Jörg Schwenk

Sicherheit und Kryptographie im Internet

Von sicherer E-Mail bis zu IP-Verschltisselung

vieweg

Inhaltsverzeichnis

1 Kryptographie im Internet ... 1
1.1 Was ist das „Internet" ... 1
1.2 Bedrohungen im Internet ... 4
1.3 Kryptographie ... 6
1.4 Symmetrische Kryptographie ... 6
1.5 Public-Key Kryptographie ... 12
1.6 Kryptographische Protokolle ... 18
1.7 Zertifikate ... 21
2 Datenverschlüsselung: PGP ... 28
2.1 PGP - Die Legende ... 29
2.2 PGP - Das Produkt ... 35
2.3 OpenPGP - Der Standard ... 42
2.4 PGP - Die Angriffe ... 47
2.5 Ausblick ... 55
3 Sichere E-Mail ... 56
3.1 E-Mail nach RFC 822 ... 56
3.2 Multipurpose Internet Mail Extensions (MIME) ... 57
3.3 Secure/MIME ... 60
3.4 PKCS #7 und CMS ... 70
3.5 PEM ... 75
3.6 PGP und OpenPGP ... 76
3.7 POP3 und IMAP ... 77
4 WWW-Sicherheit mit SSL ... 80
4.1 Das Hypertext Transfer Protocol (HTTP) ... 81
4.2 HTTP-Sicherheitsmechanismen ... 83
4.3 Erste Versuche: SSL 2.0 und PCT ... 87
4.4 SSL 3.0: Sicherheitsschicht über TCP ... 89
4.5 TLS: Der Internet-Sicherheitsstandard ... 101
4.6 Angriffe auf SSL ... 106
4.7 Praktische Aspekte ... 108
5 IP Security (IPSec) ... 112
5.1 Internet Protocol (IP) ... 112
5.2 Erste Ansätze: SKIP ... 114
5.3 IPSec: Überblick ... 116
5.4 IPSec Datenformate ... 120
5.5 IPSec: Schlüsselmanagament ... 126
5.6 Die Zukunft von IPSec ... 142
5.7 Praktische Aspekte ... 144
6 Multicast-Netzwerke ... 145
6.1 IPMulticast ... 145
6.2 IPSec und IP Multicast ... 147
6.3 Schlüsselvereinbarung für Gruppen ... 148
6.4 Multicast-Sicherheit im Internet ... 161
7 Link Layer-Sicherheit ... 162
7.1 PPP-Sicherheit ... 162
7.2 WirelessLAN ... 172
7.3 Mobilfunk ... 174
8 Neue Entwicklungen ... 180
8.1 Code-Signatur ... 180
8.2 Digital Rights Management ... 186
8.3 XML-Sicherheit ... 190
9 Literatur ... 198