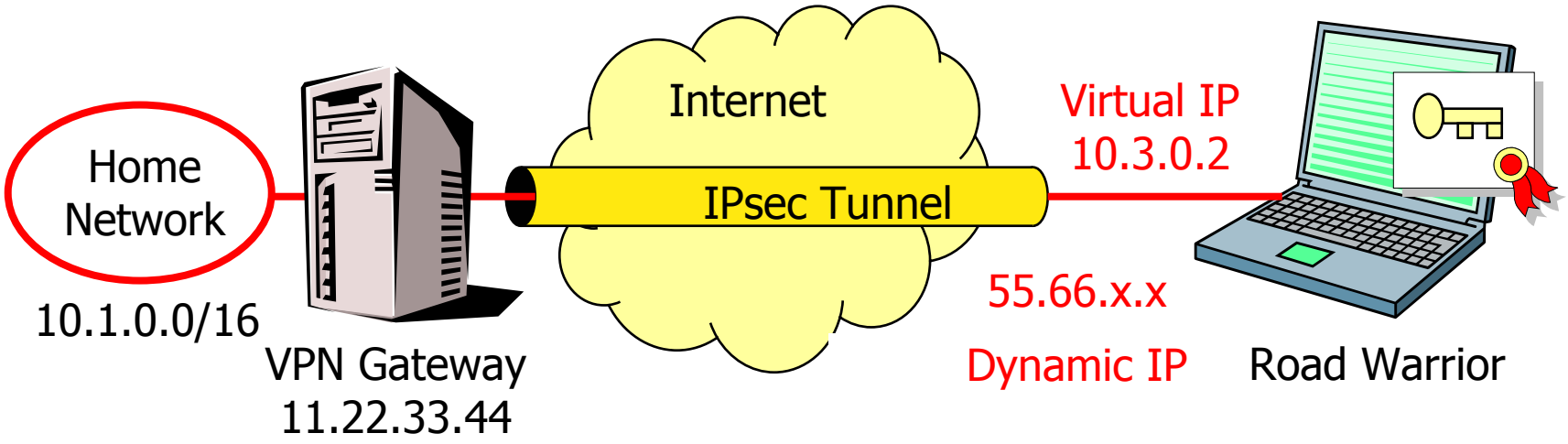
Zürcher Hochschule Winterthur

Large-Scale Road Warrior Access based on X.509 Certificates and DHCP-over-IPsec

Prof. Andreas Steffen
Zurich University of Applied Sciences
Winterthur, Switzerland

The „Road Warrior" Remote Access Case

Zürcher Hochschule Winterthur



- Road warriors sign on to their home network via IKE with varying IP addresses assigned dynamically by their local ISP.
- Authentication is usually based on RSA public keys and X.509 certificates issued by the home network.
- Virtual IP assigned statically or dynamically by the home network. Remote hosts thus become part of an extruded net.

Requirements for Large-Scale VPN Deployment

Zürcher Hochschule Winterthur

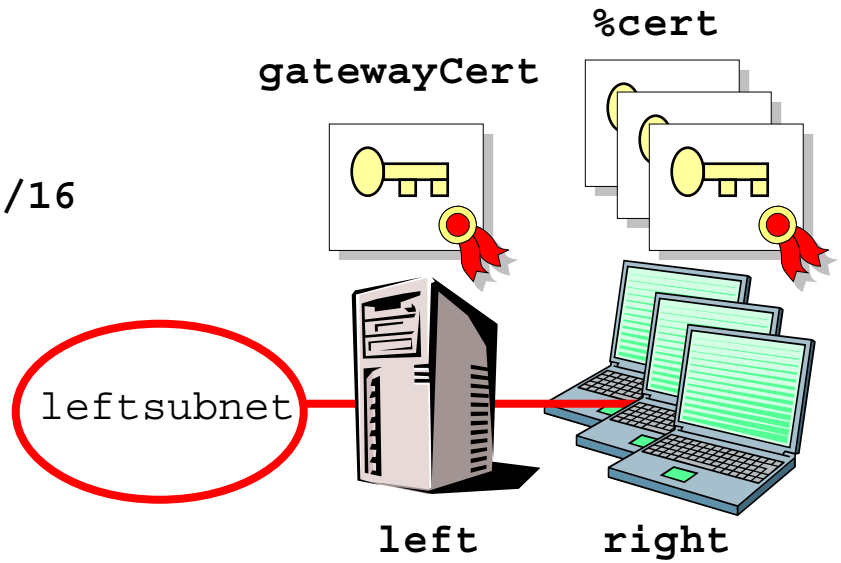
- Automatic assignment of virtual IP addresses
  - Avoid error-prone individual configuration of VPN clients
- Authentication based on X.509 certificates
  - Preshared secrets do not scale well with the number of VPN clients
  - Preshared secrets do not work with dynamic IPs and IKE Main Mode
- Safe storage of private keys
  - VPN road warrior certificates and private keys should preferably be stored on smard cards or USB tokens.
- User authentication and access control policies
  - VPN access control usually based on X.509 user certificates
  - Timely updates of certificate revocation lists are of utmost importance.
  - Better: Separate user authentication and access control

