UNIK4250 Security in Distributed Systems
UNIK University Graduate Center
Spring 2012

Lecture 9
IP Security

Leif Nilsen

Outline

- IPSec
- IKEv2
- TCE 621

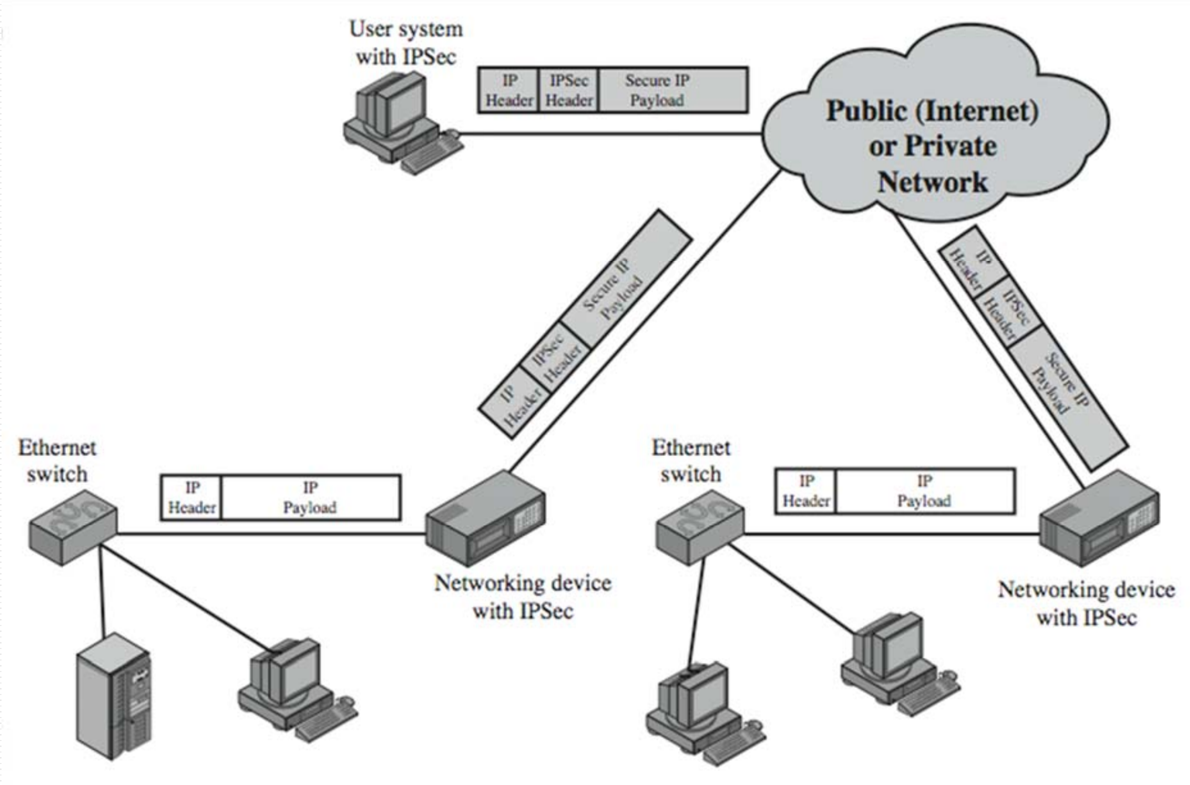
IP Security

- have a range of application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IP Security

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet
- need identified in 1994 report
  - need authentication, encryption in IPv4 & IPv6

IP Security Uses



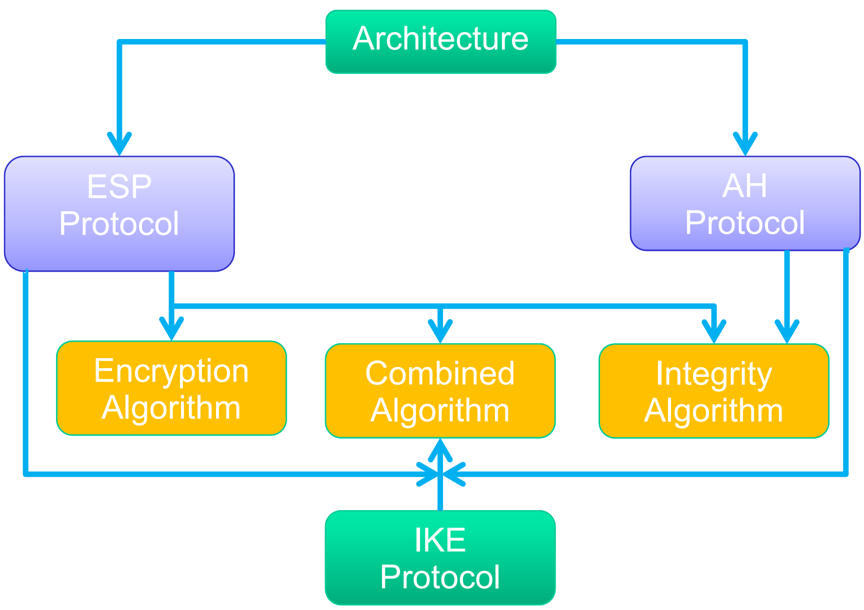
Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

IP Security Architecture

- specification is quite complex, with groups:
  - Architecture (IPsec version 3)
    - RFC4301 *Security Architecture for Internet Protocol*
  - Authentication Header (AH)
    - RFC4302 *IP Authentication Header*
  - Encapsulating Security Payload (ESP)
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - Internet Key Exchange (IKE)
    - RFC5996 *Internet Key Exchange (IKEv2) Protocol*
    - *NOTE – Replaces RFC4306 and RFC4718*
  - Cryptographic algorithms
  - Other

IPSEC/IKE Document Interrelationships



IPSEC Specification Roadmap

- RFC 6071 IP Security (Ipsec) and Internet Key Exchange (IKE) Document Roadmap
  – 63 pages
  – Discuss approx 100 different RFCs that may have an impact on IPsec implementations!

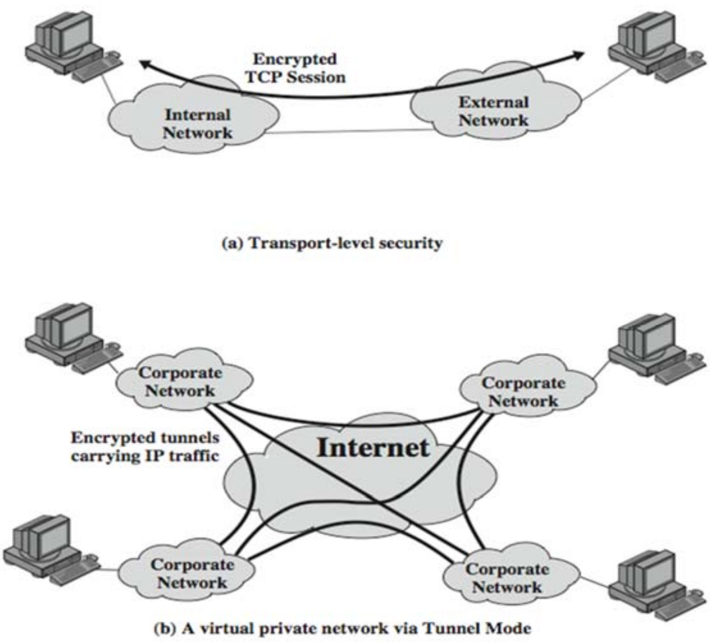
IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  – a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

