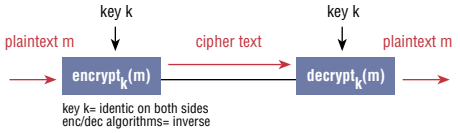
JOHN CORDIER ACADEMY

IP security reference card

telindus
Belgacom ICT

SYMMETRIC CRYPTO



Historic:

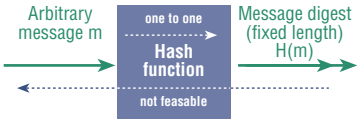
Caesar
Substitution
Vigenère
Vernam
...

Symmetric Ciphers

Stream cipher	Block cipher
Applied on each digit	Applied on equal data blocks
RC4.SEAL	(3)DES: ECB, CFB, OFB,.. IDEA, RC2, AES RC5, Blowfish, CAST-128

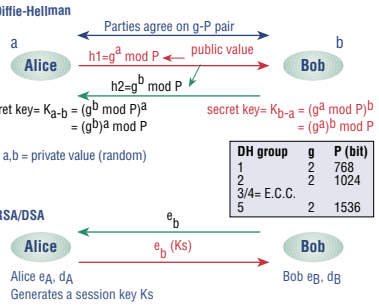
Name	Key Length (bit)	Block Size (bit)
DES	56	64
3DES	112/168	64
IDEA	128	64
Blowfish	32-448	64
CAST-128	40-128	64
RC2	8-1024	64
RC5	0➔2040	128
AES	128-256	128

HASHING



Algorithm	Output (bit)
Checksum	16
MD4	128
MD5	128
SHA-1	160
SHA-xxx	256 / 384 / 512
RIPEMD-160	160

KEY EXCHANGE MECHANISMS

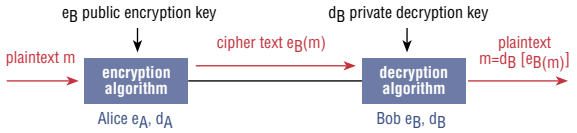


DH group	g	P (bit)
1	2	768
2	2	1024
3/4= E.C.C.		
5	2	1536

PUBLIC KEY CRYPTO

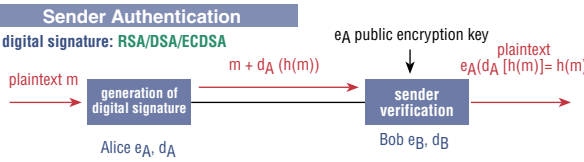
Secrecy

main use: sending over session keys = digital envelope: RSA



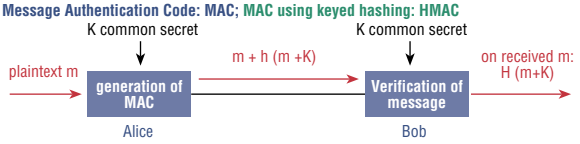
Sender Authentication

digital signature: RSA/DSA/ECDSA



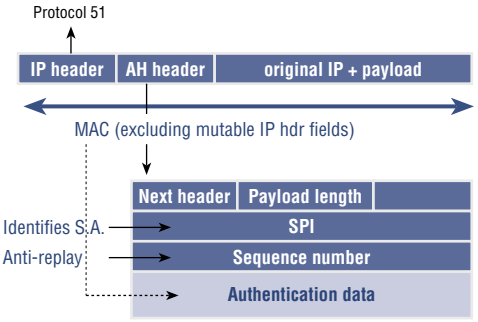
Message integrity

Message Authentication Code: MAC; MAC using keyed hashing: HMAC

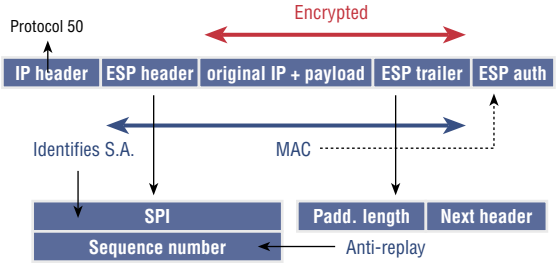


IPsec (TUNNEL MODE)

Authentication Header (AH)

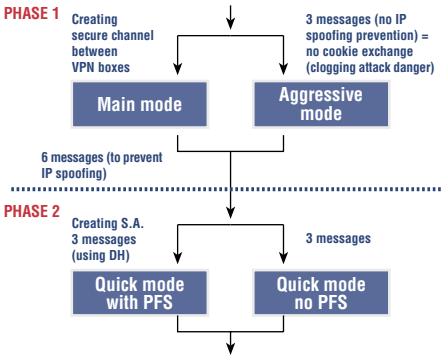


Encapsulation Security Payload (ESP)



