit hohem Verkehrsaufkommen können solche Intrusion-Detection-Systeme an die Grenzen ihrer Verarbeitungskapazität kommen. Abhängig von der vorhanden Hardware treten dann zufällige Paketverluste auf.

Reicht die Verarbeitungskapazität nicht aus um den gesamten Verkehr zu untersuchen, muss die vorhandene Rechenleistung auf einen kleinen Teil des Verkehrs konzentriert werden, der wichtige Informationen enthält.



Aufgabenstellung

In einer früheren Diplomarbeit wurde ein Sampling-Verfahren entwickelt, welches die ersten *N* Bytes jeder beobachteten TCP-Verbindung auswählt. Es konnte gezeigt werden, dass diese ersten *N* Bytes ausreichend sind um Würmer und Bots zu erkennen.

Das Verfahren soll nun so erweitert werden, dass es auch UDP-Verkehr behandeln und *N* anhand der Systemauslastung dynamisch wählen kann. Außerdem soll untersucht werden, ob neben Bots und Würmern auch andere Arten von Angriffen in den ersten Bytes einer Verbindung gefunden werden können.

Der Umfang der Arbeit richtet sich nach dem Typ (BA/SEP oder MA/DA).

Infos & Kontakt

Lothar Braun <braun@net.in.tum.de> Tel.: 289-18010