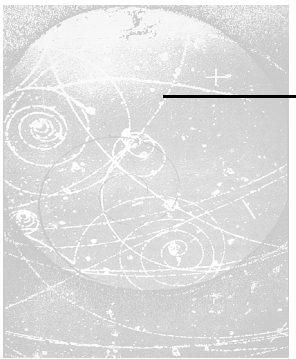

Index

A

Addressing, 24, 29–38
  anycast addressing, 31
  IPv4, 29–33
  IPv6, 33–35
  multicast addressing, 31
  unicast addressing, 31
Adleman, Leonard, 12
Advanced Encryption Standard (AES), 44
Advanced Research Projects Agency (ARPA), 4
AES cipher, 9, 178
AES-CBC, 52
Agee, Ryan, 226
Aggressive mode exchange, 56–57, 122–23
Algorithm, 3
Antireplay, 75, 222–23
Anycast addressing, 31
Application layer, 25
Application level, security, 40–41
Applied Cryptography (Schneier), 21
Architecture, IPSec, 45–46
Architecture Document for IPSec (RFC2401), 45
ARPANET, 4, 24
Asymmetric ciphers, 11–13
  El-Gamal, 13
  RSA, 12
Asynchronous Transfer Mode (ATM), 26
Attribute payload, 106
Authentication, 13–15

in antiquity, 2
digital signature, 13–15
Authentication Header (AH), 44, 45, 52–53, 93–100
defined, 93
header, 53, 94–95
modes, 96–97
transport mode, 96
tunnel mode, 96–97
processing, 97–99
input processing, 99–100
output processing, 97–99
Authenticator, 50, 84

B

Bellare, Mihir, 16
Birthday Attacks, 21
Block ciphers, 9–10
Blowfish cipher, 9
Blowfish-CBC, 52
Broadcast, 29
Bump in the Stack (BITS), 46, 63–64, 168
Bump in the Wire (BITW), 46, 168

C

Caesar Cipher, 2
Canetti, Ran, 16
CAST cipher, 9, 178
CAST-CBC, 52
Certificate payload, 105
Certificate request payload, 105
Certificates, 241–43
authentication of, 242–43
revoked, 244–45
Chained tunnels, 175–76
Checksum field:
IPv4 header, 157
IPv4 tunnel header, 33
Cipher block chaining (CBC), 10–11
Encapsulating Security Payload (ESP), 51
Cipher Feedback Mode (CFB), 11
Ciphers, 9–13, 50
asymmetric, 11–13
block, 9–10
stream, 9–10
substitution, 2
symmetric, 9–11
Class field:
IPv6 tunnel header, 157
Clipper Chip debate, 3
Cocks, Clifford, 12
Collision, 8
Communication technology, growth of, 3
Compression, 218–21
input processing, 220–21
output processing, 220
Computationally secure cryptosystems, 4
Computationally secure public key algorithms, 11
Confidentiality, in antiquity, 2
Cryptographic building blocks, 6–18
authentication, 13–15
ciphers, 9–13
key exchanges, 16–18
message integrity, 15–16
one-way functions, 6
one-way hash functions, 8–9
trap doors, 6–8
Cryptographic history/techniques, 1–21
building blocks, 6–18
denial of service attacks, 20
Internet:
rise of, 4
security, 5

perfect forward secrecy, 19–20
secrets in history, 2–3
Cryptography and Data Security (Denning), 21

D

DARPA (Defense Advanced Research Project Agency), 24
Data link layer, 26, 28
security, 42
DECNET, 24
Decryption, 10
Deep Crack, 88
Denial of service attacks, 20
Deployment:
policy, 139–40
architecture, 137
Deployment scenarios, 177–214
four-office company example, 185–95
fully-meshed configuration, 186–92
hub-and-spoke configuration, 192–95
multiple company extranet example, 195–204
each site hosts extranet, 200–204
single site hosts extranet, 196–200
outsourcing networks, 204–14
extranets, 207–9
intranets, 206
issues, 212–14
multiple ISP's issues, 214
PE- vs. CE-based solution, 205–6
policy, 212–13
security in ISP network, 213
third-party extranet, 209–12
DES-CBC, 52
Destination address field:
IPv4 header, 157
IPv4 tunnel header, 33
IPv6 header, 34
IPv6 tunnel header, 157
Destination-based options, 35
Diffie-Hellman key exchange, 17–18, 109, 178, 225
Diffie, Whitfield, 12, 17
Digital Encryption Standard (DES), 44
Digital signature, 13–15
and Digital Signature Algorithm (DSA), 14
and one-way hash functions, 14
and RSA, 15
verification of, 14
Digital Signature Algorithm (DSA), 15, 75, 115
Digital Signature Standard (DSS), 13–14, 55
Discard action:
SPD entries, 48
Discrete Logarithm Problem, 7, 13
Domain Name System (DNS), 24, 25, 38–39
Domain of Interpretation (DOI), 54, 61, 113, 128, 141

