

DIPLOMARBEIT

Entwicklung eines sicheren, erweiterten E-Mail-Systems
Thomas Hildmann <hildmann@prz.tu-berlin.de>
Matr.Nr. 130931

Fachbereich Informatik
Institut fuer Kommunikations- und Softwaretechnik
Technische Universitaet Berlin
Prof. Dr.-Ing. Stefan Jaehnichen

ABSTRAKT

Der E-Mail-Dienst ist neben dem WWW der wichtigste Dienst im Internet. In ihrer klassischen Form ist die E-Mail jedoch nicht sicher und die Adressen sind sehr statisch. Es gibt verschiedene Produkte, die das Konzept der "sicheren E-Mail" umsetzen. Viele dieser Implementationen sind jedoch entweder auf bestimmte Plattformen beschaenkt, in ihrer Benutzung nicht ausreichend einfach, um grosse Akzeptanz zu finden oder bringen zumindest groessere Einschraenkungen bezueglich E-Mails an Gruppen von Empfaengern mit sich.

Ziel dieser Arbeit war der Entwurf und die prototypische Implementierung eines E-Mail-Systems, das E-Mails automatisch ver- und entschluesst, signiert und ueberprueft, ohne das vom Benutzer ein weitreichendes Wissen ueber Schluessel, deren Herkunft usw. gefordert wird. Die Absicherung erfolgt also voellig automatisch. Die Verwaltung von Schluesseln kann an eine zentrale Stelle der Organisation uebergeben werden.

Ferner zeigt die Arbeit, wie eine sichere E-Mail-Umgebung mit einem rollenbasierten Zugriffsmodell gekoppelt werden kann, um flexiblere Mailinglisten (Postverteiler) zu realisieren und die Modellierung einer Organisationsstruktur zur Grundlage einer E-Mailadressierung nutzen zu koennen.

Es werden auch Fragen behandelt, wie eine Virenueberpruefung in das System integriert werden koennte und wie eine Administration des Organisationsmodells ueber E-Mail aussehen koennte. Auch die Frage nach der Einbettung in bestehende Mail-Infrastrukturen wird diskutiert.