Linux FreeS/WAN as a VPN Gateway

Zürcher Hochschule Winterthur

- Available from www.freeswan.ca / www.strongsec.com
  - OpenSource IPsec stack for Linux 2.2 and 2.4 kernels
  - X.509 certificate support developed by ZHW !!!
  - Easy installation via RedHat/SuSE/Debian/Mandrake RPMs
  - Number of VPN tunnels is limited by hardware resources, only.
  - Linux Free/SWAN can also be used as a VPN client
- Road Warrior and Virtual IP support using X.509 certificates:

```
conn road-warrior
    right=%any
    rightrsasigkey=%cert
    rightsubnetwithin=10.3.0.0/16
    left=%defaultroute
    leftsubnet=10.1.0.0/16
    leftcert=gatewayCert.pem
    auto=add
```

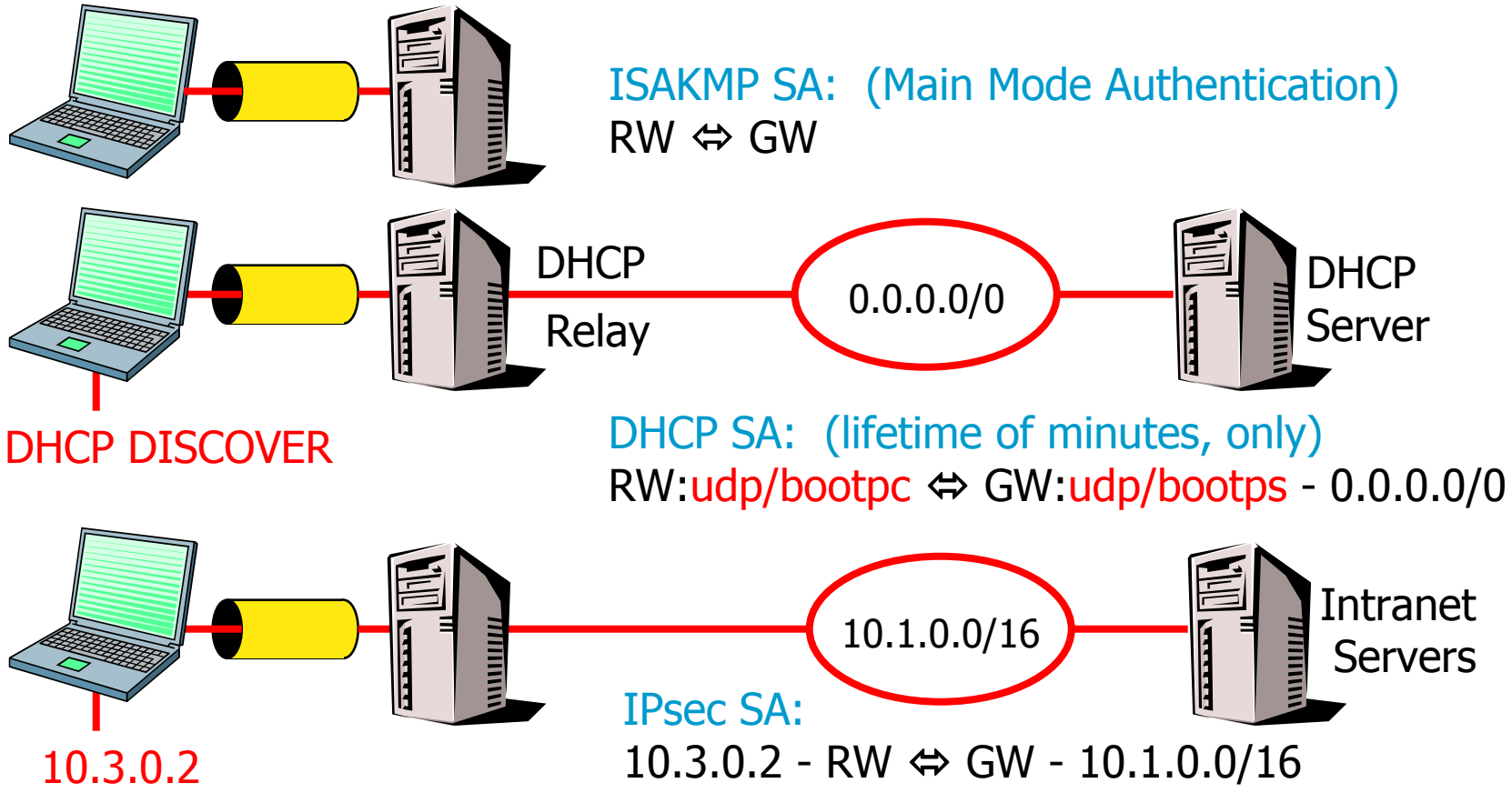


- Simple configuration

Virtual IP Assignment via DHCP-over-IPsec

Zürcher Hochschule Winterthur

- Internet Draft : draft-ietf-ipsec-dhcp-13.txt
- Currently supported by SSH Sentinel and Linux FreeS/WAN



DHCP-over-IPsec Features

Zürcher Hochschule Winterthur

- Features
  - By providing a Virtual IP plus additional network information like e.g. local DNS and WINS server addresses, DHCP-over-IPsec can offer the same functionality as the heavy-weight L2TP-over-IPsec protocol.