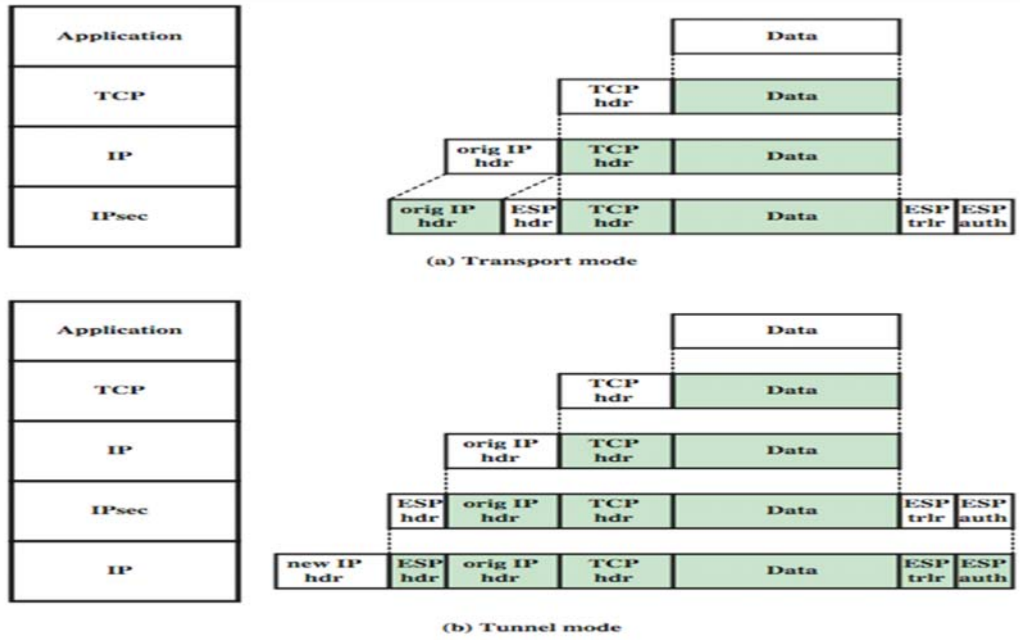
Transport and Tunnel Modes

- Transport Mode
  - to encrypt & optionally authenticate IP data
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- Tunnel Mode
  - encrypts entire IP packet
  - add new header for next hop
  - no routers on way can examine inner IP header
  - good for VPNs, gateway to gateway security

Transport and Tunnel Modes



Transport and Tunnel Mode Protocols



Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

Security Policy Database

- relates IP traffic to specific SAs
  - match subset of IP traffic to relevant SA
  - use selectors to filter outgoing traffic to map
  - based on: local & remote IP addresses, next layer protocol, name, local & remote ports

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Encapsulating Security Payload (ESP)

- provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality
- services depend on options selected when establish Security Association (SA), net location
- can use a variety of encryption & authentication algorithms

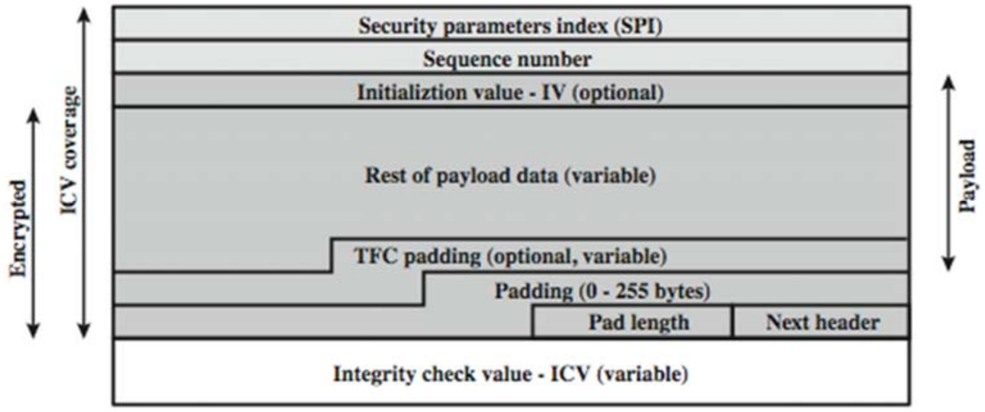
Encryption & Authentication Algorithms & Padding

- ESP can encrypt payload data, padding, pad length, and next header fields
  - if needed have IV at start of payload data
- ESP can have optional ICV for integrity
  - is computed after encryption is performed
- ESP uses padding
  - to expand plaintext to required length
  - to align pad length and next header fields
  - to provide partial traffic flow confidentiality

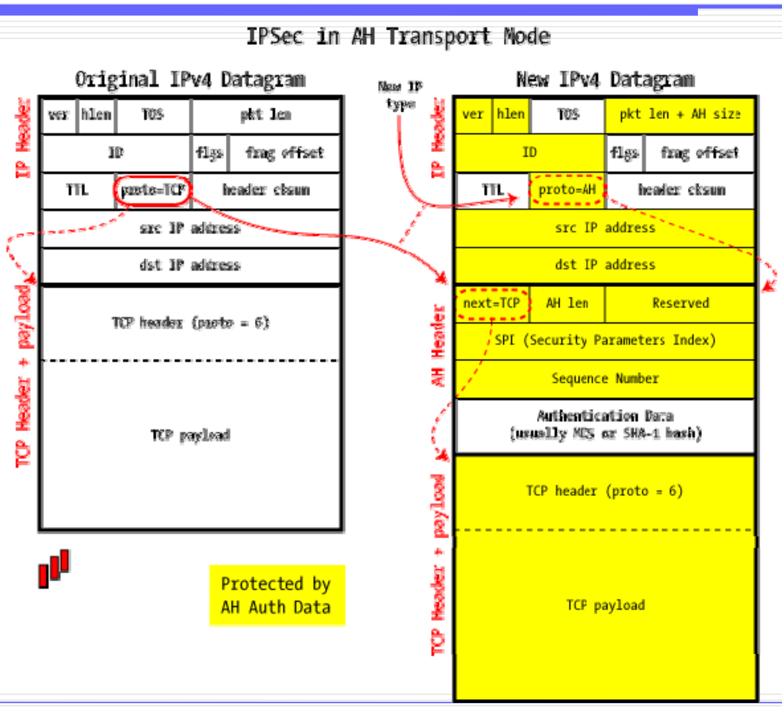
Anti-Replay Service

- replay is when attacker resends a copy of an authenticated packet
- use sequence number to thwart this attack
- sender initializes sequence number to 0 when a new SA is established
  - increment for each packet
  - must not exceed limit of $2^{32} – 1$
- receiver then accepts packets with seq no within window of ($N – W+1$)

