
Inhaltsverzeichnis

1	Einführung	1
2	Als offenes Netzwerk bietet das Internet Angreifern leichte Beute	3
3	Sicherheitsziele und Bedrohungen im Internet	5
4	Grundbegriffe der Kryptografie	9
5	Vertraulichkeit und Verschlüsselung	11
5.1	Symmetrische Verschlüsselungsverfahren mit geheimen Schlüsseln	11
5.2	Asymmetrische Verschlüsselungsverfahren mit öffentlichen Schlüsseln	15
5.3	Hybride Verschlüsselungsverfahren	16
6	Authentifikation	19
6.1	Passwort-basierte Authentifikation	19
6.2	Weitere Authentifikationsprotokolle und mögliche Angriffe	20
6.3	Sicheres Authentifikationsprotokoll	22
6.4	Man-in-the-Middle Attacke gegen Authentifikation mit asymmetrischer Verschlüsselung	24
7	Digitale Signaturen	27
7.1	Datenintegrität und Authentizität	27
7.2	Message Digest	30
7.3	Beispiele bekannter kryptografischer Hashfunktionen zur Erzeugung von Message Digests	32
7.4	Angriffe auf kryptografische Hashfunktionen	33

8	Public Key Infrastrukturen und Zertifikate	35
8.1	Schlüsselverteilzentrum (KDC)	36
8.2	Zertifizierungsstelle (CA) und digitale Zertifikate	37
8.3	Vertrauensmodelle	40
9	Glossar sicherheitstechnischer Begriffe	43

Sicherheit und Vertrauen im Internet

Eine technische Perspektive

Meinel, C.; Sack, H.

2014, VIII, 48 S. 15 Abb., Softcover

ISBN: 978-3-658-04833-4