

EINLADUNG

Zeit: Mittwoch, 12. Juli 2006, 14.00 Uhr

Ort: AH 5, Ahornstr. 55

Referent: Dr. Dogan Kesdogan
RWTH Aachen

Titel: Vertraulichkeit in Kommunikationsnetzen

Abstract:

Vertraulichkeit ist eine der drei Grundsäulen der Informationssicherheit und unterscheidet sich fundamental von den beiden anderen Sicherheitszielen Integrität und Verfügbarkeit. Wenn Integrität und Verfügbarkeit als 'Korrektheit' beschrieben werden können, so hat Vertraulichkeit das Ziel, die Information geheim zu halten.

In der klassischen Sicherheitsforschung wird Vertraulichkeit üblicherweise mit Kryptographie gleichgesetzt. Mit dem überwältigenden Anstieg der vernetzten Rechner im alltäglichen Geschäfts- und Privatleben entstehen viele Möglichkeiten, Vertraulichkeit zu verletzen. Ein Angreifer, der das Netz abhört, kann Informationen über Geschäftsbeziehungen, interne Prozesse oder Benutzerverhalten und –vorlieben gewinnen, selbst wenn die kryptographischen Verfahren nicht gebrochen werden können. Neue Vertraulichkeitstechniken sollen in offenen Umgebungen (z.B. dem Internet) einen besseren Schutz liefern.

In dem Vortrag wird eine mathematische Modellierung der Vertraulichkeit vorgestellt, die sowohl eine Bewertung existierender Schutzverfahren als auch eine strukturierte Entwicklung von neuen Verfahren erlaubt.

Es laden ein: Die Dozenten der Informatik