

Vortrag Nr. 4

Donnerstag, 22. November 2007, 10.00 Uhr

Hörsaal AH 2, 52074 Aachen

Referentin: Dr. Tanja Zseby, FOKUS Berlin

Die Bedeutung passiver Messverfahren für die Sicherheit in Kommunikationsnetzen

Anomalien im Netzwerkverkehr sind häufig ein Indiz für Netzwerkangriffe in festen und mobilen Netzen. Anomalie-Erkennungsverfahren können im Gegensatz zu signaturbasierten Verfahren auch neuartige unbekannte Angriffe entdecken. Dafür ist es wichtig, über passive Messverfahren gezielt und effizient die nötigen Informationen bereitzustellen. Die hohe Dynamik von Netzwerkverkehrsmustern führt jedoch zu einem sehr variablen Ressourcenverbrauch, der unkontrollierten Datenverlust zu Folge haben kann. Eine kontrollierte Datenselektion und die Adaptation von Messparametern an die Netzwerksituation können dem entgegenwirken. Um Daten von verschiedenen Beobachtungspunkten aufeinander beziehen zu können, müssen zudem die Messprozesse und die Datenauswahl an den Beobachtungspunkten synchronisiert werden.

In dem Vortrag werde ich Herausforderungen und Lösungsansätze für den Einsatz von passiven Messverfahren zur Anomalie-Erkennung vorstellen.