Sender: first encrypt, then authenticate
Receiver: first authenticate, then decrypt

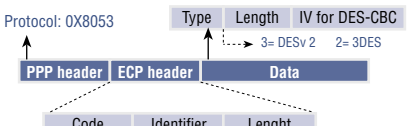
IKE NEGOTIATION



PPP SECURITY

Encryption

1. ECP:IETF Session key= aggreed upon prior to encryption
Encryption not applied to LCP / ECP packets

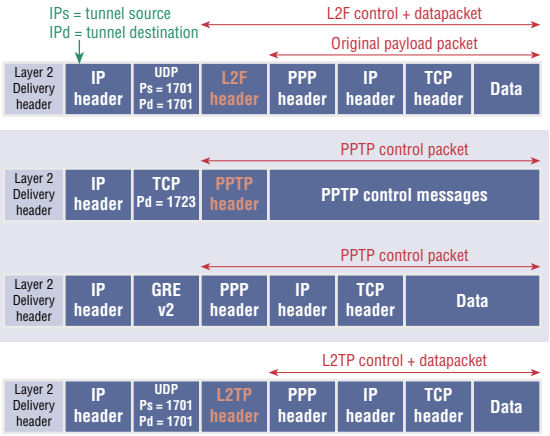


Code	Identifier	Lenght
1	Configure - Request.	
2	Configure - Ack.	
3	Configure - Nak	
4	Configure - Reject.	
5	Configure - Request.	
6	Configure - Ack.	
7	Code - Reject.	

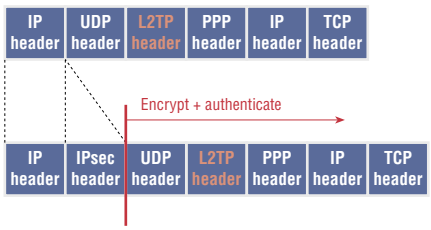
2. MPPE: Microsoft PtoP encryption:
RC4 key length negotiable: 40-56-128 bits

Authentication: EAP (RFC 2284)

L2F - PPTP - L2TP

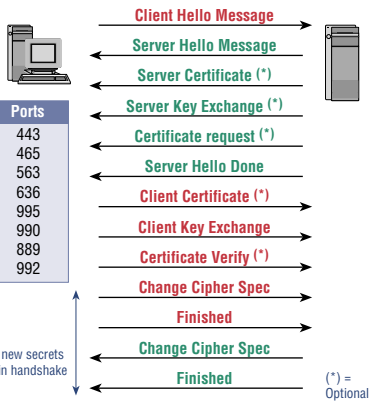


L2TP IN IPSEC (TRANSPORT MODE)



Goal: - user authentication
- user receives new network parameters

OVERVIEW OF TLS HANDSHAKE MESSAGES



Name	Ports
https	443
ssmtp	465
snntp	563
sldap	636
spop3	995
ftps	990
ftp-data	889
telnets	992

OPENSSL (COMMAND OVERVIEW)

Generating keys
openssl genrsa [-out filename] [-passout arg] [-des] [-des3] [-idea] [-f4] [-3] [-rand file(s)] [numbits]

Requesting a certificate
openssl req [-in filename] [-out filename] [-new] [-key filename] [-keyout filename] [-[md5|sha1|md2|mdc2]] [-config filename] [-subj arg] [-x509] [-days n] [-set_serial n] [-extensions section] [-reqexts section]

Generating a certificate
openssl x509 [-in filename] [-out filename] [-serial] [-hash] [-email] [-startdate] [-enddate] [-purpose] [-req] [-md2|-md5|-sha1|-mdc2] [-clrext] [-extfile filename] [-extensions section]

CA management
openssl ca [-gencrl] [-revoke file] [-crl_reason reason] [-crl_hold instruction] [-crldays days] [-days arg] [-md arg] [-cert file] [-selfsign] [-in file] [-out file] [-notext] [-outdir dir] [-infiles] [-extensions section] [-extfile section]

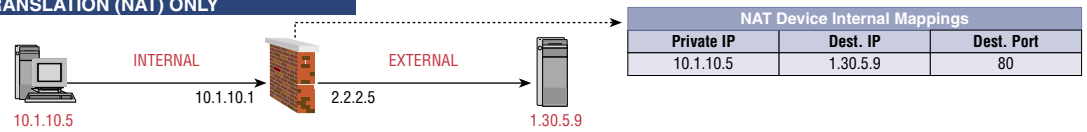
Encoding
openssl enc -ciphername [-in filename] [-out filename] [-pass arg] [-e] [-d] [-a] [-A] [-k password] [-kfile filename] [-K key] [-iv IV] [-p] [-P] [-bufsize number] [-nopad] [-debug]

