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

03. Februar 2005, 15.00 Uhr c. t.
FernUniversität in Hagen, Universitätsstr. 11, 58084 Hagen
Raum C 13, 3. Etage im TGZ

"A New Approach for Computation Result Protection in the Mobile agent paradigm"
Herr Suphithat Songsiri
Lehrgebiet Kommunikationssysteme
Fachbereich Elektrotechnik und Informationstechnik, FernUniversität in Hagen

Zusammenfassung:
One of the primary security challenges of the mobile agent paradigm is that of protecting the result of computation carried out by a mobile agent against an attack by a malicious host. There are various proposals that appeared in the literature. Beside their benefits, a well-known vulnerability of their technique is the collusion attack. The collusion attack mainly considered in this presentation is the two colluders truncation attack, which could be engendered by the leakage of a one time private key. We demonstrate the prevention of the two colluders truncation attack, the detection of other forms of collusion attacks, and the identification of the malicious host.

"Anonymität im World Wide Web"
Herr Dr. Thomas Demuth

Zusammenfassung:
Nach vorherrschender Meinung kann man sich im World Wide Web anonym bewegen, sofern man keine statische IP-Adresse nutzt, auf Web-Seiten keine persönlichen Daten hinterläßt, keine Cookies akzeptiert und Java und Javascript in seinem Web-Browser deaktiviert hat. Stimmt diese Annahme? Der Vortrag zeigt einen Angriff auf Nutzer des World Wide Web auf, der alleine auf den Protokollinformationen basiert, die bei jeder Kommunikation zwischen einem Web-Client und einem Web-Server ausgetauscht werden. Der Angriff basiert auf Methoden des Information Retrieval und kann in Echtzeit durchgeführt werden.