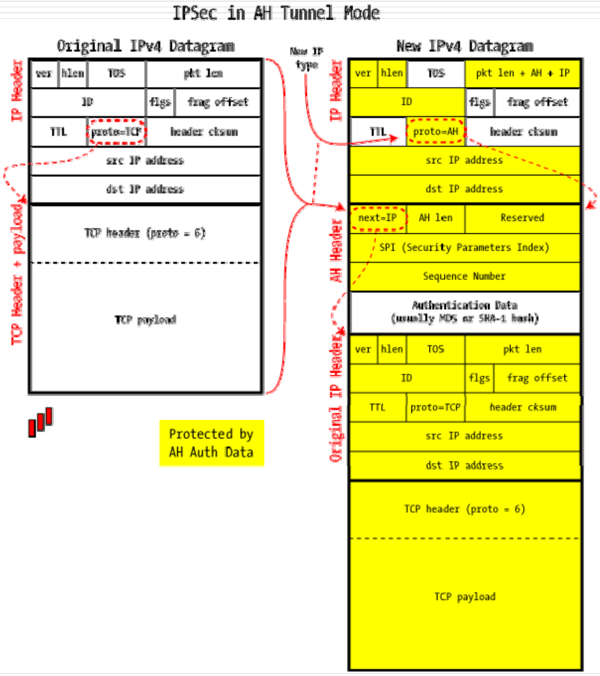
Encapsulating Security Payload



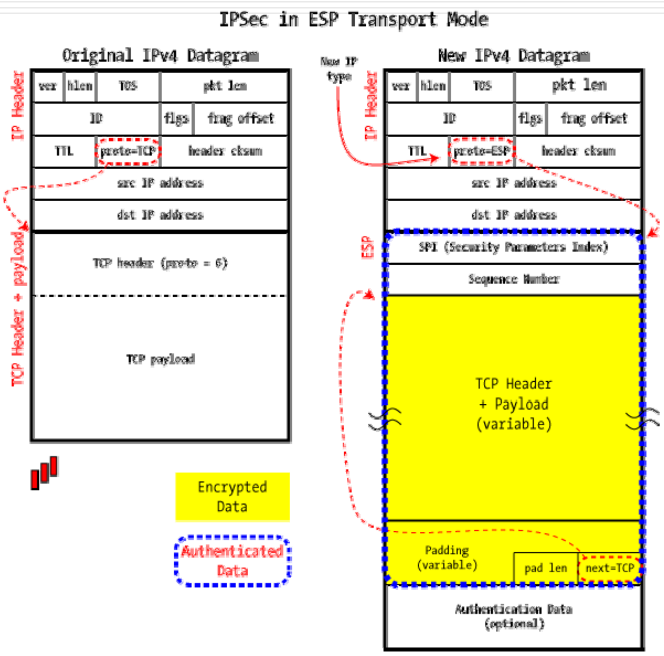
AH – Transport mode



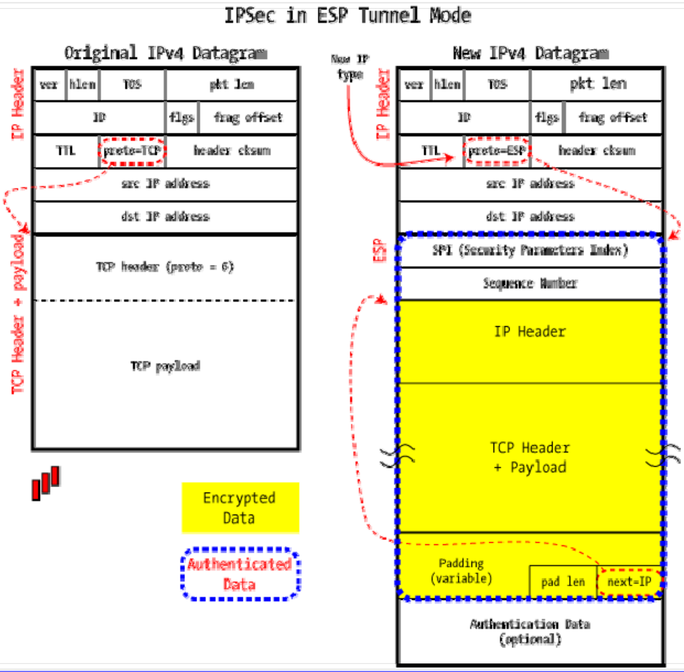
AH – Tunnel mode



ESP – Transport mode



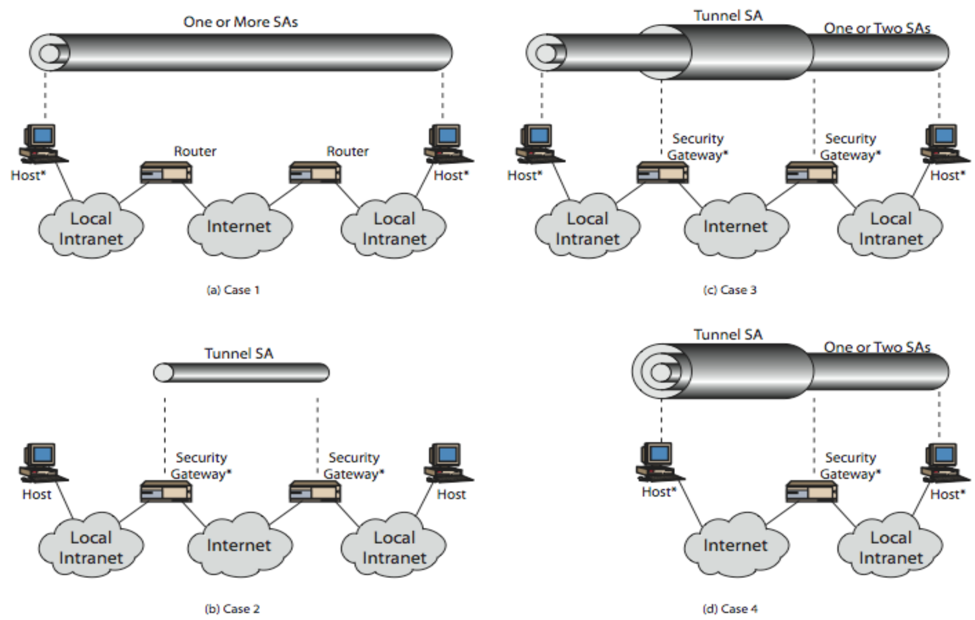
ESP – Tunnel mode



Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - transport adjacency
    - iterated tunneling
- combining authentication & encryption
  - ESP with authentication, bundled inner ESP & outer AH, bundled inner transport & outer ESP