E

El-Gamal, 13
Electronic Code Book (ECB) mode, 10
Ellis, James, 12
Encapsulating Security Payload (ESP), 44, 45, 50–52, 83–91
algorithms, 50
authenticator, 84
cipher block chaining (CBC) mode, 51
defined, 83

encryptor, 84
header, 51–52, 84–86
SPI field, 83
modes, 86–87
transport mode, 86–87
tunnel mode, 86–87
padding, 86
processing, 88–91
inbound processing, 89–91
outbound processing, 88–89
Encrypted Key Exchange (EKE), 21
Encryption, 235
Encryptor, 84
End-to-end security, 168–69
Enigma, 3
Ethernet, 26
Exclusive-or (XOR) function, 8–9
Extension headers field:
IPv6 tunnel header, 157

F

Federal Information Processing Standard (FIPS), 15
Feedback mode:
symmetric ciphers, 10
Firewall and VPN gateway interaction, 183–85
Flags field:
IPv4 header, 156
IPv4 tunnel header, 32
Flow id field, IPv6 tunnel header, 157
Flow label field, IPv6 header, 34
Four-office company scenario, 185–95
fully-meshed configuration, 186–92
hub-and-spoke configuration, 192–95
Fragmentation, 35–36, 80
and PMTU, 162–66
Fragmentation offset field:
IPv4 header, 156
IPv4 tunnel header, 32

G

Group access package, 229–30
Group key distribution center (GKDC), 229–30

H

Harder, Eric, 226
Hash payload, 105
Header chaining, 33
Header length field:
IPv4 header, 156
IPv4 tunnel header, 32
Hellman, Martin, 12, 17
Hierarchical trust model, 244
HMAC, 16, 19
HMAC-MD5, 16, 47, 52, 152, 178
HMAC-MD5-96, 88
HMAC-RIPEMD, 47
HMAC-SHA, 16, 47, 52, 178
HMAC-SHA-96, 88
Hop-by-hop options, 35
Hop limit field:
IPv6 header, 34
IPv6 tunnel header, 157
Host ID, 29
Host implementation, 62
Hub-and-spoke, 175

I

IANA (Internet Assigned Number Authority), 105
ICMP (Internet Control Message Protocol), 36, 80–81

error messages, handling, 166
processing, 166
Identification field:
IPv4 header, 156
IPv4 tunnel header, 32
Identification payload, 105
Implementation:
IPSec (IP Security), 143–46
architecture, 144–51
Internet Key Exchange (IKE), 144, 149–51
IPSec base protocols, 144, 145–46
policy, 145
SA management, 145
SADB, 144, 146–49
SPD, 144, 146–49
Inbound processing, 79–80
ESP, 89–90
Initialization Vector (IV), 10
Input processing:
AH, 99–100
compression, 220–21
Internet, 24
security, 39–42
application level, 40–41
basic services, 39–40
data link layer, 42
network layer, 41–42
transport layer, 41
Internet Key Exchange (IKE), 48, 54–58, 101–29, 144, 149–51, 178
aggressive mode exchange, 56–57, 122–23
cookies, exchange of, 56–57
defined, 101–2
Domain of Interpretation (DOI), 128
IKE informational exchange, 127
and ISAKMP, 112–28
keys for the IPSec protocols, 61
main mode exchange, 55–57, 117–22, 178–79
new group exchange, 127–28
and policy, 139
processing, 153–54
quick mode exchange, 56, 58, 123–27
SA, creation of, 55–56
suite for, 179
Internet Research Task Force (IRTF), 234–35
Internet Security Association and Key Management Protocol, ***See*** **ISAKMP**
Internet Service Providers (ISPs), 4
Intranets, 140
and network layer security, 42
IP address, parts of, 29
IP broadcast, 29
IP Payload Compression Protocol (PCP), 218–20
IPSec (IP Security), 80
anti-replay, 48–50
architecture, 45–46, 59–81
Architecture Document for IPSec (RFC2401), 45
Authentication Header (AH), 44, 45, 52–53
base protocols, 144, 145–46
chained tunnels, 175–76
defined, 44
Domain of Interpretation (DOI), 54, 61, 128, 141
Encapsulating Security Payload (ESP), 44, 45, 50–52
end-to-end security, 168–69
fragmentation, 80
future of, 217–46
compression, 218–21
key recovery, 235–37

