

15.01.2013

Einladung

Am Montag, 04.02.2013, 10:30 Uhr, Hörsaal M6

spricht

Dr. Pavel Laskov

über

*“Selbstlernende Systeme für die Erkennung von
neuartigen IT-Sicherheitsbedrohungen.”*

Die stetige Entwicklung von fortgeschrittenen Hacker-Angriffstechniken schürt ein wachsendes Interesse an der Anwendung von Datenanalyse-Methoden in der IT-Sicherheit. Nach Angaben von Antiviren-Herstellern werden täglich über 100,000 Beispiele von neuer Schadsoftware im freien Umlauf gesichtet. Automatische Analysetechniken sind daher unabdingbar, um aus dieser Datenflut wesentliche Merkmale von neuen Angriffen zu erkennen und neue Schutzmechanismen zu entwickeln. Eine weitere Herausforderung stellt die zunehmende Raffinesse der Angriffe. Die jüngsten Beispiele von professionell entwickelter Schadsoftware wie Stuxnet oder Flame zeigen, dass Sicherheitsinstrumente auch gegen vorher unbekannte Angriffe gewappnet werden müssen, um einen adequaten Schutz zu leisten.

Methoden des maschinellen Lernens stellen ein wirksames Werkzeug für die Abwehr von neuartigen Sicherheitsbedrohungen. Durch die automatische Erstellung von leistungsfähigen Entscheidungsmodellen ermöglichen Lernmethoden eine zeitnahe Anpassung von Sicherheitsinstrumenten. In diesem Vortrag werden die Grundbausteine für die Entwicklung von selbstlernenden Sicherheitssystemen vorgestellt und deren Anwendung auf konkreten Schutzmechanismen erläutert. Um den besonderen Anforderungen der IT-Sicherheit Rechnung zu tragen, wie z. B. die Notwendigkeit von Echtzeit-Entscheidungen oder Robustheit gegen manipulierte Daten, werden im Vortrag speziell entwickelte Lernalgorithmen vorgestellt. Als Ausblick werden offene methodischen Fragen sowie potentielle Anwendungen von sicheren Lerntechnologien erörtert.

Auf diesen Vortrag wird besonders hingewiesen

Martin Stein, Dekan