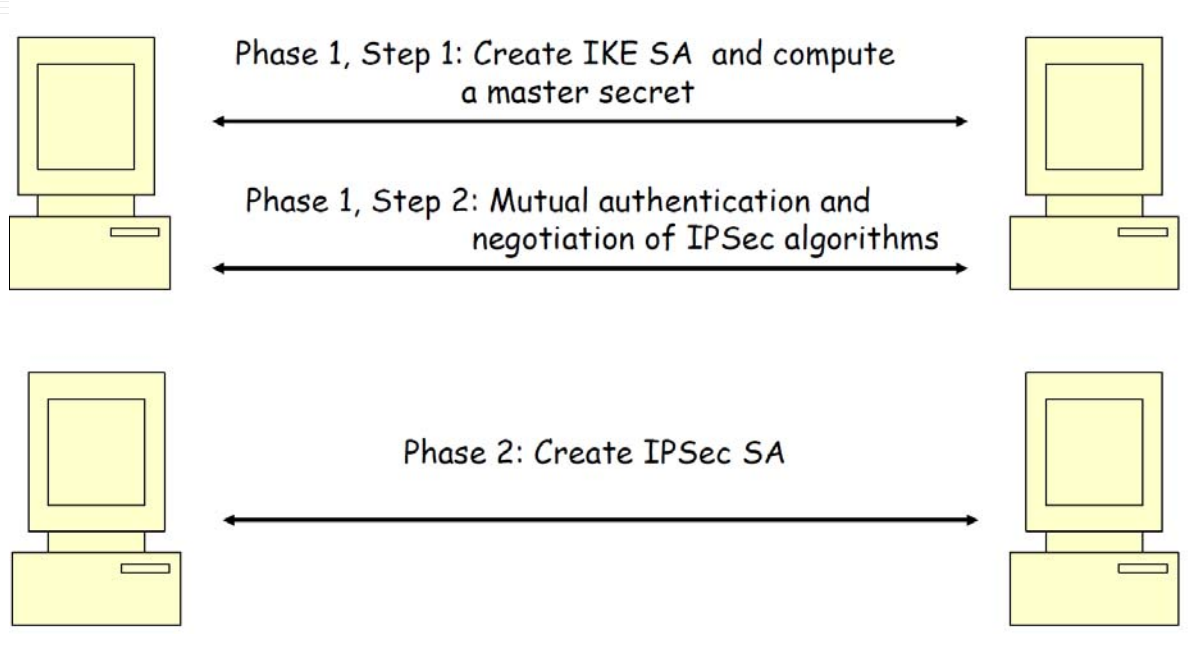
Combining Security Associations



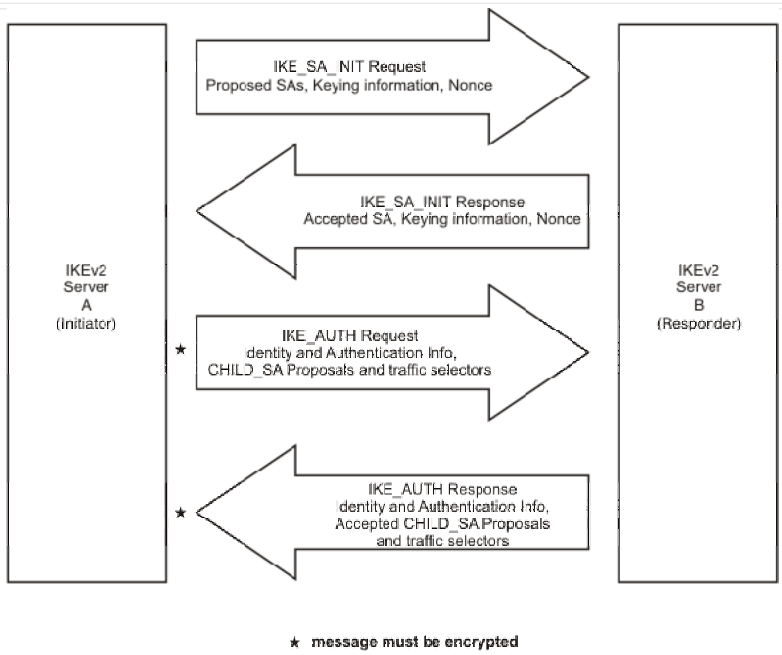
IPSec Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements (legacy protocols – replaced by IKEv1 and IKEv2)

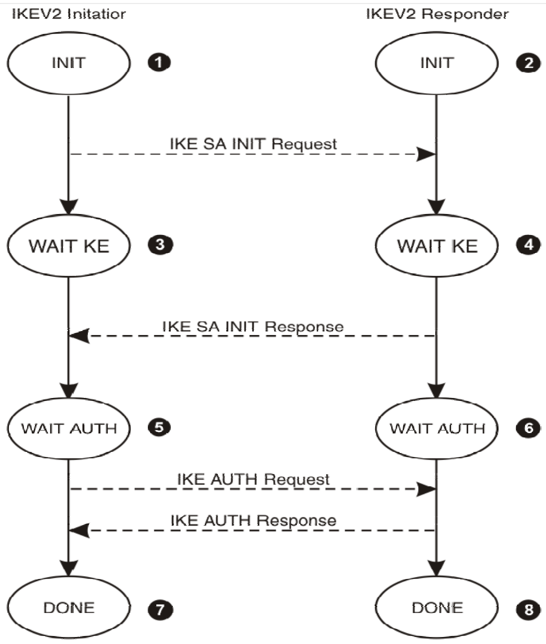
IKE main steps



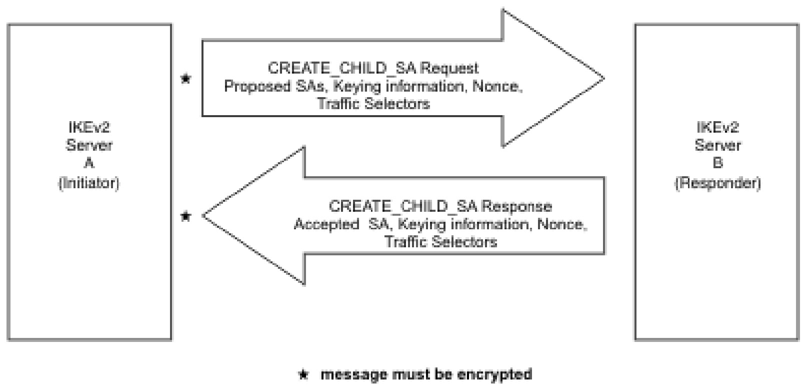
IKE phase 1



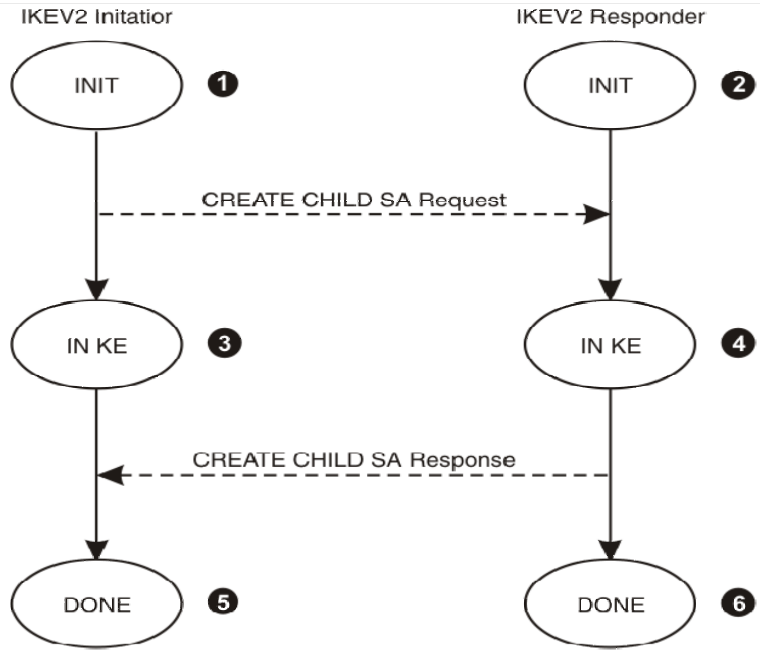
IKE phase 1



IKE phase 2



IKE phase 2



IKEv2 protocol

- Phase 1, Step 1: IKE_SA_INIT
  - Negotiate IKE algorithms
  - Compute secret keys for IKE
  - Compute master secret k_d for computing IPSec keys in Phase 2.
- Phase 1, Step 2: IKE_AUTH
  - Mutual authentications
  - Negotiation of IPsec algorithms (piggybacked here)
- Phase 2: CREATE_CHILD_SA
  - Setup AH or ESP security associations

Phase 1.1: IKE_SA_INIT (1)

Initiator | Responder

HDR, SAi1, KEi, Ni →

← HDR, SAr1, KEr, Nr, [CERTREQ]

- HDR (IKE header)
  - Version number
  - SPIi: A value chosen by the initiator to identify this IKE security association.
  - ……
- SAi1
  - Supported Crypto algms of initiator for the IKE_SA (DH group, encrpt, authen algor for protecting the messages in Phase 1.2 and Phase 2)
- KEx
  - Diffie-Hellman Values
- Nx
  - Nonce of Initiator/Responder
- SAr1
  - Expressed the choice based on SAi1
- [CERTREQ]
  - Optional request preferred CA

Phase 1.1: IKE_SA_INIT (2)

- After this two messages, each party can generate SKEYSEED based on the values in KEi and KEr by DH
  - SKEYSEED=prf(Ni | Nr, g^(s_is_r)) [Remark: s_i the secret of I]

    Nonces add the freshness to the key materials.
  - {SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr } = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr)

    The prefix of output of the function prf+ is cut into pieces as different keys
- SK_d is the master secret that will be used to compute IPSec SA keys later in Phase 2.
- Following messages in Phase 1.2 will be encrypted and integrity protected by SK_ai, SK_ei, SK_ar, SK_er respect.
- SK_pi and SK_pr are pre-shared secret keys for authentication in Phase 1.2 (technical details of this authentication method is omitted here. We will introduce the authentication using digital certificate next only).