Layer 2 Tunneling Protocol (L2TP), 237–41
multicast, 222–35
public key infrastructure, 241–46
ICMP (Internet Control Message Protocol), 80–81
implementation, 62–66, 143–46
architecture, 144–51
Bump in the Stack (BITS), 63–64
fragmentation and PMTU, 162–66
host implementation, 62
Internet Key Exchange (IKE), 144, 149–51
IPSec base protocols, 144, 145–46
IPSec protocol processing, 151–62
OS integrated, 62–63
policy, 145
router implementation, 64–66
SA management, 145
SADB, 144, 146–49
SPD, 144, 146–49
Internet Key Exchange (IKE), 54–58
kernel, and policy, 138–39
modes, 66–71, 168
transport mode, 66–68, 168
tunnel mode, 68–71, 168
nested tunnels, 172–74
policy, 47–48, 61
processing, 77–80
ICMP (Internet Control Message Protocol) processing, 166
inbound processing, 79–80
outbound processing, 78–79
road warriors, 171–72
roadmap, 60–61
security associations (SAs), 46–47, 54
security policy, 76–77
selectors, 48, 76–77
destination address, 77
name, 77
protocol, 77
source address, 76
upper layer ports, 77
SPD database, 76
stack layering, 63
VPNs (virtual private networks), 170–71
IPSec protocol processing, 151–62
example of, 152
inbound processing, 159–62
IPSec layer, steps performed by, 159–60
possible failures, 161
tunneled processing, 161–62
outbound processing, 151–59
IKE processing, 153–54
SA processing, 154–58
SPD processing, 153
IPv4, 28
addressing, 29–33
header, 31–33
checksum, 33
destination address, 33
flags, 32
fragmentation offset, 32
header length, 32
identification, 32
length, 32
options, 33
protocol, 33
source address, 33
Time To Live (TTL), 32
type of service (TOS), 32
version field, 31–32
IPv6:
addressing, 33

advantage of, 33
extensions headers, 34–35
header, 34
flow label, 34
hop limit, 34
next header, 34
payload length, 34
source and destination address, 34
traffic class, 34
version field, 34
ISAKMP, 102–12
cookies, 108–10
exchanges and phases, 107–8
generic header, 104
header, 103
and IKE, 112–28
messages, 106–7
payloads, 103–6
hash payload, 105
key exchange payload, 105
nonce payload, 105
signature payload, 105
vendor ID payload, 105
policy negotiation, 110–12

K

Kerberos, 40
Key encrypting key (KEK), 226–29
Key exchange payload, 105
Key exchanges, 16–18
Diffie-Hellman key exchange, 17–18
RSA key exchange, 18–19
Key management in multicast security, 225–29
forced member removal, 225
group access package, 229–30
group key distribution center (GKDC), 229–30
join latency, 225
key encrypting key (KEK), 226–29
protocols, 226
rekeying, 225
secure multicast key distribution, 229–30
Key recovery, 235–37
and IPSec, 236–37
Keyed hashing, 16
Knapsack problem, 21
Krawczyk, Hugo, 16, 102

