

Stichwortverzeichnis IT-Sec WWW

3DES (Triple-DES)	67
AA (Attribute Authorities)	118
AAI (Authentication and Authorization Infrastructure)	139
Abstract Syntax Notation (ASN)	124
Active Content	163
Active Server Pages (ASP)	197, 212
ActiveX	182
additional layer effect	263
Advances Encryption Standard (AES)	67
AES (Advances Encryption Standard)	67
AH (Authentication Header)	87, 90, 91f
Alternative approaches and technologies	260
Anomaly detection	260
anonymity	220
Anonymizing HTTP proxy servers	229
Anonymous browsing	217, 229
Anonymous e-mail-forwarding	221
Anonymous publishing	230
Apache Web Server API	195, 206
API (Application Programming Interface)	195
Application layer security protocols	99
Application Layer	12
Application Level Gateway	53
Application Programming Interface (API)	195
Application Server	192
AS (Authentication Server)	142
ASN (Abstract Syntax Notation)	124
ASP (Active Server Pages)	197, 212
Asymmetric Cryptography	68
Attribute Authorities (AA)	118
Attribute Certificate	117, 146
Authentication and Authorization Infrastructure (AAI)	136, 139
Authentication Header (AH)	87, 90, 91f
Authentication Server (AS)	142
Authenticode (Microsoft)	165, 185
Authorization	138
Basic Authentication	31
Bastion Host	54
BBBOnline	232
Bellcore's Trusted Software Integrity System (BETSI)	165
BER	124
BETSI (Bellcore's Trusted Software Integrity System)	165
Binary Mail Attachment	166
BITS (Bump-in-the-stack)	97
BITW (Bump-in-the-wire)	97
blocking	249
Blowfish	67
British Central Computer and Telecommunications Agency (CCTA)	258
Browser	17
Bump-in-the-stack (BITS)	97
Bump-in-the-wire (BITW)	97
CA (Certification Authorities)	118, 129, n73
CAST-128	67
CCTA (British Central Computer and Telecommunications Agency)	258
CCTA Risk Analysis and Mgmt Methodology (CRAMM)	258
Censorship on the WWW	247
Central Computer and Telecommunications Agency (CCTA)	258
Certificate Management and Public Key Infrastructures	115
Certificate Repository	129
Certificate Revocation List (CRL)	131
Certificate Revocation	130

Certificate	116
Certificate-based authentication	39
Certificate-based credential systems	135
Certificate (verschiedene Arten)	132
Certificate for the WWW	132
Certification Authorities (CA)	118, 129, n73
Certification chain	127
Certification Path	127
CFS (Cryptographic File System)	99
CGI (Common Gateway Interface)	194, 198f
cgi-bin	203
ChangeCipherSpec	107
Chaum mixing network	221f, 229
Circuit Level Gateway	52
ClientKeyExchange	107
Client-side Scripting Language	173
Client-side Security	160
Collision Resistance	64
Collision Resistant Hash Function	64
COM (Component Object Model)	182
Common Gateway Interface (CGI)	194, 198f
completely trusted	n72
Component Object Model (COM)	182
Computational Security	63
Conclusions and Outlook	262
Configuring the browser	57
Content blocking	249
Content rating and self-determination	250
Content	241
Control Access	29
Cookies	224f
Copyrights	242
Corporate Signing Key (CSK)	n74
Countermeasure	20
CRAMM (CCTA Risk Analysis and Mgmt Methodology)	258
Credential System	135
CRL (Certificate Revocation List)	131
Crowds	229
Cryptographic File System (CFS)	99
Cryptographic Algorithm	62
Cryptographic hash functions	64
Cryptographic Techniques	61
Cryptographic protocol	62
Cryptography	62
CSK (Corporate Signing Key)	n74
Data Encryption Standard (DES)	67
DCE (Open Group Distributed Computing Environment)	144
DCMS	134
Denial of Service Attacken	9
DER	124
DES (Data Encryption Standard)	67
DH (Diffie-Hellman)	70
Dial-up-Client	83
Differential Fault Analysis (DFA)	21
Differential Power Analysis (DPA)	21
Diffie-Hellman (DH)	70
Digest Access Authentication	35
Digital copyright labeling	240
Digital Enveloping	71
Digital Millennium Copyright Act (DMCA)	244
Digital Signature Standard (DSS)	70
Digital Watermarking	238, 240f, 243
Distributed Computing Environment (DCE)	144