Phase 1.2: IKE_AUTH (1)

Initiator | Responder

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr} →

← HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

- {...}
  - indicated payloads are encrypted and integrity protected using that direction's SK_e & SK_a and the IKE encryption and auth algorithms
- IDi, IDr
  - For auth based on preshared secrets SK_pi, SK_pr (details omitted)
- Auth
  - Preshared secrets (SK_pi, SK_pr) + ID
  - Digital certificates
- SAi2/SAr2 piggybacked here
  - For CREATE_CHILD_SA
- TS
  - Traffic Selector Info (IP Add + Port)
  - It defines which traffic to be protected by SAi2, SAr2
  - It contains protocol, port range, address range
  - TSi = (0, 0-65535,192.0.2.202-192.0.2.202)
  - TSr = (0, 0-65535,192.0.2.0-192.0.2.255)

The Whole Picture of Phase 1

Initiator | Responder

HDR, SAi1, KEi, Ni →

← HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr} →

← HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

Remark 1: [CERTREQ] means authentication with digital certificate.
Remark 2: "SK{}" means encryption using the keys sk_{ei} and sk_{er} .
Remark 2: SAi2 and SAr2 are negotiations of IPSec SA algorithms, piggybacked in this authentication step.

Mutual Authent. by AUTH (2)

- Two Authentication Methods
  - Digital Signature Based
    - Requires individual [CERT] exist in both messages
    - [CERTREQ] indicates to us certificate authentication
    - Initiator signs the 1 st message appended by Nr and prf(SKai,IDi)
    - Responder signs the 2 nd message appended by Ni and prf(SKar,IDr)
  - Pre-shared Key (SK_pi, SK_pr)
    - HMAC using negotiated prf function
    - AUTH = prf(prf(Shared Secret, "Key Pad for IKEv2"), <msgoctets>)

CHILD_SA Negotiations in IKE_AUTH

- Establishment of CHILD_SA is piggybacked in IKE_AUTH
- Initiator proposes SAi2 in message 3
- Responder answers SAr2 in message 4
- Traffic protected by the SA is also negotiated through traffic selectors (TSi, TSr)

Phase 2: CREATE_CHILD_SA

Initiator | Responder

HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]} →

← HDR, SK {SA, Nr, [KEr], [TSi, TSr]}

- [N]: Indication negotiation of new IPSec SA
- [KEx]
  - Diffie-Hellman value, different from those in Phase 1.1
  - Used only when PFS is required. In this case, they will be used in computing new IPSec keys
- [TSx]
  - Traffic Selector Negotiations for new IPSec SA
  - Used only when [N] is used
- If [N] is not used, this is the 1st IPSec SA creation under this IKE SA
- The protection SK{} here is by the IKE SA negotiated before.
- Ni and Nr should be different from those in Phase 1.1.

- An established IKE SA may be used to create many IPSec SAs and may be used for a long time.
- A set of IPSec algorithms was already negotiated in Phase 1.2. However, if a new IPSec SA should be created, then [N] is used to indicate this. At the same time, new [KEi] and [TSi, TSr] (different from those in Phase 1.2) may be negotiated.
- The Ni and Nr here are different from those in Phase 1.1, and will be used to compute IPSec secret keys.

Finally, Keys for AH or ESP

- After CREATE_CHILD_SA, the key(s) for AH or ESP will be generated!
- KEYMAT = prf+(SK_d, Ni | Nr)
  – Ni and Nr are the new nonces in Phase 2
- For stronger PFS
  – KEYMAT = prf+(SK_d, g^(s_i s_r) (new) | Ni | Nr),
  – Where s_i and s_r are the new DH values in Phase 2, SK_d is the old one Phase 1, Ni and Nr are new ones in Phase 2.
- 160-bit prt+ is used twice for generating 256-bit Key for AES

Re-keying

- Secret keys of IKE, ESP and AH should be only used in a limited of time.
- After SA lifetime expires, re-keying has to be done.
- Either side thinks an SA has been enough time, it negotiates a new SA.
- After the new SA is setup, delete the old one.

IKE Payloads & Exchanges

- have a number of payload types:
  – Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- payload has complex hierarchical structure
- may contain multiple proposals, with multiple protocols & multiple transforms

Cryptographic Suites

- variety of cryptographic algorithm types
- to promote interoperability have
  - RFC4308 defines VPN cryptographic suites
    - VPN-A matches common corporate VPN security using 3DES & HMAC
    - VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - provide choices for ESP & IKE
    - AES-GCM, AES-CBC, HMAC-SHA, ECDH, ECDSA

How many keys are needed?

- SK_ei and Sk_ai - *Used by initiator for encryption and authentication of IKE messages*
- SK_er and Sk_ar - *Used by responder for encryption and authentication of IKE messages*
- SK_pr and Sk_pr - *Used when generating an AUTH payload*
- SK_d – *Used for derivation of further keying material for Child SAs*

In total 7 keys are needed

Pseudo-Random Function (PRF)

- PRF function takes a variable length key, variable length data, and produces a fixed length output n e.g. slightly modified HMAC
- For generating keying material and authentication of IKE
- In RFC4307: Recommended PRF
- PRF_HMAC_SHA1 MUST RFC2104
- PRF_HMAC_MD5 MAY RFC2104
- PRF_AES128_CBC SHOULD+ AES-PRF

Derivation of key material – PRF+

- prf+ (K,S) = T1 , T2 , T3 , T4 , ...
- where:
- T1 = prf (K, S | 0x01)
- T2 = prf (K, T1 | S | 0x02)
- T3 = prf (K, T2 | S | 0x03)
- T4 = prf (K, T3 | S | 0x04)

- where
- | means concatenation
- 0x01 etc. are constants
- A number of Ti's are computed iteratively as needed

Generating Keying Material for Child SAs

- A single Child SA is created by the IKE_AUTH exchange, and additional Child SAs can optionally be created in CREATE_CHILD_SA exchanges.
- Keying material for them is generated as follows:
  – KEYMAT = prf+(SK_d, Ni | Nr)
  – Where Ni and Nr are the nonces from the IKE_SA_INIT exchange if this request is the first Child SA created or the fresh Ni and Nr from the CREATE_CHILD_SA exchange if this is a subsequent creation.