L

L2TP Access Concentrator (LAC), 238
L2TP Network Server (LNS), 238
Layer 2 Tunneling Protocol (L2TP), 237–41
compulsory configuration, 238
defined, 237
implementing as a UDP-based IP protocol, 239–40
network access with, 239
and security, 240
types of configurations, 238
voluntary configuration, 238
LDAP (Lightweight Directory Access Protocol), 135–36
Length field:
IPv4 header, 156
IPv4 tunnel header, 32
IPv6 tunnel header, 157

M

Main mode exchange, 55–57, 117–22, 178–79
Management, policy, 132, 137–39
IKE support, 139
interfaces defined by, 137

kernel support, 138–39
MD5 (Message Digest 5), 8
Message authentication codes (MACs), 15–16
Message ID, 57–58
Message integrity, 15–16
keyed hashing, 16
message authentication codes (MACs), 15–16
MILNET, 4
MKMP, 230–35
group key manager (GKM), 231
key distribution protocol, 233–34
MKMP-aware routers, 231–32
multicast data distribution tree, 231–32
Router Alert option, on solicitation message, 231
scaling ability, 234
Multicast, 222–35
key management, 225–29
multicast key management protocol (MKMP), 230–35
secure multicast key distribution, 229–30
source authentication, 222–25
Multicast addressing, 31
Multicast key management protocol, ***See*** **MKMP**
Multicast packets, 36–37
Multiple company extranet scenario, 195–204
each site hosts extranet, 200–204
single site hosts extranet, 196–200
Multiple header processing, 158–59

N

Nested tunnels, 172–74
Network Address Translation (NAT), 169
Network ID, 29
Network Interface Card (NIC), 239
Network layer, 26, 28
security, 41–42
Networking protocol architectures, 24
New group exchange, 127–28
Next header field:
IPv6 header, 34
IPv6 tunnel header, 157
Nonce payload, 105
NSFnet, 4

O

Oakley, 102
One-way functions, 6–7
One-way hash functions, 8–9
and digital-signature verification, 14
Options field:
IPv4 header, 157
IPv4 tunnel header, 33
Orman, Hilarie, 102
OSI, 24
OSPF (Open Shortest Path First), 61
Outbound processing, 78–79
ESP, 88–89
IPSec protocols:
IKE processing, 153–54
SA processing, 154–58
SPD processing, 153
Output Feedback Mode (OFB), 11
Output processing:
AH, 99–100
compression, 220
Outsourcing networks scenario, 204–14
extranets, 207–9
intranets, 206

issues, 212–14
multiple ISP's issues, 214
PE- vs. CE-based solution, 205–6
policy, 212–13
security in ISP network, 213
third-party extranet, 209–12

P

Padding, 98
Path MTU discovery (PMTU), 36
and fragmentation, 162–66
host implementation, 163
router implementation, 163–66
Payload Compression Protocol (PCP), 218–20
and Internet Key Exchange (IKE), 219
processing, 219–20
Payload length field, IPv6 header, 34
Payloads:
hash payload, 105
key exchange payload, 105
nonce payload, 105
signature payload, 105
vendor ID payload, 105
PCP, 218–20
Perfect forward secrecy (PFS), 19–20, 56
PGP, 40
Photuris key exchange, 108
PHP, 177–214
Point-to-point protocol (PPP), 237, 240
Policy, 131–41, 145
compared to standards, 132
configuring between domains, 140
defined, 132
definition requirement, 133–35
deny, 179
deployment, 132, 139–40
architecture, 137
IPSec, 47–48
keywords, 179
language, 178–80
management, 132, 137–39
IKE support, 139
interfaces defined by, 137
kernel support, 138–39
permit, 179
protect, 179
remote access, 181–85
representation/distribution, 135–37
setting up, 141
site-to-site, 180
Privacy, and anonymity, 4
Private key encryption, 14
Protect action, SPD entries, 48
Protection suites, 55
Protocol field:
IPv4 header, 157
IPv4 tunnel header, 33
Protocol stack, 24–28
application layer, 25
data link layer, 26, 28
network layer, 26, 28
transport layer, 25–27
Public key algorithms, 10–12
El-Gamal, 12
RSA, 12
Public key cryptography, 12
Public Key Infrastructure (PKI), 241–46
certificates, 241–43
revoked, 244–45
hierarchical trust model, 244
namespace, 245
single-level type, 243

