

SS2003 – WWWsec

Index	Script	Book
AAIs (authentication and authorization infrastructures) <i>Microsoft .NET, Kerberos, PKI-based</i>	136ff	213ff
AAs – attribute authorities	118	186
access control HTTP	29	26
ActiveX controls	182ff	283ff
AH (IPsec)	87, 91	133
anonymity <i>sender, receiver, unlinkability</i>	220	320
Anonymous browsing	229f	328ff
Anonymous publishing	229f	336ff
application-level gateways	53	64ff
ASP (active server pages)	212	312
asymmetric cryptography (public key)	68ff	96ff
attacks	9, 21	
attribute certificates	117, 146	186, 242
binary mail attachment	166	271
CAs – certification authorities	118	186
Censorship on the WWW <i>content blocking, content rating</i>	247ff	359ff
Certificate Management, PKI	115ff	185ff
certification path (chain)	127	192
certification revocation <i>(automatic, on-line cert repository, CRLs, OCSP)</i>	131	196ff
CGI (common gateway interface), FastCGI	194, 198ff	300ff
circuit-level gateways (e.g. SOCKS)	52	58ff
client-side security	160ff	267ff
COM (Component Object Model)	182	283
computational vs. unconditional security	63	88
content rating (vs. self-determination)	250ff	360
cookies	224ff	324ff
cryptographic algorithm (Def.)	62	88
cryptographic protocol (Def.)	62	88
cryptographic techniques	62ff	87ff

cryptography (Def.)	62	87
digital enveloping → hybrid systems	71	103f
digital watermarking	238	349
dynamic packet filtering (= stateful inspection)	50f	57f
electronic cash systems	155	255f
electronic CC-payments		259f
electronic checks		257f
electronic payment systems <i>(prepaid, pay-now, pay-after payment system)</i>	150ff	249ff
ESP (IPsec)	87, 93	135
executable/active content	163	267ff
Faktorisierungsproblem	70	
FastCGI	208f	310
firewall / proxy servers	42ff	49ff
firewall configurations (dual-homed, screened host, screened subnet)	54f	68ff
Firewall traversal <i>(proxied/tunneled)</i>	113	178ff
formal risk analysis	258f	378
hash functions	64f	90f
helper applications / plug-ins	168ff	272f
hierarchical trust model (X.509 certificates)	126	189, 192
HTTP	27	21ff
HTTP basic authentication	31	29
HTTP certification based auth (→ SSL/TLS)	39	41
HTTP digest authentication	35	34
hybrid systems (symm. + asymm.) e.g. → digital enveloping	71	103f
IKE/IPsec	89	136ff
IKMP, IPSP	85	
Intellectual property protection <i>usage control, digital watermarking</i>	234	347ff
Internet layer (TCP/IP 2) security protocols	84ff	125ff
internet layer sec prot implementations <i>(native, BITS, BITW)</i>	97	141
Internet security protocols (→ Network/ Internet/ Transport/ Application layer security prot.)	75ff, 100	117ff

Internet-Model (TCP/IP)	12	
intrusion detection / security scanning	260	381f
IPsec protocols	85	131ff
IPsec transport/tunnel mode	90	132
IPv6	85	
Java applets	177ff	278ff
JDK <i>1.0 → sandbox, 1.1 → trusted signed code, 1.2 → security policy</i>	179ff	281
JSP (java server pages)	213	313
Kerberos-based AAIs	142	231ff
key management (IPsec)	95	137
layer 2 (network) tunneling	80f	124
layer 3 (transport) tunneling	80f	
malicious attacks	9	
micropayment systems	158	261f
Microsoft .NET Passport <i>(standard, secure channel, strong credential sign-in)</i>	140	216ff
NAT (network address translation)	56	74ff
network access layer (1) security protocols	77ff	118
network address translation (NAT)	56	74ff
OLE (Object Linking and Embedding)	182	283
OSI vs. TCP/IP	12	
passive mode FTP (→ dynamic packet filtering)	51	58
PGP	67ff	
PGP vs. X.509 certificates (public key)	68, 123	
PKI – Public Key Infrastructure	115ff	185ff
PKI-based AAIs		241ff
plug-ins / helper applications	168ff	272f
PMI (privilege management infrastructure)	148	
Point-to-Point Tunneling Protocol (PPTP)	82	122
Privacy Protection and Anonymity Services	216ff	317ff
privacy standards	231f	341
proxy servers / firewalls	42ff	49ff

public key cryptography (asymmetric) <i>RSA, DH, ElGamal, DSS, ECC</i>	68ff	96ff
Risk management	256ff	375ff
router (→ static level packet filtering)	48	54f
screening routers (→ static level packet filtering)	48	55
scripting languages (client-side)	174f	275ff
secret key cryptography (symmetric) <i>DES, 3DES, IDEA, SAFER, Blowfish, CAST-128, RC2/5/6, RC4, AES</i>	66ff	82ff
security scanning / intrusion detection	260	379f
self-determination (vs. content rating)	250ff	360
Server APIs	206f	309
Server-side Security	189ff	297ff
SESAME	144	240
side-channel attacks	21	
SSI (server-side includes)	210f	311
SSL handshake protocol	106	161ff
SSL record format protocol	105	159f
SSL/TLS (application layer)	101ff	153ff
SSL/TLS certificates	112	175ff
SSLRef, SSLeay	108	
stateful inspection (= dynamic packet filtering)	50f	57f
static packet filtering	48	54f
symmetric cryptography (secret key)	66ff	82ff
TCP/IP Referenzmodell	12	
Transport layer security protocols (SSL/TLS)	98	143ff
unconditional vs. computational security	63	88
VPN		124
vulnerability, threats, countermeasures	20	
Web of Trust / PGP	67ff	
X.509 certificate	68, 120	