IKEv2 exchange types

RFC5996

Value	Exchange Type	Reference
0-33	Reserved	[RFC5996]
34	IKE_SA_INIT	[RFC5996]
35	IKE_AUTH	[RFC5996]
36	CREATE_CHILD_SA	[RFC5996]
37	INFORMATIONAL	[RFC5996]
38	IKE_SESSION_RESUME	[RFC5723]
39-239	Unassigned	
240-255	Private use	[RFC5996]

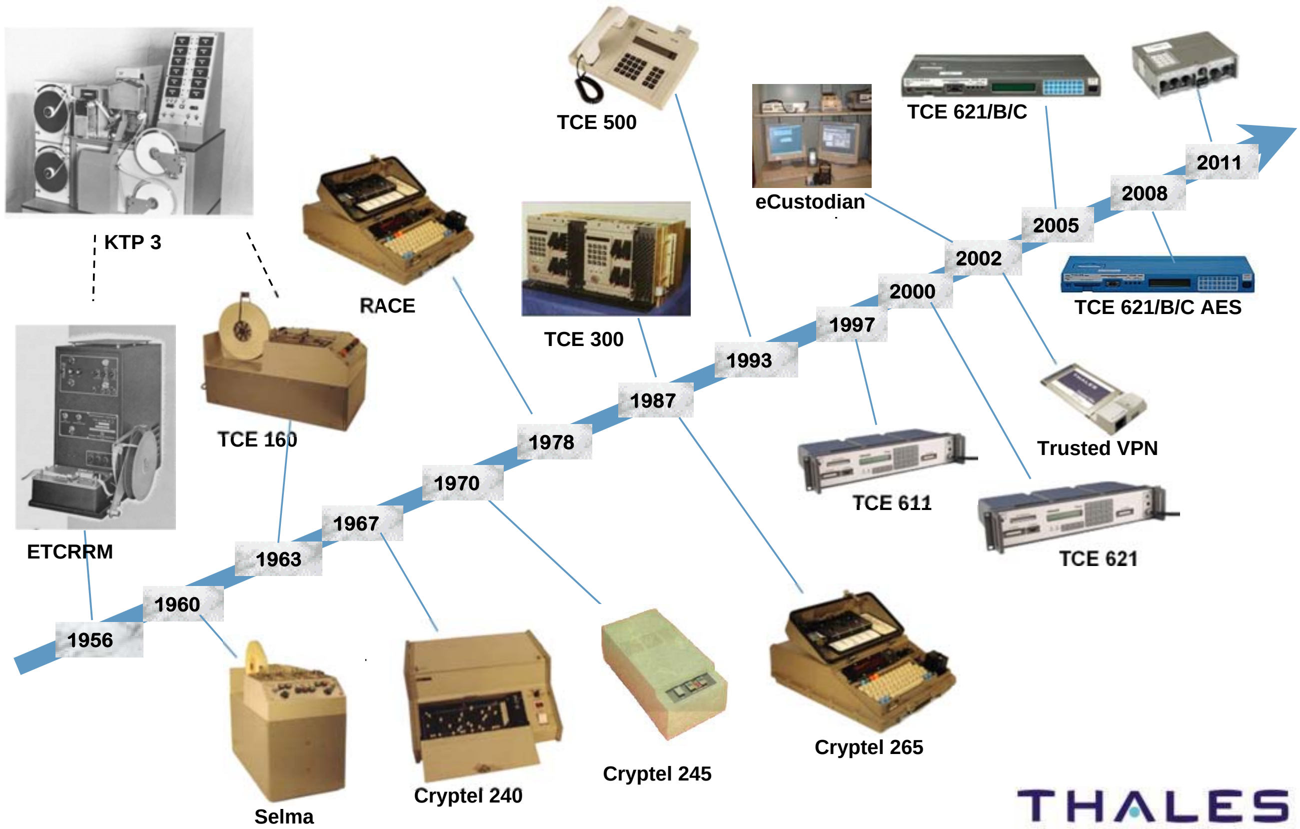
IKEv2 DH-groups

Number	Name	Reference
0	NONE	[RFC5996]
1	Group 1 - 768-bit MODP Group	[RFC5996]
2	Group 2 - 1024-bit MODP Group	[RFC5996]
3-4	Reserved	[RFC5996]
5	1536-bit MODP Group	[RFC3526]
6-13	Unassigned	[RFC5996]
14	2048-bit MODP Group	[RFC3526]
15	3072-bit MODP Group	[RFC3526]
16	4096-bit MODP Group	[RFC3526]
17	6144-bit MODP Group	[RFC3526]
18	8192-bit MODP Group	[RFC3526]
19	256-bit random ECP group	[RFC5903]
20	384-bit random ECP group	[RFC5903]
21	521-bit random ECP group	[RFC5903]
22	1024-bit MODP Group with 160-bit Prime Order Subgroup	[RFC5114]
23	2048-bit MODP Group with 224-bit Prime Order Subgroup	[RFC5114]
24	2048-bit MODP Group with 256-bit Prime Order Subgroup	[RFC5114]
25	192-bit Random ECP Group	[RFC5114]
26	224-bit Random ECP Group	[RFC5114]
27-1023	Unassigned	
1024-65535	Private use	[RFC5996]

Derivation of keys using ECDH

- ..\..\..\..\OldDisk\Mathematica\ecdh_demo.nb

60 years of experience



THALES

Cryptel®-IP – References

National use of Cryptel-IP components

- **Various ministries**
  - Defence, Interior, Foreign affairs, Justice etc
- **Defence forces**
  - Army, Navy, Air Force, Special operation forces
- **Material commands, Intelligence services**
- **Rack mounting, communication modules, tracked vehicles, ships, airplanes etc.**

Government-to-government sales only

THALES

Cryptel®-IP users

Germany, Netherlands, France, Norway, Denmark, Czech R, Canada, Poland, UK, Belgium, Italy, Hungary, USA, Greece, Slovenia, Slovakia, Latvia, Estonia, Albania, Lithuania, Eurocorps, Portugal, Spain, Luxembourg, Turkey

NATO users
- SHEDCOINS
- NNCCRS
- NGCS-PTC
- Afghan MN
- 1st,2nd and 3rd signal battalion
- LINC/DCIS
- SACEURs VTC

NATO bodies
- NC3A
- BICES (NBA)
- NAMSA
- NACMA
- NAPMO

Operations
- ISAF
- NRF
- KFOR/SFOR
- Iraq

Partners
- Eurocorps
- EUFOR

+ national use in 25 countries

THALES

A complete family of products

Products			Algorithms and Accreditation levels: TCE 621	Algorithms and Accreditation levels: TCE 621 AES
TCE 621/C	600 Mbit/s	**For fixed networks in controlled environment**	Cosmic Top Secret	NATO Secret
TCE 621/Z	600 Mbit/s	**For fixed networks in less controlled environment**		NATO Secret
TCE 621/M	30 Mbit/s	**For mobile networks**	NATO Secret	NATO Secret
TCE 671	-	**For management of TCE 621s in networks**	Cosmic Top Secret	NATO Secret

Approvals

- **TCE 621/C:** CTS
- **TCE 621/C AES:** NATO Secret
- **TCE 621/Z:** Under evaluation for Hemmelig – expected 4Q11
- **TCE 621/M:** Hemmelig – NATO Secret expected 4Q11
- **TCE 621/M AES:** Under evaluation for Hemmelig – expected 4Q11

THALES

General security features

Electronic and/or manual key distribution

Manual key distribution on

- SMART cards
- Paper tape (KOI-18)
- Data Transfer Device (DTD)

Tamper protected case

- Content erased when opened

Tempest approved

- According to SDIP 27 level A

NATO approved crypto algorithms

- Secret and/or public algorithm

THALES

General features

Low latency – well suited for

- VoIP
- Video conferencing

No session setup time

- Once configured, always configured
- Crypto system is self synchronising

No or little management traffic

- Dependant on operating mode and configuration

System is flexible and scalable

- From 2 units in manual mode to 1000 units in automatic mode

Easy installation and configuration

- Enter configuration data
- Enter keys for use with SMC

Run-time operation

- No day-to-day operation necessary
  - Unless necessary to declassify unit by removing CIK
  - Personal activation when configured
- Keys for use with SMC loaded at regular intervals

