Herbsttagung 2013

der

MATHEMATISCHEN GESELLSCHAFT IN HAMBURG

GEGRÜNDET 1690

zusammen mit dem
Fachbereich Mathematik
der Universität Hamburg

Sicherheit im Internet

Freitag und Samstag, 25. und 26. Oktober 2013
Geomatikum, Hörsaal H2
Bundesstraße 55, 20146 Hamburg

Herbsttagung 2013

Sicherheit im Internet

Freitag, 25. Oktober 2013, Hörsaal H2 (Geomatikum)

16:00	Begrüßung und Einführung
16:15 – 17:15	Bernd Klauer: *Infizierbare Hardware*
17:15 – 17:40	Kaffeepause
17:40 –18:40	Constanze Kurz: *Unwanted Eavesdroppers – Die Überwachung des gesamten Netzverkehrs*
ab ca. 19:30	Nachsitzung im Hotel „Mövenpick“, Sternschanze 6, 20357 Hamburg. Für das Essen wird ein Unkostenbeitrag von EUR 30,00 erhoben. Um Anmeldung bis 18. Oktober 2013 wird gebeten.

Samstag, 26. Oktober 2013, Hörsaal H2 (Geomatikum)

10:00 – 11:00	Hannes Federrath: *Informationssicherheit und technischer Datenschutz durch verteilte Systeme*
11:00 – 11:30	Kaffeepause
11:30 – 12:30	Hubert Kiechle: *Mathematische Methoden zur Sicherung von Daten*

Bernd Klauer
Helmut-Schmidt-Universität Hamburg

Infizierbare Hardware

Die kommenden Hardware-Generationen werden von der Eigenschaft der Konfigurierbarkeit geprägt sein. Das bedeutet, dass die dabei verwendeten integrierten Schaltungen nach ihrer Fertigung auf der Logikebene noch veränderbar sind. Solche Schaltungen, die als FPGAs (Field Programmable Gate Arrays) bezeichnet werden, sind heute in einer Komplexität verfügbar, die die Darstellung von Mehrkernprozessoren in einem konfigurierbaren Logikbaustein ermöglicht.

Im Vortrag wird zunächst in die Historie und die Technologie der konfigurierbaren Logik eingeführt. Danach werden aus den zahlreichen Vorteilen in den Bereichen Performanz und Energieeffizienz die Risiken, die Veränderbarkeit von Hardware mit sich bringt, aufgezeigt und erörtert.

*****

Constanze Kurz
Hochschule für Technik und Wirtschaft, Berlin

Unwanted Eavesdroppers – Die Überwachung des gesamten Netzverkehrs

Die Snowden-Enthüllungen haben der Öffentlichkeit ein Ausmaß an heute verwendeten technischen Überwachungsmethoden gezeigt, das sich zuvor nur wenige vorstellen konnten. Es folgte eine wochenlange internationale Diskussion um Menschen- und Bürgerrechte im digitalen Zeitalter, um die Kontrolle der Kommunikationsüberwachung von NSA & Co und darüber, wie dem "Überwachungswahn" überhaupt noch Einhalt geboten werden könnte.
Der Vortrag wird nicht nur die wichtigsten Erkenntnisse des Abhörskandals zusammenfassen, sondern sich den Fragen zuwenden, die nach wie vor zu beantworten sind: Auf welchen Wegen werden die Daten im Internet von den Geheimdiensten abgegriffen? Und welche langfristigen Fragen sind zu stellen, wenn es um die Zukunft der Kommunikation und der Netze geht?

*****

Hannes Federrath
Universität Hamburg

Informationssicherheit und technischer Datenschutz durch verteilte Systeme

Als Schutzziele für die Sicherheit von informationstechnischen Systemen gelten seit mindestens 30 Jahren Vertraulichkeit, Integrität und Verfügbarkeit. Moderne Verfahren der Informationssicherheit sind – ebenso wie die Kommunikationssysteme selbst – heute meist als verteilte Systeme ausgestaltet. Verteiltheit bedeutet einerseits Mehrfachauslegung (Redundanz) von Systemteilen zur Verbesserung der Verfügbarkeit, aber auch Diversität (Verschiedenartigkeit der Herkünfte) zur Verbesserung der Sicherheit vor systematischen Fehlern, aber auch zum Schutz vor trojanischen Pferden (Schutz vor verdeckten Kanälen). Außerdem bieten kryptographische Bausteine wie das DC-Netz und Mix-Netz Möglichkeiten zum Schutz der Anonymität von Netzteilnehmern, die ohne Verteiltheit überhaupt nicht realisierbar sind.

*****

Hubert Kiechle
Universität Hamburg

Mathematische Methoden zur Sicherung von Daten

Daten, die über offene Kanäle (wie z.B. das Internet) ausgetauscht werden, sind verschiedenen Gefahren ausgesetzt. So können *zufällige* Störungen (wie der berühmte Blitzschlag) die Daten verfälschen oder gänzlich unbrauchbar machen. Diesem Problem begegnet die **Codierungstheorie**.

Die **Kryptologie** versucht gegen *gezielte* Zugriffe auf Daten zu schützen. Solche gezielten Zugriffe werden z.B. von Gangstern aber auch von Geheimdiensten durchgeführt. In beiden Gebieten spielen mathematische Methoden eine wichtige Rolle. Der Vortrag bietet einen kurzen Ausflug zu einigen dieser Methoden.

*****