strongSwan
The Linux IPsec Solution
Prof. Andreas Steffen
andreas.steffen@hsr.ch
Where the heck is Rapperswil?
HSR - Hochschule für Technik Rapperswil

- University of Applied Sciences with about 1000 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)
Virtual Private Networks

Internet

Head Quarters
10.1.0.0/16

VPN Gateway
11.22.33.44

VPN Tunnel

VPN Client
10.3.0.2

 „Road Warrior“

VPN Tunnel

VPN Gateway
55.66.77.88

Subsidiary
10.2.0.0/16

55.66.x.x
strongSwan User-Mode-Linux VPN Testbed
IPsec is a Layer 3 Standard

ESP/AH & IKE

IPsec Tunnel Mode using ESP

Before applying ESP

IPv4
IPv6

Original IP Header Layer 4 Header Data

Encapsulating Security Payload (ESP): RFC 4303

After applying ESP

IPv4
IPv6

Outer IP Header ESP Header Original IP Header Layer 4 Header Data ESP Trailer ESP Auth

• IP protocol number for ESP: 50 (has no ports!!!)
• ESP authentication is optional but usually used in place of AH (51)
• ESP is implemented by the Linux 2.6 kernel (Dave Miller et al.)
Internet Key Exchange – IKEv1 Main Mode

- IKEv1 Quick Mode – another three messages to negotiate traffic selectors
IKEv2 – Authentication and first Child SA

Initiator | UDP/500 | Responder
---|---|---
IKE Header | SA$_1^i$ | KE$_i$ | N$_i$

1. IKE_SA_INIT exchange pair

IKE Header | SA$_1^r$ | KE$_r$ | N$_r$

2. IKE_AUTH exchange pair

IKE Header | ID$_i$ | Cert$_i$ | ID$_r$

3. encrypted

4. IKE_AUTH exchange pair

encrypted

• IKE_SA_INIT exchange pair

• IKE_AUTH exchange pair
IKEv2 – Additional Child SAs

- CREATE_CHILD_SA exchange pair

Initiator

IKE Header

N

SAi

Ni

IKE Header

encrypted

KEi

TSi

TSr

Responder

IKE Header

SAr

Nr

IKE Header

encrypted

KER

TSi

TSr

UDP/500
strongSwan
Software Architecture
The FreeS/WAN Genealogy

1999
- FreeS/WAN 1.x

2000
- X.509 1.x Patch
- Super FreeS/WAN
- FreeS/WAN 2.x

2003
- Openswan 1.x

2004
- Openswan 2.x
- strongSwan 2.x

2005
- Openswan 3.x
- strongSwan 4.x

2006
- IKEv1 only
- IKEv1 & IKEv2

2007
- ITA IKEv2 Project

A. Steffen, 21.11.2008, AusCert-strongswan.ppt 12
The strongSwan IKE Daemons

IKEv1

- ipsec
- whack

- pluto

- ipsec.conf

IKEv2

- ipsec
- starter

- stroke

- charon

- LSF

- raw socket

- native IPsec

- UDP/500 socket

- LSF

- Linux 2.6 kernel

- Netlink XFRM socket

- stroke socket

- whack socket
IKEv2 Daemon – Software Architecture

- credentials
  - receiver
  - socket
  - sender
- backends
  - charon
  - bus
  - scheduler
  - processor
  - IKE Manager
    - IKE SA
      - CHILD SA
    - IKE SA
      - CHILD SA
    - IKE SA
      - CHILD SA
- kernel interface
  - file logger
  - sys logger
  - IPsec stack

16 concurrent worker threads
Configuration and Control
The FreeS/WAN way
IKEv2 Mixed PSK/RSA Authentication

#ipsec.secrets for roadwarrior carol

```
carol@strongswan.org : \PSK "FpZAZqEN6Ti9sqt4ZP5EWcqx"
```

#ipsec.conf for roadwarrior carol

```
conn home
  keyexchange=ikev2
  authby=psk
  left=%defaultroute
  leftsourceip=%config
  leftid=carol@strongswan.org
  leftfirewall=yes
  right=192.168.0.1
  rightid=@moon.strongswan.org
  rightsubnet=10.0.0.0/16
  auto=start
```

#ipsec.secrets for gateway moon

```
carol@strongswan.org : \PSK "FpZAZqEN6Ti9sqt4ZP5EWcqx"
dave@strongswan.org : \PSK "jVzONCF02ncsgiSlmIXeqhGN"
```

