RSA
Rivest, Shamir, Adelman
Key Generation
two large prime numbers, third coprime
Key Distribution
each side sends own public key
all traffic is encrypted with public key
all traffic is decrypted with private key
RC4 (Rivest Code 4)
array (S) up to 256B, two integers
KSA - Key Scheduling Algorithm
LFSR - Linear Feedback Shift Register
weak - separation of nonce and key
use for WEP, SSL, RDP, SSH
MD5 (Message Digest 5)
Cryptographic hashing function
any input → 128b/16B hex output
the input is divided to fixed-len blocks
padding to be divisible with 512
hash → data integrity, one-way hash
SHA (Secure Hash Algorithm)
created by NIST
SHA-0, SHA-1 (160b), SHA-2 (256b)
DES (Data Encryption Standard)
IBM - Lucifer code, then NIST/NSA → DES
64b input → OPER → 64b output
1998 - DES Cracker, break within 3 days
3DES
no additional investments for DES support
encrypt, decrypt, encrypt
3 diff keys can be used (if 1 key = DES)
temp solution between DES and AES
AES (Advanced Encryption Standard)
FIPS 197, 2001, Rijndael Algorithm
3 diff keys - 128, 192 and 256
low memory reqs, using wireless often
IPSec
RFC 2401, RFC 2402 (AH), RFC 2046 (ESP)
2 phases - 1.ISAKMP, 2.IPSec
AH (Auth Header), ESP (Enc Sec Payload)
Tunnel vs. Transport mode
SA (Security Association)
unidirectional relationship between 2 nodes
auth, integr, AH vs. ESP
SPI (Sec Parameter Index)
ISAKMP/IKE
ISAKMP - Inet Sec Assoc and Key Mngt Prot
IKE - Internet Key Exchange
ISAKMP, SKEME, Oakley
ISAKMP → frame format for key exchange
IKE → the content of above frames
ISAKMP - DOI, Situation and Proposal
Phases
IKE 1 → securing the channel
creates SA, bidir communication
Modes - main (6msg) and aggressive (3m)
Auth - PSK, RSA, DSS
IKE 2 → Quick Mode
2 unidir SAs, hash from Phase 1
IKE Extension → NAT-Traversal, XAuth
IKEv2
native support of NAT-T, Mobiity
3 messages only
DPD, DoS attack resilience
GDOI
Group Domain of Interpretation
based on ISAKMP, hub-and-spoke
group-policy, RSA-2048
TEK - Traffic Authentication Key
encryption of data plane
KEK - Key Encrypting Key
encryption of control plane

AH (Authentication Header)
Authentication, Data Origin Authentication
HMAC-MD5-96 → 512b blocks, XOR
IP protocol 51
ESP (Encapsulating Security Payload)
AH + confidentiality
All the inner headers are encrypted
IP protocol 50
Simple Cert Enrollment Protocol (SCEP)
Dig Certs as scalable as possible
Requestor → IPSec client
SCEP SA
SSL/TLS/
created by Netscape, v1 never published
symmetric cryptography system, on top TCP
public key, random S - pre-master secret
master secret K, Session Resumption
client auth - server sends auth msg to client
Exportability, Encoding
Message Auth Check - loss prevention
TLS Handshake and Record Protocol
DTLS (Datagram TLS)
stream oriented TLS
no delays, need of reordering, loss prevent
SSH
secure channel client-server
telnet replacement
TCP/22, public key cryptography
password, public/private key
SSH, SCP, RSH, RSYNC, SFTP...
v1, v2, v1.99
RADIUS
Remote Auth Dial-In User Services
over UDP
Access-request, Access-reject, Access-accept, Access-chalenge
same for accounting
legacy ports 1645/1646
new ports 1812/1813
TACACS+
Termi Access Control Access Control Sys
Cisco proprietary, TCP/UDP 49
all data are encrypted
support of PAP/CHAP
LDAP
Lightweight Directory Access Protocol
Device authentication, directory services
over TCP, more see Section 1
EAP
Extensible Authentication Protocol
Authentication framework
EAP-MD5
easy to deploy, open standard, not so secure
uses MD5 challenge, not mutual auth
EAP-TLS
Developed by MS, open standard
per packet confidentiality and integrity
mutual auth, need of certificate (client/server)
EAP-TTLS
as EAP-TLS but not needed certificate on client
EAP-FAST
Flexible Auth via Secure Tunneling
developed by Cisco, addresses the issue of LEAP
TLS tunnel, no PKI
shared secret key → PAC
2 phases
Phase 1 - mutual auth and creates TLS tunnel
Phase 2 - cred exchange via protected tunnel
PEAP
protected EAP,developed by Cisco+MS+RSA
outer TLS tunnel, inner tunnel - any type
PEAPv0 - EAP-MSCHAPv2
PEAPv1 - EAP-GTC
LEAP
Lightweight EAP
Cisco proprietary,WLAN method
mutual auth, vulnerable to dict attack
PKI
Public Key Infrastructure
provides digital certificate
Cert - bind pub key to identity
CA - Certificate Authority
RA - Registration Authority
Directory Services
CRL - Certification Revocation List
SCEP
Certificate enrollment
802.1x
authentication framework for wire/less net
using EAP on the MAC layer - via PPP/IEEE 802
Supplicant (client) - send request
Authenticator (Switch/AP) - fwd req to RADIUS
Authentication Server - RADIUS Server
Port states
authorized → granted access, fwd packets
unauthorized → dropping traffic
MAB, Guest Portal, Redirecting traffic
WEP, WPA, WPA2
seesection 1
WCCP
Web Cache Communication Protocol
Cisco proprietary
web cache proxy - transparent, forward
WCCPv1 - TCP/80, GRE encaps, no pswd
WCCPv2 - TCP/UDP, adds MD5 pswd
Redirection
L2 - same L2 subnet, direct forwarding
GRE - different subnet, GRE betw IOS and WSA
SXP
Cisco SGT Exchange Protocol
SGT → Security Group Tag
part of TrustSec solution
Authentication
Group-based access control
Data encryption
EAP + 802.1X + Radius server
using SGT (16b) to identify the TrustSec domain
SXP - protocol for propagating IP-to-SGT
DHCP Snooping, IP Device Tracking
TCP/64999, MD5 for authentication
MACSec
802.1AE - auth + encryption of L2 traffic
Security Tag - EtherType extension
utilizing 802.1x and Radius server to operate
MKA - MACSec Key Agreement
discovers the MACSec peers and exchg keys
DNSSec
IETF std, security extension to DNS
against DNS based attacks, e.g. DNS Poisoning
using digital signatures for DNS communication
DNS Root zone - public key (chain of trust)
Key mngmt - key rollover, KSK - key signing keys