DMCA (Digital Millennium Copyright Act)	244
DNS Security (DNSSEC)	99
DNSSEC (DNS Security)	99
DOS-Attacken	9
Downloads	162
DSS (Digital Signature Standard)	70
Dual-Homed Firewall Configuration	54
Dynamic packet filtering or stateful inspection	50
Early work	221
ECC (Elliptic Curve Cryptography)	70
ECDH	70
ECDSA	70
Electronic cash systems	155
Electronic checks	156
Electronic credit-card payments	157
Electronic Identification (eID)	119
Electronic Payment Systems	150, 152
ElGamal	70
Elliptic Curve Cryptography (ECC)	70
e-mail anonym	221
Encapsulating Security Payload (ESP)	87, 90, 93f
Encoding Rules	124
Encrypted Session Manager (ESM)	98
ESM (Encrypted Session Manager)	98
ESP (Encapsulating Security Payload)	87, 90, 93f
Everything beta-effect	263
exec	211
Executable Content	163
eXtensible Markup Language (XML)	18
eXtensible rights Markup Language (XrML)	149
External Viewers	169
FastCGI	196, 208f
Fingerprints	242
Firewall Configuration	54
Firewall traversal	113
Firewall	44f
Formal risk analysis	258
Freedom Network	229
Generation of pseudorandom bit sequences	73
Generic security model	23
GII (Global Information Infrastructure)	7
Global Information Infrastructure (GII)	7
GoodPriv@cy	232
Group-Based Authorization and Access Control	40
Hash Function	64
Helper applications and plug-ins	168f
Hidden URL	29
Host-based scanning	260
HTTP Basic Authentication	31
HTTP Digest Access Authentication	35
HTTP GET Method	200
HTTP POST Method	200
HTTP Security	25
HTTP User Authentication	30
HTTP	15f, 26f, 191
Hybrid System	71
Hypertext Transfer Protocol	15f, 26f, 191
ICMP	12
ICRA (Internet Content Rating Association)	253
IDEA (International Data Encryption Algorithm)	67
Identity Providers	141
IETF PKIX WG	128
IGMP	12

