



Kolloquium des Graduiertenkollegs „Mathematische und ingenieurwissenschaftliche Methoden der sicheren Datenübertragung“

17. Juni, 15.00 Uhr

FernUniversität in Hagen, Universitätsstr. 11, 58084 Hagen
Raum C 12, 3. Etage im TGZ

"Virtuelle Poststelle, eine zentrale Security Plattform"

Prof. Dr.-Ing. Norbert Pohlmann (Lehrgebiet Verteilte Systeme und Informationssicherheit, FH Gelsenkirchen)

Zusammenfassung:

Trotz vielfältiger Möglichkeiten den Mailverkehr im Internet mitzulesen, sind heutzutage immer noch weniger als 5% aller E-Mails verschlüsselt. Doch kaum eine andere Internetanwendung erfreut sich einer vergleichbaren Akzeptanz und Verbreitung, ungeachtet der mangelhaften Sicherheit. Nicht ohne Grund steht das Thema E-Mail-Sicherheit deshalb ganz oben auf der To-do-Liste vieler Unternehmen. E-Mails haben in vielen Bereichen die traditionelle Kommunikation per Telefon, Brief oder Fax abgelöst. Bis auf wenige isolierte PGP- und S/MIME-Inseln, gibt es in der Praxis kaum fundierte Konzepte für unternehmensweite und –übergreifende E-Mail Sicherheitslösungen. Die Ursache für die zögerliche Umsetzung sind die hohen Kosten für die Infrastruktur durch Clientsoftware, Token, Lesegeräte, Rollout, Helpdesk, Migration und Zertifikatsmanagement. Die "Virtuelle Poststelle" stellt eine neuartige, pragmatische Lösung zur Sicherung des kompletten E-Mail-Verkehrs bereit. Aufgrund des zentralen Ansatzes ist diese den herkömmlichen End-to-End-Lösungen hinsichtlich Kosten und Leistungsfähigkeit weit überlegen. Als Erweiterung der bereits genutzten E-Mail-Server sorgt die "Virtuelle Poststelle" für die Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur) des gesamten E-Mail-Verkehrs.

„Intrusion Detection - Einführung und Überblick“

Dipl.-Ing Alex Esoh (Fachgebiet Kommunikationstechnik, Fernuniversität Hagen)

Zusammenfassung:

Zur Entdeckung von Angriffen auf Informationssysteme werden im allgemeinen zwei grundlegende Methoden eingesetzt: Anomalie-Erkennung (Anomaly Detection) und Missbrauchserkennung (Misuse Detection). Bei der Anomalie-Erkennung wird ein Profil der zu überwachenden Größe -beispielsweise der CPU Nutzung- erstellt (Langzeitverhalten) und mit der aktuellen Realisierung derselben (Kurzzeitverhalten) verglichen. Bei Überschreitung eines vorher festgelegten kritischen Wertes (Schwellwert) wird das gerade eingetretene Ereignis als Intrusion bewertet.

Bei der Missbrauchserkennung werden angriffsspezifische Signaturen erstellt, in einer Signaturdatenbank gespeichert, und es wird dann der zu überwachende Datenstrom genau nach diesen vorher schon bekannten spezifischen Angriffsmustern systematisch durchsucht.

In diesem Vortrag werden verschiedene Ansätze, die sowohl zur Einbruchs- als auch zur Missbrauchserkennung eingesetzt werden, erläutert. Hauptaugenmerk wird dabei auf den Einsatz statistischer Methoden zur Entdeckung von Anomalien gerichtet.