

EINLADUNG

Zeit: Montag, 19. November.2007, 13.30 Uhr

Ort: AH 2, Ahornstr. 55

Referent: Prof. Dr.-Ing. Ulrich Greveler, Fachhochschule
Münster

Titel: Sicherheitsaspekte bei breitbandigen Internetzu-
gängen und Insider- Angriffen auf verschlüsselte
Übertragung

Abstract:

Drahtlose Datenübertragungen können i. a. nicht nur vom gewünschten Empfänger aufgefangen werden sondern von vielen weiteren Parteien, die sich in der Reichweite befinden. Auch bei einigen kabelgebundenen Technologien ist dies möglich, wenn die Leitungen für gebündelte Signale verwendet werden. Unverschlüsselte Übertragungen sensibler Daten stellen neben der offensichtlichen Gefährdung des Datenschutzes auch ein dem privaten Internetnutzer i. a. nicht bewusstes Sicherheitsproblem dar, da wichtige Protokolle in höheren Schichten implizit Vertraulichkeit bedingen.

Um Vertraulichkeit zu gewährleisten, ist starke Ende-zu-Ende- Verschlüsselung ein wirksamer Mechanismus. Die Grundannahme ist hierbei, dass beide Parteien sich korrekt verhalten, da sie ein gemeinsames Interesse haben, ihre Kommunikation wirksam abzusichern. Es gibt jedoch Fälle, bei denen diese Annahme nicht zutrifft und ein Kommunikationspartner (der Empfänger) die Vertraulichkeit zur Etablierung eines Broadcast-Kanals aufheben möchte, während der Sender (ein Netzbetreiber) das gegenteilige Interesse verfolgt. Der Empfänger agiert dann als Insider, der den Mechanismus, den der Sender bestimmt hat, im Interesse einer dritten Partei unwirksam werden lässt. Im Vortrag werden aktuelle Forschungsergebnisse für diese Angriffe dargestellt und mögliche Gegenmaßnahmen vorgeschlagen.

Es laden ein: Die Dozenten der Informatik