THALES

Cryptel®-IP technical features

Functional features

- **Supports both IPv4 and IPv6**
- **Quality of Service**
  - TOS-byte transferred
- **Redundancy**
  - Based on VRRP
  - Hot standby on device level
- **Multicast**
  - Based on IGMP
- **UDP encapsulation**
  - NAT and firewall traversing
- **SW update**
  - Remote as well as locally
- **Configurable ICMP/SNMP support**
  - Monitoring possible
  - Traps to network management centre

THALES

TCE 621/C – Features

Infrastructure IP encryption device

- **High capacity**
- **Redundant, multicast**
- **External power source**
  - 110 / 220 VAC

Designed for rack mounting

- **Invisible for end users**

Removable crypto ignition key

- **Declassified when removed**


TCE 621/C


TCE 621/C AES


TCE 621 Black

Fast and reliable high grade IP encryption

THALES

TCE 621/M – Features

Miniature IP encryption device

- Pocket size (160x120x44mm)
- Two activation modes
  - Personal code or
  - CIK only
- External power source (10-30 VDC)

Designed for rough use

- Water proof, submersible down to 10 meters
- Extended temperature range
- Shock, vibration, etc.
- No light or sound emission
- Low EMC profile

Small, lightweight and robust high grade IP encryption

THALES

TCE 621/M operational modes

Traditional operation

- Traffic enabled when CIK is inserted
  - Functionality as of TCE 621/A, /B and /C
  - Default configuration also in TCE 621/M
- Suitable in controlled area

Personal use

- User must authenticate to enable traffic
  - Insert CIK and enter PIN at regular intervals
    - Interval is configurable
    - Length of PIN is configurable
  - Warning before period expires (LED-blink)
- TCE 621/M kept under personal control
  - CIK should be kept separately as a security measure

TCE 621/M designed to be used outside controlled area

THALES

TCE 671 – Security Management Centre

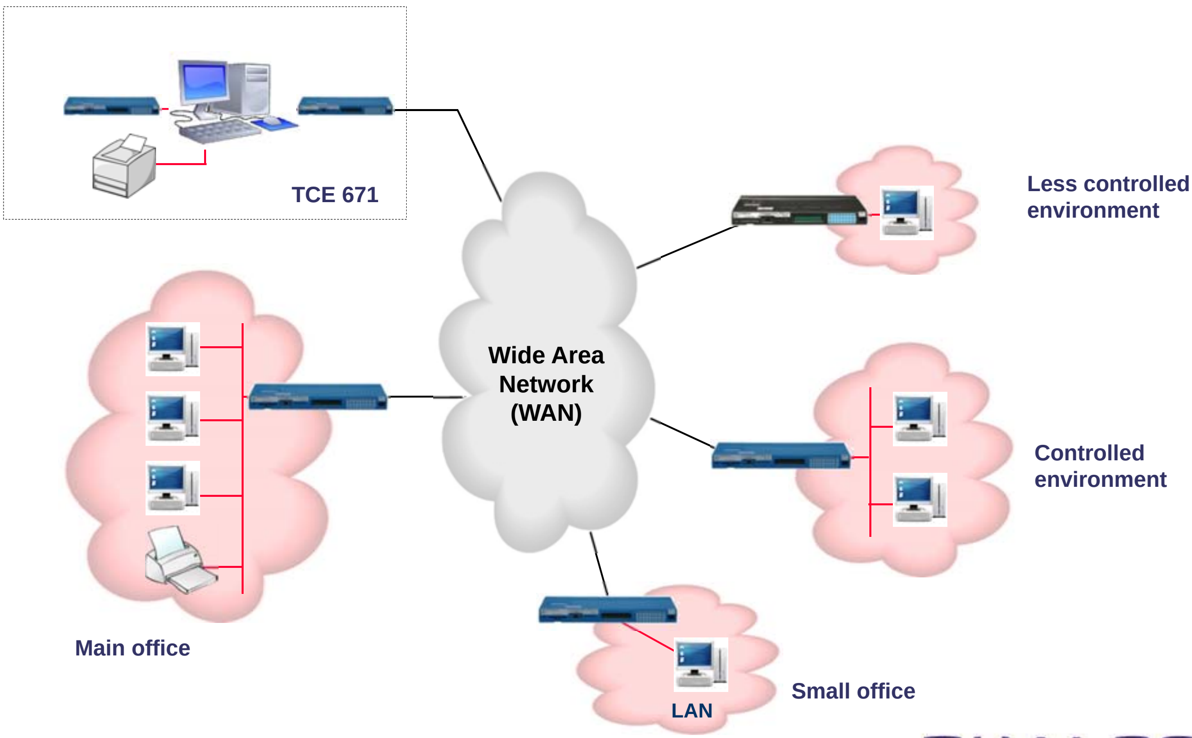
Main features:

- **Key Management including Electronic Key Distribution (EKD)**
  - Loading of keys from fill device
    - Including import of keys from an offline system
  - Local generation of keys
- **Management of Access Control Information**
- **System Monitoring (Audit functions)**
- **General Systems Management**