SECURITY RELATED URLs

ICRI	http://www.law.kuleuven.ac.be/icri/
PacketStorm	http://www.packetstormsecurity.com/
SANS	http://www.sans.org
CVE database	http://cve.mitre.org
CERT	http://www.cert.org
SecurityFocus	http://www.securityfocus.com
Linux Security	http://www.linuxsecurity.com
NIST	http://csrc.ncsl.nist.gov
mailinglist overview	http://archives.neohapsis.com
BUGTRAQ Mailinglist	http://www.securityfocus.com
SECUNIA Mailinglist	http://www.secunia.co.uk
Sec. Resource Center	http://csrc.nist.gov/
COAST	http://www.cerias.purdue.edu/coast
IPtables	http://www.netfilter.org
Internet Storm Center	http://incidents.org
SNORT signatures updates	http://www.whitehats.com/ids/
Microsoft Security Downl.	http://www.microsoft.com/downloads
BCVG	http://www.ebcug.com/info.php
Newsgroups	comp.security.announce comp.os.linux.security comp.os.ms-windows.nt.admin.security

V1.0

NETWORK ADDRESS TRANSLATION (NAT) ONLY

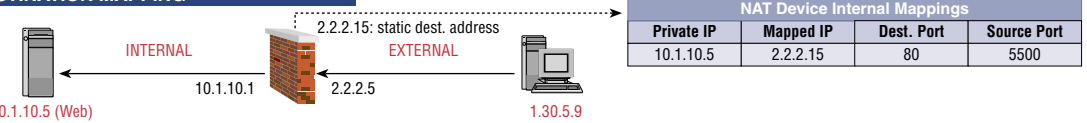


NAT Device Internal Mappings		
Private IP	Dest. IP	Dest. Port
10.1.10.5	1.30.5.9	80

Source IP 10.1.10.5	Dest. IP 1.30.5.9	Source Port 5500	Dest. Port 80	→	Source IP 2.2.2.5	Dest. IP 1.30.5.9	Source Port 5500	Dest. Port 80
Source IP 1.30.5.9	Dest. IP 10.1.10.5	Source Port 80	Dest. Port 5500	←	Source IP 1.30.5.9	Dest. IP 2.2.2.5	Source Port 80	Dest. Port 5500

STATIC SOURCE/DESTINATION MAPPING

- Static Source Mode NAT (1-1): Checkpoint
- Static Destination Mode NAT (1-1): Checkpoint
- Mapped IP: Netscreen

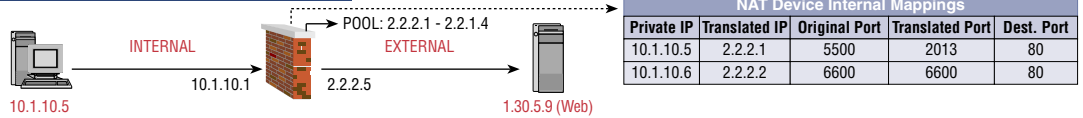


NAT Device Internal Mappings			
Private IP	Mapped IP	Dest. Port	Source Port
10.1.10.5	2.2.2.15	80	5500

Source IP 1.30.5.9	Dest. IP 2.2.2.15	Source Port 5500	Dest. Port 80	→	Dest. IP 1.30.5.9	Dest. IP 10.1.10.5	Source Port 5500	Dest. Port 80
Source IP 2.2.2.15	Dest. IP 1.30.5.9	Source Port 80	Dest. Port 5500	←	Source IP 10.1.10.5	Dest. IP 1.30.5.9	Source Port 80	Dest. Port 5500

MULTIPLE ADDRESSES TRANSLATED TO A POOL OF ADDRESSES

- Cisco: Static NAT
- Netscreen: DIP
- Linux: SNAT

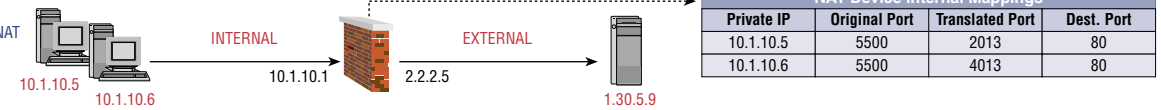


NAT Device Internal Mappings				
Private IP	Translated IP	Original Port	Translated Port	Dest. Port
10.1.10.5	2.2.2.1	5500	2013	80
10.1.10.6	2.2.2.2	6600	6600	80