IKE (Internet Key Exchange)	87, 89	Layer 2 Tunneling	80f	PGP (Pretty Good Privacy).....	99
IKMP (Internet Key Management Protocol)	85	Layer 3 Tunneling	80f	PGP Certificates.....	123, n67
Implications for firewalls.....	187	Legal issues	74	PGP Key servers.....	n76
Information Superhighway	7	Liberty Alliance Project.....	141	PGPadmin.....	n74
Intellectual Property Protection.....	234, 235	LNS (L2TP Network Server).....	83	Photuris Key Management Protocol.....	96
Intermediate CA Certificate.....	132	MAC (Message Authentication Code).....	91	PICS (Platform for Internet Content Selection).....	251f
International Data Encryption Algorithm (IDEA).....	67	marginally trusted.....	n72	PKCS (Public Key Certificate Standard)	109
Internet Content Rating Association (ICRA).....	253	MARION (Methodologie d'analyse des risques...)	258	PKI (Public Key Infrastructure).....	118
Internet Key Exchange (IKE).....	87, 89	MD2, MD4, MD5.....	65	PKI-Based AAI.....	139, 145
Internet Key Management Protocol (IKMP)	85	MEHARI (Methode Harmonisee d'analyse...)	258	PKIX (Public Key Infrastructure X.509).....	128
Internet layer security protocols.....	84	Message Authentication Code (MAC)	91	Platform for Internet Content Selection (PICS).....	251f
Internet Layer	12	meta-introducer.....	n73	Platform for Privacy Preferences Project (P3P).....	232
Internet Security Association and Key Mgmt Protocol (ISAKMP)	87, 96	Methode Harmonisee d'analyse (MEHARI).....	258	Plug-ins	170
Internet Security Protocols.....	75	Methodologie d'analyse des risques... (MARION)	258	PMI (Privilege Management Infrastructure).....	148
Internet Service Provider (ISP)	219	Micropayment systems.....	158	Point-to-Point Tunneling Protocol (PPTP)	81f
Internet Worm.....	9	Microsoft .NET Passport.....	140	PPP	12, 79
Internet	7	Microsoft Authenticode.....	165, 185	PPTP (Point-to-Point Tunneling Protocol)	81f
introducer.....	n73	Minimal Disclosure Certificate.....	135	Preimage Resistance.....	64
Intrusion detection	260	MKMP (Modular Key Management Protocol).....	96	Prepaid Payment Systems.....	154
invalid.....	n72	Modular Key Management Protocol (MKMP)	96	Privacy Enhancing Technologies (PET)	233
IP address blocking.....	249	Mosaic	17	Privacy Protection and Anonymity Services	216
IP next generation (IPng).....	85	Mozilla.....	17	Privacy seals	232
IP Security (IPSec)	85	NAT	56	Privacy	233
IP Security Protocol (IPSP)	85	National Information Infrastructure (NII).....	7	Private Communication Technology (PCT)	111
IP spoofing.....	9	Network access layer security protocols.....	77	Private key ring.....	n70
Ipng (IP next generation).....	85	Network Access Layer	12	Private Key.....	68
IPSec (IP Security).....	85	Network Address Translation (NAT)	56	Privilege Management Infrastructure (PMI).....	148
IPSP (IP Security Protocol).....	85	Network based scanning	260	Profile.....	128
IPv6.....	85	NFS.....	12	Property Protection.....	235
IPX.....	80	NII (National Information Infrastructure)	7	Protecting copyrights.....	242
ISAKMP (Internet Security Association and Key Mgmt Protocol).....	87, 96	NIS/YP	12	Protection of cryptographic keys.....	72
ISAPI.....	195, 206	NIST I-NLSP	84	Proxy Servers and Firewalls.....	42
ISO NLSP	84	Nonce	37	Pseudorandomly generated Bits.....	73
ISO TLSP.....	98	NSA/NIST SP3	84	PSTN	79
ISP (Internet Service Provider)	219	NSA/NIST SP4	98	Public Key Certificate Standard (PKCS)	109
ITU-T X.509.....	120	NSAPI	195, 206	Public Key Certificates	116, 121
Janus	230	OAKLEY Key Determination Protocol.....	96	Public Key Cryptography	68
JAP.....	229	Oakley.....	87	Public Key Infrastructure (PKI).....	118
Java Applets.....	173f, 177	Object Linking and Embedding (OLE).....	182	Public Key Infrastructure X.509 (PKIX)	128
Java Server Pages (JSP).....	197, 213	OCSP (Online Certificate Status Protocol).....	131	Public key ring.....	n70
Java Virtual Machine (JVM)	178	OLE (Object Linking and Embedding).....	182	Public Key	68
Java.....	177, 199	One-way Hash-Function.....	64	Publius	230
JavaScript.....	173, 175f	Onion routing and the Freedom Network.....	229	Python	199
Jscript.....	173f, 212	Online Certificate Status Protocol (OCSP).....	131	Random Bits.....	73
JSP (Java Server Pages).....	197, 213	Open Group Distributed Computing Environment (DCE).....	144	RAS	79
JVM (Java Virtual Machine).....	178	OpenPGP.....	n76	RC2, RC4, RC5, RC6.....	67
KDS (Key Distribution Center)	142	Opera	17	Receiver anonymity	220
Kerberos-based AAls	99, 142	origin.....	241	Recipient labeling	242
Key Distribution Center (KDS).....	142	owner trust.....	n72	recipient	241
Key Ieditimacy.....	n72	owner	241	Recreational Software Advisory Council (RSAC)	253
Key Management API	95	Ownership labeling	242	Remote System.....	83
Key revocation.....	n75	P3P (Platform for Privacy Preferences Project)	232	Repository.....	129
Key rings.....	n70	Padding	94	Restricting Access.....	29
Key servers.....	n76	Passive Mode FTP	51	Revocation.....	130, n75
keylegit.....	n72	Password Sniffing	9	Revoker.....	n75
L2F (Layer 2 Forwarding).....	81f	Pay-after Payment Systems.....	154	Rewebber Service.....	230
L2TP (Layer 2 Tunneling Protocol)	81f	Payment Systems	154	RIPEM	65
L2TP Access Concentrator (LAC)	83	Pay-now Payment Systems	154	RIPEMD.....	65
L2TP Network Server (LNS).....	83	PCT (Private Communication Technology).....	111	Risk Analysis.....	257
Label.....	242	PER	124	Risk Management Process	257
LAC (L2TP Access Concentrator)	83	Perl.....	199	Risk Management.....	138
Layer 2 Forwarding (L2F).....	81f	Personal Certificate.....	132	Risk Management	256
Layer 2 Tunneling Protocol (L2TP)	81f	PET (Privacy Enhancing Technologies)	233	Rivest, Shamir, Adleman (RSA).....	70