Q

Quick mode exchange, 56, 58, 123–27

R

Remote access policies, 181–85
addressing, 185
firewall and VPN gateway interaction, 183–85
RIPEMD, 8
Rivest, Ron, 12
Road warriors, 171–72
ROT-13-cipher, 9–10
Router implementation, 64–66
Bump in the Wire (BITW), 64–65
implications on packet-forwarding capabilities of the router, 65
IPSec contexts, 66
native implementation, 64–65
Routers, 26
Routing, 24
RSA, 12, 75, 115, 178
and digital signature, 15
RSA key exchange, 18–19

S

SA management, 145
SADB, 144, 146–49
Secure multicast key distribution, 229–30
Secure Shell, 40
Security Association Database (SADB), 46–47
Security association payload, 105
Security associations (SAs), 46–47, 71–74, 222
management, 73–74
creation, 73–74
deletion, 74
parameters, 74–77
antireplay window, 75
lifetime, 75
mode, 75
PMTU parameters, 75
sequence number, 74
sequence number overflow, 75
tunnel destination, 75
processing, 154–58
multiple header processing, 158–59
transport mode header processing, 154–55
tunnel mode processing, 155–58
Security Parameter Index (SPI), 71–72
Security Parameter Index (SPI), 46–47, 71–72
Security Policy Database (SPD), 47–48
"Security through obscurity," 3
Selectors, 48
SHA (Secure Hash Algorithm), 8
Shamir, Adi, 12
Signature payload, 105
Site-to-site policies, 180
SKEME, 102
SKEYID, 115–17
SMuG working group:
Internet Research Task Force (IRTF), 235
SNA, 24
Source address field:
IPv4 header, 157
IPv4 tunnel header, 33
IPv6 header, 34
IPv6 tunnel header, 157
Source authentication:
multicast, 222–25
SPD, 144, 146–49
processing, 153
Stream ciphers, 9–10
Subnets, 30
Substitution ciphers, 2

Symmetric ciphers, 9–11
AES cipher, 9
block ciphers, 9–10
Blowfish cipher, 9
CAST cipher, 9
Cipher Block Chaining (CBC), 10–11
Cipher Feedback Mode (CFB), 11
Electronic Code Book (ECB) mode, 10
feedback mode, 10
Output Feedback Mode (OFB), 11
stream ciphers, 9–10

T

TCP/IP protocol suite, 4, 23–42
addressing, 24, 29–38
Domain Name System (DNS), 38–39
fragmentation, 35–36
history of, 24
ICMP (Internet Control Message Protocol), 36
multicast packets, 36–37
protocol stack, 24–28
routing, 24
Transmission Control Protocol (TCP), 37–38
transport layer, 37–38
User Datagram Protocol (UDP), 37–38
3DES-CBC, 52
Time To Live (TTL) field:
IPv4 header, 156–57
IPv4 tunnel header, 32
Token Ring, 26
Traffic class field:
IPv6 header, 34
Transmission Control Protocol (TCP), 37–38
Transport layer, 25–27
security, 41
TCP/IP, 37–38
Transport Layer Security (TLS), 41
Transport mode, 66–68, 168
ESP, 86–87
Transport mode header processing, 154–55
AH processing, 155
defined, 154–55
ESP processing, 155
Trap door function tree, 7–8
Trap doors, 6–8
Triple-DES (3DES), 117, 135, 178
Tunnel mode, 68–71, 168
ESP, 86–87
Tunnel mode processing, 155–58
defined, 155
IPv4 tunnel header, 156–57
IPv6 tunnel header, 157–58
Type Of Service (TOS) field:
IPv4 header, 156
IPv4 tunnel header, 32

U

Unicast addressing, 31
User Datagram Protocol (UDP), 37–38, 43

V

Vendor ID payload, 105
Version field:
IPv4 header, 156
IPv4 tunnel header, 31–32
IPv6 header, 34
IPv6 tunnel header, 157

VPNs (virtual private networks), 140, 170–71
and firewall interaction, 183–85
and network layer security, 42

W

Wallner, Debby, 226
Williamson, Malcolm, 12
World War II, U.S. Army code cracking in, 2–3

Z

Zero knowledge proof, 21