Source IP 10.1.10.5	Dest. IP 1.30.5.9	Source Port 5500	Dest. Port 80	→	Source IP 2.2.2.1	Dest. IP 1.30.5.9	Source Port 2013	Dest. Port 80
Source IP 1.30.5.9	Dest. IP 10.1.10.5	Source Port 80	Dest. Port 5500	←	Source IP 1.30.5.9	Dest. IP 2.2.2.1	Source Port 80	Dest. Port 2013

NETWORK ADDRESS & PORT TRANSLATION

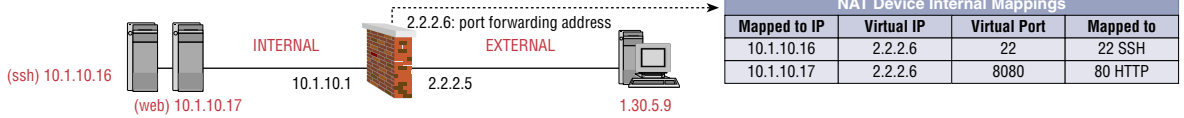
Linux: masquerading
Checkpoint: dynamic NAT/Hide Mode NAT
Netscreen: NAPT
Cisco: overloading



NAT Device Internal Mappings			
Private IP	Original Port	Translated Port	Dest. Port
10.1.10.5	5500	2013	80
10.1.10.6	5500	4013	80

Source IP 10.1.10.5	Dest. IP 1.30.5.9	Source Port 5500	Dest. Port 80	→	Source IP 2.2.2.5	Dest. IP 1.30.5.9	Source Port 2013	Dest. Port 80
Source IP 10.1.10.6	Dest. IP 1.30.5.9	Source Port 5500	Dest. Port 80	→	Source IP 2.2.2.5	Dest. IP 1.30.5.9	Source Port 4013	Dest. Port 80

PORT FORWARDING



NAT Device Internal Mappings			
Mapped to IP	Virtual IP	Virtual Port	Mapped to
10.1.10.16	2.2.2.6	22	22 SSH
10.1.10.17	2.2.2.6	8080	80 HTTP

Source IP 1.30.5.9	Dest. IP 10.1.10.16	Source Port 9483	Dest. Port 22	←	Source IP 1.30.5.9	Dest. IP 2.2.2.6	Source Port 9483	Dest. Port 22
Source IP 1.30.5.9	Dest. IP 10.1.10.17	Source Port 5098	Dest. Port 80	←	Source IP 1.30.5.9	Dest. IP 2.2.2.6	Source Port 5098	Dest. Port 80

X509 v3 CERTIFICATE

Signed By issuer

Version = 3
Serial Number
Algorithm Identifier (1)
Issuer (2)
Period of Validity
Subject (3)
Subject's Public Key (4)
Issuer Unique ID
Subject Unique ID
Extensions (5)
Signature

(1) O.ID for Digital signatures:
DSS SHA 2.16.840.1.101.22.1.1
RSA MD5 1.2.840.113549.1.1
(2) X.500 name (dn)
(3) X.500 name (dn) & email address
for rootCA-cert: issuer = subject
(4) Public Key Algorithm: rsaEncryption
RSA
- Public Key: (1024 bit)
- Modulus (1024 bit): .....
- Exponent: 65537 (0x10001) or 3

(5) Critical / non-critical
- Extensions to support CP's
  - Basic constraints extension
  - Policy Mapping extension
  - Policy Constraints extension
- Private extensions
- Extension to support indirect CRL
- Extension to support cert-chain building

X509 CRL FORMAT

Signed By issuer

Version
Signature (1)
Issuer (2)
This update
Next update
List of revoked certs (3)
...
...
...
Extensions (4)
Signature

(1) Algorithm ID (eg HMAC-MD5)
(2) Distinguished name of issuer
(3) Contains entries:
For every entry:
- Cert serial number
- Revocation date/time
- Optional: Per entry extensions

(4) Per CRL extensions
Per Entry: Reason code
Per CRL:
- Authority Key Identifier
- Issuer Alternative Name
- CRL serial nr
- Issuing Distribution Point (indirect CRL)
- Delta CRL Indicator

JOHN CORDIER ACADEMY

www.jcacademy.com

IP Security

reference card© v.2.0

telindus

Belgacom ICT