Root CA Certificate.....	132
Root-CA.....	n73
RPC.....	12
RSA (Rivest, Shamir, Adleman).....	70
RSAC (Recreational Software Advisory Council).....	253
RTP.....	12
S/MIME (Secure MIME).....	99
SAD (Security Association Database).....	89
SAFER.....	67
Screened Subnet Firewall Configuration.....	55
Screening Routers.....	48
Scripting Language.....	172, 173
SDSI (Simple Distributed Security Infrastructure).....	122
Second-Preimage Resistance.....	64
Secret key cryptography.....	66
Secure European Systems for Applications... (SESAME).....	144
Secure Key Exchange Mechanism (SKEME).....	96
Secure MIME (S/MIME).....	99
Secure Shell (SSH).....	99
Security Association Database (SAD).....	89
security in V2.0 effect.....	263
Security Manager.....	179f
Security Parameter Index (SPI).....	89, 92, 94, 95
Security Policy Database (SPD).....	89
Security Policy.....	24, 46
Security Scanning.....	260
Security zones.....	186
Sender anonymity.....	220
Sequence Number guessing.....	9
Server API.....	195, 206
Server Certificate.....	132
Server configuration.....	40
Server-Side Includes (SSI).....	197, 210f
Server-side Security.....	189
Service Providers.....	141
SESAME (Secure European Systems for Applications...).....	144
Session Hijacking.....	9
Set-Cookie.....	226
SHA-1.....	65
Side Channel attack.....	21
Signature recognition.....	260
Signature trust.....	n72
Signature.....	n68
sigtrust.....	n72
SILS (Standards for Interoperable LAN/MAN Security).....	77
Simple Distributed Security Infrastructure (SDSI).....	122
Simple Key Management for Internet Protocols (SKIP).....	96
Simple Object Access Protocol (SOAP).....	19
Simple Public Key Infrastructure (SPKI).....	122
Site Certificate.....	132
SKEME (Secure Key Exchange Mechanism).....	96
SKIP (Simple Key Management for Internet Protocols).....	96
SLIP.....	12
SOAP.....	19
SOCKS.....	52
Software Publisher Certificate.....	132
SPD (Security Policy Database).....	89
SPI (Security Parameter Index).....	89, 92, 94, 95
SPKI (Simple Public Key Infrastructure).....	122
SSH (Secure Shell).....	99
SSI (Server-Side Includes).....	197, 210f
SSL Alert Protocol.....	104
SSL and TLS certificates.....	112

SSL and TLS Protocols.....	101
SSL Application Data Protocol.....	104
SSL Change CipherSpec Protocol.....	104
SSL Handshake Protocol.....	104, 106
SSL Protocol.....	102
SSL Record Protocol.....	104, 105
SSLLeay.....	108
SSLRef.....	108
Standards for Interoperable LAN/MAN Security (SILS).....	77
standards rubber stamp effect.....	263
Stateful Inspection.....	50
Static Packet Filtering.....	48
stdin.....	199
stdout.....	199
SwlPe.....	84
TAZ Servers.....	230
Tcl.....	199
TCPA (Trusted Computing Platform Association).....	239
TGS (Ticket Granting Server).....	142
third-party tracking service.....	226
Threat model.....	257
Threat.....	20
Threats Analysis.....	257
Ticket Granting Server (TGS).....	142
Timing Attacks.....	21
TLS Protocol.....	111
Traffic analysis.....	222
Transparent Firewall.....	57
Transport layer security protocols.....	98
Transport Layer.....	12
Triple-DES (3DES).....	67
Trust Management.....	138
TRUSTe.....	232
Trusted Computing Platform Association (TCPA).....	239
Trusted introducer.....	n73
UDDI.....	19
Unconditional Security.....	63
Universal Description Discovery and Integration (UDDI).....	19
unknown.....	n72
untrusted.....	n72
URL blocking.....	249
URL.....	200
Usage control.....	238, 239f
User authentication authorization, and access control.....	28
User Based Authorization and Access Control.....	40
User ID.....	n68
valid.....	n72
VBScript.....	173f, 212
Vendor sponsored incompatibility effect.....	263
Virtual Private Network.....	80f
Virtual Tunneling Protocol (VTP).....	80
Voluntary privacy standards.....	231
VPN.....	80f
VTP (Virtual Tunneling Protocol).....	80
Vulnerabilities, threats, and countermeasures.....	20
Vulnerabilities Analysis.....	257
WAIS.....	12
Watermarking.....	238, 240f , 243
Web Bugs.....	228
Web Server.....	28, 192
Web Services Inspection Language (WSIL).....	19
Web Services Markup Language (WSDL).....	19
Web Services.....	18f

Wobbly code effect.....	263
World Wide Web.....	15
Wrapper.....	205
WSDL.....	19
WSIL.....	19
WWW.....	15, 223
X.509 Certificates.....	123, n68
X.509.....	120, 145
XML Security.....	99
XML.....	18
XrML (eXtensible rights Markup Language).....	149