SS2003 – WWWsec

Index	Script	Book									
TCP/IP Referenzmodell	12		unconditional vs. computational security	63	88	PGP vs. X.509 certificates (public key)	68, 123		scripting languages (client-side)	174f	275ff
OSI vs. TCP/IP	12		hash functions	64f	90f	X.509 certificate	68, 120		Java applets	177ff	278ff
Internet-Model (TCP/IP)	12		secret key cryptography (symmetric) <i>DES, 3DES, IDEA, SAFER, Blowfish, CAST-128, RC2/5/6, RC4, AES</i>	66ff	82ff	SSL/TLS (application layer)	101ff	153ff	JDK	179ff	281
malicious attacks	9		symmetric cryptography (secret key)	66ff	82ff	SSL record format protocol	105	159f	1.0 → <i>sandbox</i> , 1.1 → <i>trusted signed code</i> , 1.2 → <i>security policy</i>		
attacks	9, 21		public key cryptography (asymmetric) <i>RSA, DH, ElGamal, DSS, ECC</i>	68ff	96ff	SSL handshake protocol	106	161ff	OLE (Object Linking and Embedding)	182	283
side-channel attacks	21		asymmetric cryptography (public key)	68ff	96ff	SSLRef, SSLeay	108		COM (Component Object Model)	182	283
vulnerability, threats, countermeasures	20		hybrid systems (symm. + asymm.) e.g. → digital enveloping	71	103f	Firewall traversal (<i>proxied/tunneled</i>)	113	178ff	ActiveX controls	182ff	283ff
HTTP	27	21ff	digital enveloping → hybrid systems	71	103f	Certificate Management, PKI	115ff	185ff	Server-side Security	189ff	297ff
access control HTTP	29	26	Faktorierungsproblem	70		PKI – Public Key Infrastructure	115ff	185ff	CGI (common gateway interface), FastCGI	194, 198ff	300ff
HTTP basic authentication	31	29	Internet security protocols (→ Network/ Internet/ Transport/ Application layer security prot.)	75ff, 100	117ff	attribute certificates	117, 146	186, 242	FastCGI	208f	310
HTTP digest authentication	35	34	network access layer (1) security protocols	77ff	118	CAs – certification authorities	118	186	Server APIs	206f	309
HTTP certification based auth (→ SSL/TLS)	39	41	layer 2 (network) tunneling	80f	124	AAs – attribute authorities	118	186	SSI (server-side includes)	210f	311
proxy servers / firewalls	42ff	49ff	layer 3 (transport) tunneling	80f		hierarchical trust model (X.509 certificates)	126	189, 192	ASP (active server pages)	212	312
firewall / proxy servers	42ff	49ff	VPN		124	certification path (chain)	127	192	JSP (java server pages)	213	313
static packet filtering	48	54f	Point-to-Point Tunneling Protocol (PPTP)	82	122	certification revocation (<i>automatic, on-line cert repository, CRLs, OCSP</i>)	131	196ff	Privacy Protection and Anonymity Services	216ff	317ff
screening routers (→ static level packet filtering)	48	55	Internet layer (TCP/IP 2) security protocols	84ff	125ff	AAIs (authentication and authorization infrastructures) <i>Microsoft .NET, Kerberos, PKI-based</i>	136ff	213ff	anonymity <i>sender, receiver, unlinkability</i>	220	320
router (→ static level packet filtering)	48	54f	IPv6	85		Microsoft .NET Passport (<i>standard, secure channel, strong credential sign-in</i>)	140	216ff	cookies	224ff	324ff
dynamic packet filtering (= stateful inspection)	50f	57f	IPsec protocols	85	131ff	Kerberos-based AAIs	142	231ff	Anonymous browsing	229f	328ff
stateful inspection (= dynamic packet filtering)	50f	57f	IKMP, IPSP	85		SESAME	144	240	Anonymous publishing	229f	336ff
passive mode FTP (→ dynamic packet filtering)	51	58	AH (IPsec)	87, 91	133	PKI-based AAIs		241ff	privacy standards	231f	341
circuit-level gateways (e.g. SOCKS)	52	58ff	ESP (IPsec)	87, 93	135	PMI (privilege management infrastructure)	148		Intellectual property protection <i>usage control, digital watermarking</i>	234	347ff
application-level gateways	53	64ff	IKE/IPsec	89	136ff	electronic payment systems (<i>prepaid, pay-now, pay-after payment system</i>)	150ff	249ff	digital watermarking	238	349
firewall configurations (dual-homed, screened host, screened subnet)	54f	68ff	IPsec transport/tunnel mode	90	132	electronic cash systems	155	255f	Censorship on the WWW <i>content blocking, content rating</i>	247ff	359ff
NAT (network address translation)	56	74ff	key management (IPsec)	95	137	electronic checks		257f	self-determination (vs. content rating)	250ff	360
network address translation (NAT)	56	74ff	internet layer sec prot implementations <i>(native, BITS, BITW)</i>	97	141	electronic CC-payments		259f	content rating (vs. self-determination)	250ff	360
cryptographic techniques	62ff	87ff	Transport layer security protocols (SSL/TLS)	98	143ff	micropayment systems	158	261f	Risk management	256ff	375ff
cryptography (Def.)	62	87	Web of Trust / PGP	67ff		client-side security	160ff	267ff	formal risk analysis	258f	378
cryptographic algorithm (Def.)	62	88	PGP	67ff		executable/active content	163	267ff	security scanning / intrusion detection	260	379f
cryptographic protocol (Def.)	62	88				binary mail attachment	166	271	intrusion detection / security scanning	260	381f
computational vs. unconditional security	63	88				helper applications / plug-ins	168ff	272f			
						plug-ins / helper applications	168ff	272f			