

Beiträge zum Parlamentarischen Abend 2006

des Deutschen Verbandes Technisch-Wissenschaftlicher Vereine e.V. (DVT)

29. November 2006

Sicherheit in der Grundlagenforschung – Aktuelle Entwicklungen

Referent: Prof. Dr. Ernst W. Mayr, Vizepräsident der
Gesellschaft für Informatik e.V. (GI), Lehrstuhl für Effiziente Algorithmen
und Institut für Informatik, TU München

(Autorisierte Fassung vom 27.11.2006)

– Es gilt das gesprochene Wort –

Themen:

- 1.** Probleme mit den Grundlagen: alle bekannten digitalen kryptographischen Verfahren beruhen auf unbewiesenen (wenn auch offenbar recht verlässlichen) Annahmen. Es müssen weitere Verfahren gefunden werden, deren Sicherheit ggf. unconditionell gezeigt werden kann. Schwachstellen der bekannten Verfahren müssen untersucht und vermieden werden.
- 2.** Da sich die sicherheitsrelevanten Technologien und Algorithmen weiterentwickeln werden, ist ein modularer Aufbau sicherheitsrelevanter Systeme unerlässlich. Dies trifft auch aufgrund sich fortentwickelnder Sicherheitsanforderungen zu.
- 3.** Sicherheit in IT-Systemen ist ein umfassender Begriff, Sicherheit kann auch kompromittiert werden durch - unerlaubten physikalischen Zugang - unsichere Übertragungskanäle, Streustrahlung, usw. - zeitabhängige Phänomene. Wie weit kann "Sicherheit" als ein "abgeschlossenes" Problem betrachtet werden?
- 4.** Im Bereich des Datenschutzes ist es notwendig, Methoden und Algorithmen für flexible Zugriffs- und Verwendungsrechte zu entwickeln. Z.B. bei Grid-Computing ergeben sich hier harte Anforderungen.
- 5.** Grundlegende (im mathematischen oder informatischen Sinn) Konzepte müssen weiterentwickelt werden. Welche Rolle spielt dabei die Nichtkopierbarkeit von Objekten, insbesondere für die Entwicklung sicherer digitaler kryptographischer Systeme?