#ipsec.conf for gateway moon

```
conn rw
  keyexchange=ikev2
  authby=r satSig
  left=%defaultroute
  leftsubnet=10.1.0.0/16
  leftcert=moonCert.pem
  leftid=@moon.strongswan.org
  leftfirewall=yes
  right=%any
  rightsourceip=10.3.0.0/16
  auto=add
```
Stroke: Control Interface

```bash
carol> ipsec start

05[AUD] initiating IKE_SA 'home' to 192.168.0.1
05[ENC] generating IKE_SA_INIT request 0 [SA KE No N N]
05[NET] sending packet: from 192.168.0.100[500] to 192.168.0.1[500]
06[NET] received packet: from 192.168.0.1[500] to 192.168.0.100[500]
06[ENC] parsed IKE_SA_INIT response 0 [SA KE No N N]
06[ENC] generating IKE_AUTH request 1 [IDi CERTREQ IDr AUTH CP SA TSi TSr]
06[NET] sending packet: from 192.168.0.100[500] to 192.168.0.1[500]
07[NET] received packet: from 192.168.0.1[500] to 192.168.0.100[500]
07[ENC] parsed IKE_AUTH response 1 [IDr CERT AUTH CP SA TSi TSr N]
07[ENC] IKE_SA 'home' established between 192.168.0.100...192.168.0.1
07[IKE] installing new virtual IP 10.3.0.1
07[AUD] CHILD_SA 'home' established successfully
```
carol> ipsec status

Performance:
  uptime: 5 seconds, since Apr 28 18:30:36 2008
  worker threads: 11 idle of 16, job queue load: 1, scheduled events: 5
Listening IP addresses:
  192.168.0.100
  fec0::10
Connections:
  home: 192.168.0.100[carol@strongswan.org]...192.168.0.1[moon.strongswan.org]
  home: dynamic/32 === 10.1.0.0/16
Security Associations:
  home[1]: ESTABLISHED, 192.168.0.100[carol@strongswan.org]...192.168.0.1[moon.strongswan.org]
  home[1]: IKE SPIs: 15993ec81138c1b1_i* ce054ec02da36c8e_r, reauth in 51 minutes
  home{1}: INSTALLED, TUNNEL, ESP SPIs: c51cf634_i cf2c3efd_o
  home{1}: AES_CBC-128/HMAC_SHA1_96, rekeying in 14 minutes, last use: 2s_i 2s_o
  home{1}: 10.3.0.1/32 === 10.1.0.0/16
IKEv2 Interoperability Workshops

Spring 2007 in Orlando, Florida
Spring 2008 in San Antonio, Texas

- **strongSwan** successfully interoperated with IKEv2 products from Alcatel-Lucent, Certicom, CheckPoint, Cisco, Furukawa, IBM, Ixia, Juniper, Microsoft, Nokia, SafeNet, Secure Computing, SonicWall, and the IPv6 TAHI Project.
EAP Authentication or how to earn money

- The 3GPP Generic Access Network (GAN) enables GSM and UMTS services to be delivered over unlicensed WLAN Access Points (APs). Using IKEv2 EAP-SIM or EAP-AKA authentication the Mobile Station (MS) sets up an IPsec tunnel to the GAN Controller (GANC).

- strongSwan used in FemtoCells
- strongSwan used in industry-grade SEGWs
- Up to 20'000 concurrent tunnels
- Multiple cores with HW acceleration, e.g. Cavium Networks OCTEON MIPS64
- Google's Android???
Configuration and Control
The modular way
Plugins for charon

- **smp**
  - XML-based control and management protocol.
  - Implementation: strongSwan Manager

- **nm**
  - DBUS-based plugin for NetworkManager

- **sql**
  - Generic SQL interface for configurations, credentials & logging.
  - Implementations: SQLite & MySQL

- **eap**
  - Any EAP protocol.

- **controller**
- **credentials**
- **backends**
- **bus**

- **plugind**
  - **stroke**
  - **smp**
  - **nm**
  - **sql**

- **plugine**
  - **eap_aka**
  - **eap_sim**
  - **eap_md5**

- **plugin**
  - **...**

- **plugine**
  - **...**

A. Steffen, 21.11.2008, AusCert-strongswan.ppt 22
strongSwan Manager

IKE SA overview

hsr-net [IKE #82]: asteffen@hsr.ch <-> sidv0150.hsr.ch

asteffen@hsr.ch
2c130f0c8c8bd0b1

sidv0150.hsr.ch
dbf91323bea1a3e0

hsr-net [IPsec #164]:

10.10.0.0/23 cf6ae6b3 <- -> cfbd1f88 152.96.52.150/32

hsr-dns [IPsec #163]:

62.2.17.60/31 c4c0d2a5 <- -> cd3586ed 152.96.52.150/32

FastCGI written in C with ClearSilver templates
strongSwan Entity Relationship Diagram

SQLite and MySQL implementations
Modular Crypto Plugins
Plugins for libstrongswan

libstrongswan

- crypto
- credentials
- database
- fetcher

Factories

Plugins

- aes
- sha2
- random
- x509
- sqlite
- mysql
- curl
- ldap

- Certificate retrieval (HASH-and-URL)
- CRL fetching, OCSP
- Non-US crypto code
- No OpenSSL library
- ECCN: No License Required (NLR)
VIA EPIA-NX PadLock Crypto-Processor

- padlock plugin
  AES/SHA
  HW acceleration

- openssl plugin
  uses libcrypto-0.9.8 OpenSSL library
  - ECP DH groups
  - ECDSA signatures
  - HW engine support
Thank you for your attention!

Questions?
Thank you for your attention!

Questions?