Welcome to

Virtual Private Network

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramse@Github

5-Virtual-Private-Network.tex in the repo security-courses

IPsec

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

RFC-2409 The Internet Key Exchange (IKE) - dynamisk keying

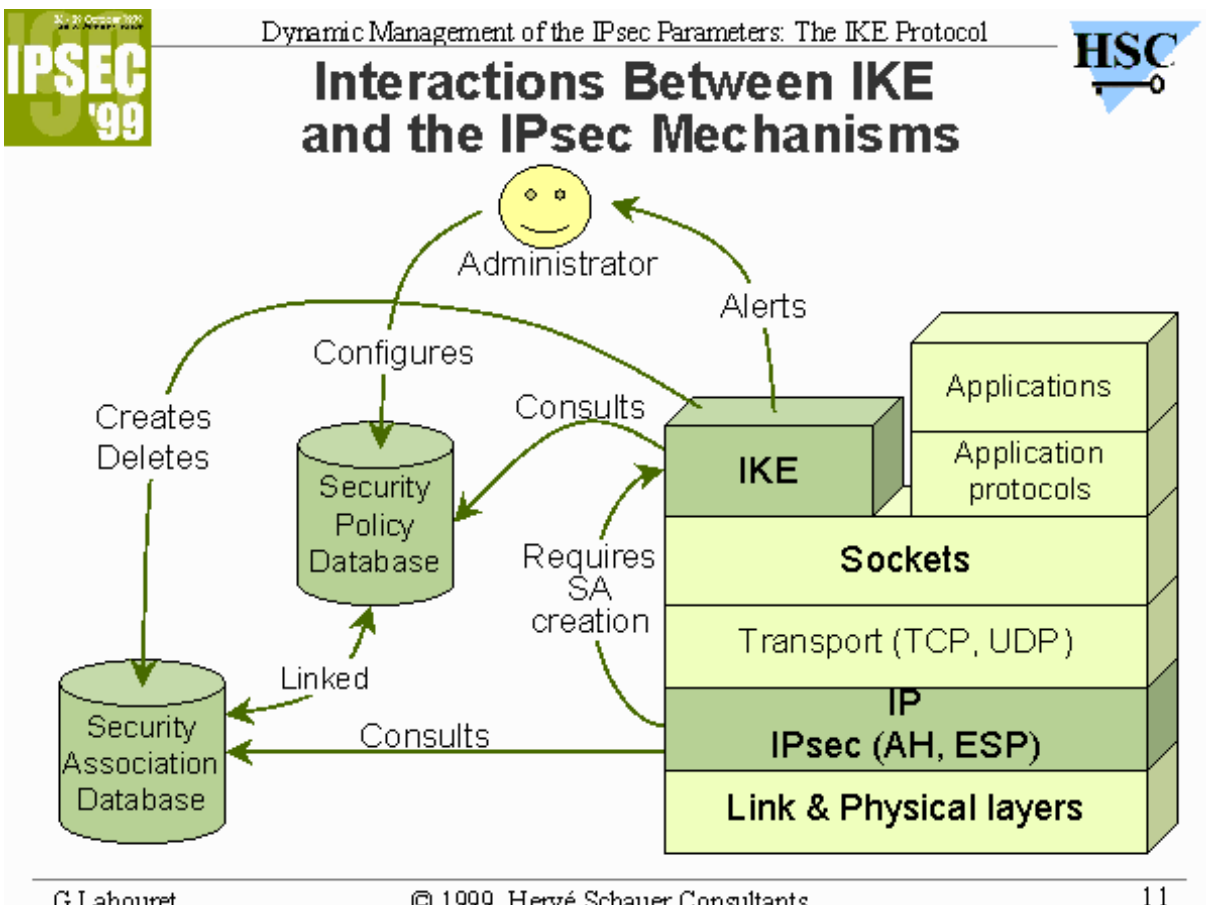
Både til IPv4 og IPv6

MANDATORY i IPv6! - et krav hvis man implementerer fuld IPv6 support

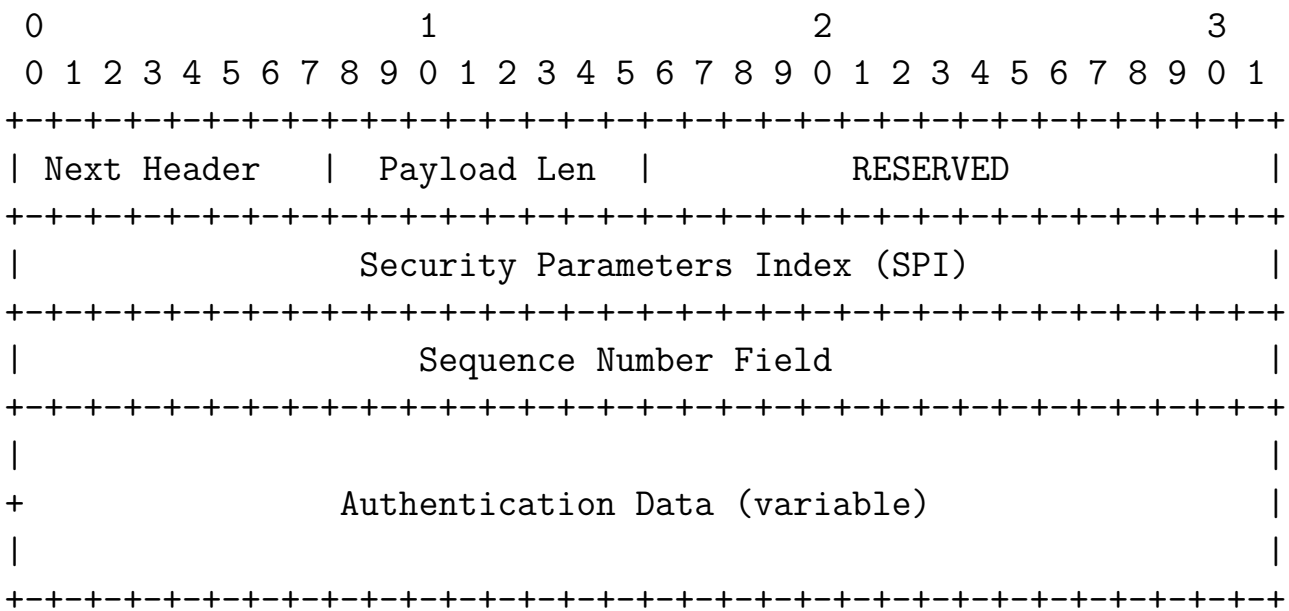
god præsentation på `http://www.hsc.fr/presentations/ike/`

Der findes IKEscan til at scanne efter IKE porte/implementationer
`http://www.nta-monitor.com/ike-scan/index.htm`

IPsec er ikke simpelt!



RFC-2402 IP AH



RFC-2402 IP AH

Indpakning - pakkerne før og efter Authentication Header:

```
            BEFORE APPLYING AH
          ----------------------------
    IPv4  |orig IP hdr  |     |      |
          |(any options)| TCP | Data |
          ----------------------------

             AFTER APPLYING AH
          ---------------------------------
    IPv4  |orig IP hdr  |    |     |      |
          |(any options)| AH | TCP | Data |
          ---------------------------------
          |<------- authenticated ------->|
               except for mutable fields
```

RFC-2406 IP ESP

Pakkerne før og efter:

```
          BEFORE APPLYING ESP
        ---------------------------------------
IPv6    |              | ext hdrs |     |      |
        | orig IP hdr  |if present| TCP | Data |
        ---------------------------------------


          AFTER APPLYING ESP
        -------------------------------------------------------
IPv6    | orig |hop-by-hop,dest*,|   |dest|   |     | ESP   | ESP|
        |IP hdr|routing,fragment.|ESP|opt*|TCP|Data|Trailer|Auth|
        -------------------------------------------------------
                                 |<---- encrypted ---->|
                               |<---- authenticated ---->|
```

ipsec konfigurationsfiler

Der er følgende filer tilgængelige

- konfigurationsfiler i NetBSD/FreeBSD/Mac OS X format - med `setkey` kommandoen
- konfigurationsfil til OpenBSD server - med `ipsecadm` kommandoen