Manages all variants of the TCE 621

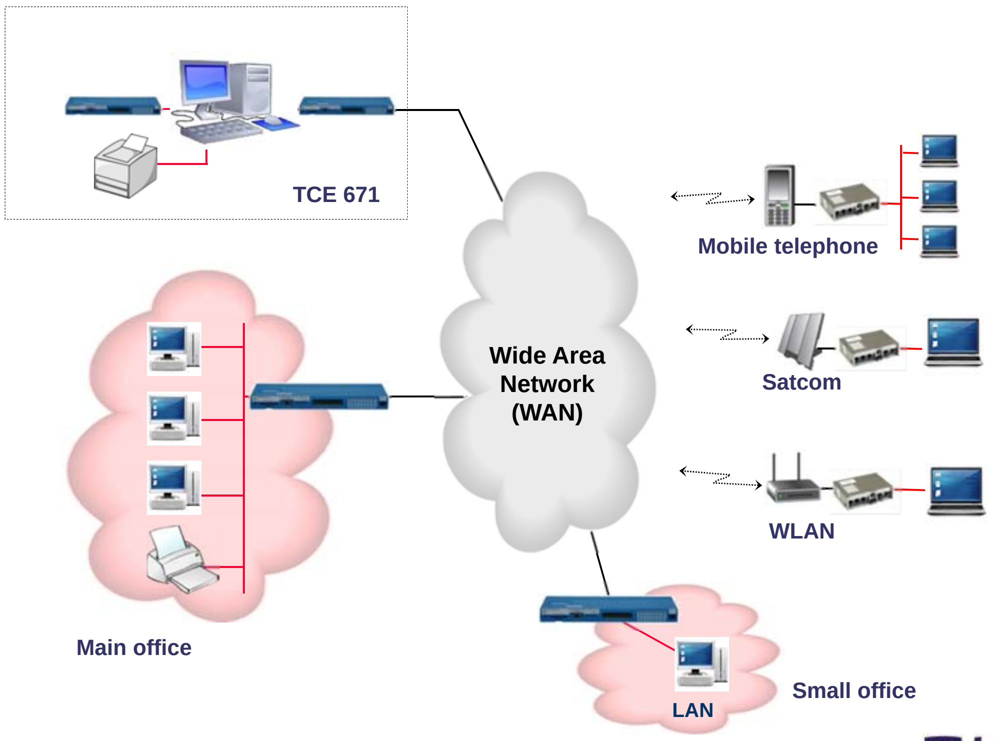
THALES

Cryptel®-IP in fixed networks



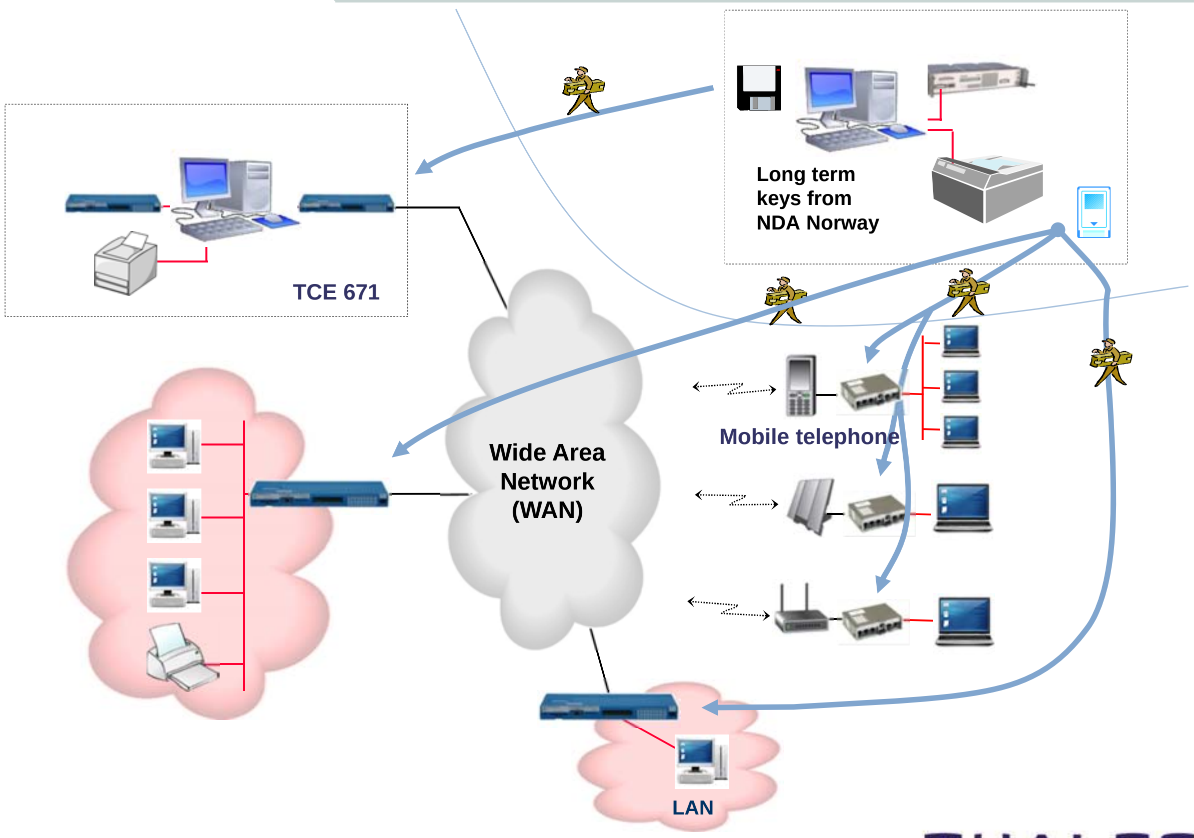
THALES

Cryptel®-IP in mobile networks



THALES

Cryptel®-IP key distribution



THALES

Key Generation Centre

Main features:

- **Offline key production for Cryptel®-IP**
- **Distribution based on**
  - Smart card and
  - Floppy
- **Dedicated HW for key generation**
- **Smart card printer/programmer**
  - Programmer interface from the dedicated HW
- **Automatic courier reports**
- **Integrated accounting facilities**

Tailored for Cryptel-IP devices

THALES

Network Planner

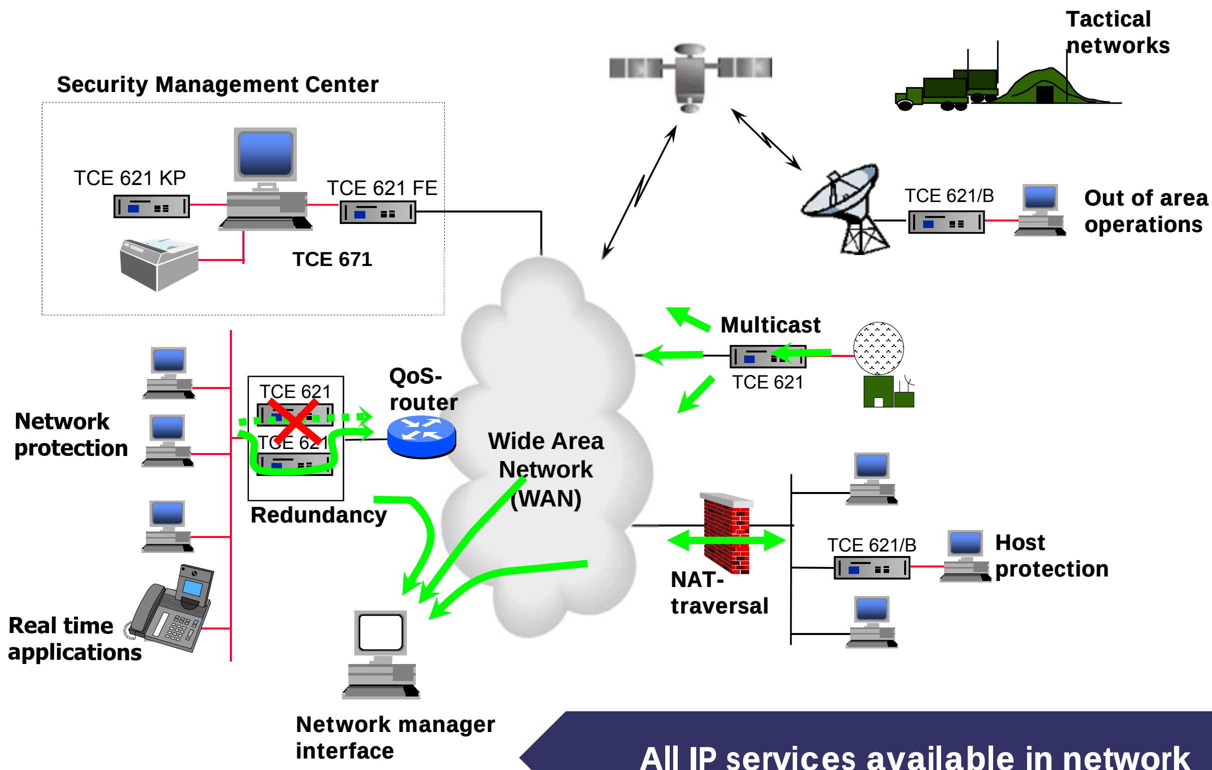
Main features

- **Offline tool for planning of Cryptel-IP networks**
  - Includes all TCE 621 variants
- **Graphical user interface**
  - Automated features
  - Easy to use application
- **Produces planning material**
  - Configuration files
  - Access control definitions
- **Runs on Windows based PCs**

System operator tool

THALES

Cryptel®-IP family today



All IP services available in network

THALES

Slide 67

oas1 - Gjøres uavhengig av versjoner
- få med dyn IPadresser
a4970; 03.03.2011

Summary

- have considered:
  - IPSec security framework
  - IPSec security policy
  - ESP/AH
  - combining security associations
  - internet key exchange
  - cryptographic suites used
  - TCE 621

Workshop – IPSec issues

1. Why is not all header fields protected by the ICV in AH?
2. Why can Transport Adjancency (ESP – AH) be preferred over ESP with authentication?
3. What is an clogging attack on IKE and how is it mitigated?
4. What is a replay attack and which mechanism does IPSec use to thwart it?