IPsec setup

Client: Mac OS X/NetBSD/FreeBSD - samme syntaks
`rc.ipsec.client`

Server: OpenBSD - bruger ipsecadm kommando
`rc.ipsec.server`

Øvelse til læseren: lav samme i Cisco IOS

Det vil ofte være relevant at se på IOS og IPsec i laboratoriet

Dette setup når vi ikke at demonstrere

rc.ipsec.client - client setup - adresser

```
#!/bin/sh
# /etc/rc.ipsec.client - IPsec client configuration
# built from http://rt.fm/~jcs/ipsec_wep.phtml
# FreeBSD/NetBSD syntaks! - used on Mac OS X
# IPv4
SECSERVER=10.0.42.1
SECCLIENT=10.0.42.53
# IPv6
#SECSERVER=2001:618:433:101::1
#SECCLIENT=2001:618:433:101::153
ESPKEY=`cat ipsec.esp.key`
AHKEY=`cat ipsec.ah.key`

# Flush IPsec SAs in case we get called more than once
setkey -F
setkey -F -P
```

rc.ipsec.client - client setup - SAs

```
# Establish Security Associations
# 1000 is from the server to the client
# 1001 is from the client to the server
setkey -c <<EOF

add $SECSERVER $SECCLIENT esp 0x1000 \
-m tunnel -E blowfish-cbc 0x$ESPKEY  -A hmac-sha1 0x$AHKEY;

add $SECCLIENT $SECSERVER esp 0x1001 \
-m tunnel -E blowfish-cbc 0x$ESPKEY -A hmac-sha1 0x$AHKEY;

spdadd $SECCLIENT $SECSERVER any -P out \
ipsec esp/tunnel/$SECCLIENT-$SECSERVER/default;

spdadd $SECSERVER $SECCLIENT any -P in \
ipsec esp/tunnel/$SECSERVER-$SECCLIENT/default;
```

rc.ipsec.server - server setup - adresser

```
#!/bin/sh
#
# Henrik Lund Kramshøj
# /etc/rc.ipsec - IPsec server configuration
# built from http://rt.fm/~jcs/ipsec_wep.phtml
# OpenBSD syntaks!
SECSERVER=10.0.42.1
SECCLIENT=10.0.42.53
#SECSERVER6=2001:618:433:101::1
#SECCLIENT6=2001:618:433:101::153

ESPKEY=`cat ipsec.esp.key`
AHKEY=`cat ipsec.ah.key`

# Flush IPsec SAs in case we get called more than once
ipsecadm flush
```

rc.ipsec.server - server setup - SAs

```
# Establish Security Associations
#
# 1000 is from the server to the client
ipsecadm new esp -spi 1000 -src $SECSERVER -dst $SECCLIENT \
-forcetunnel -enc blf -key $ESPKEY \
-auth sha1 -authkey $AHKEY

# 1001 is from the client to the server
ipsecadm new esp -spi 1001 -src $SECCLIENT -dst $SECSERVER \
-forcetunnel -enc blf -key $ESPKEY \
-auth sha1 -authkey $AHKEY
```

rc.ipsec.server - server setup - flows

```
# Create flows
#
# Data going from the outside to the client
ipsecadm flow -out -src $SECSERVER -dst $SECCLIENT -proto esp \
-addr 0.0.0.0 0.0.0.0 $SECCLIENT 255.255.255.255 -dontacq
# IPv6
#ipsecadm flow -out -src $SECSERVER -dst $SECCLIENT -proto esp \
#-addr :: :: $SECCLIENT ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff -dontacq

# Data going from the client to the outside
ipsecadm flow -in -src $SECSERVER -dst $SECCLIENT -proto esp \
-addr $SECCLIENT 255.255.255.255 0.0.0.0 0.0.0.0 -dontacq
# IPv6
#ipsecadm flow -in -src $SECSERVER -dst $SECCLIENT -proto esp \
#-addr :: :: $SECCLIENT ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff -dontacq
```