  - On the VPN gateway a DHCP Relay is required which relays DHCP messages to and from the DHCP server in the home network.
- Open Questions
  - A Virtual IP interface does not have a physical MAC address. The DHCP-over-IPsec draft does not specify how the unique client hardware address should be formed.
  - Unicast DHCP messages like e.g. DHCPREQUEST use the normal IPsec tunnel SA. What about broadcast DHCPDISCOVER messages?
- DHCP Relay Agent for Linux FreeS/WAN
  - Download: http://www.strongsec.com/freeswan/dhcprelay

User Management - CRL Distribution Points

Zürcher Hochschule Winterthur

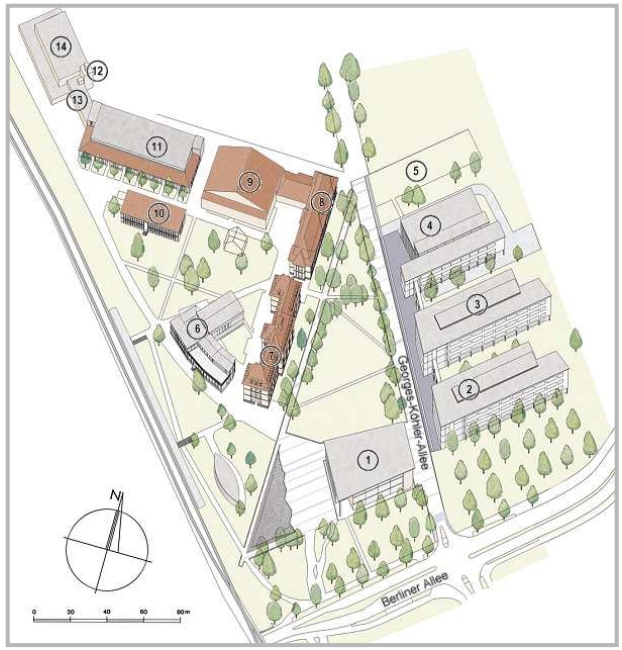
- Users are admitted on the basis of a valid X.509 certificate.
- In order to lock out a user, the corresponding certificate must be revoked and the CRL made quickly available to all VPN end points.
- A X.509v3 extension can contain one or several crlDistributionPoints that consist either of a HTTP, FTP, or an LDAP Uniform Resource Identifier (URI). Example in OpenSSL notation:

```
crlDistributionPoints =
    URI:http://www.rolex.ch/ca/cert.crl
```

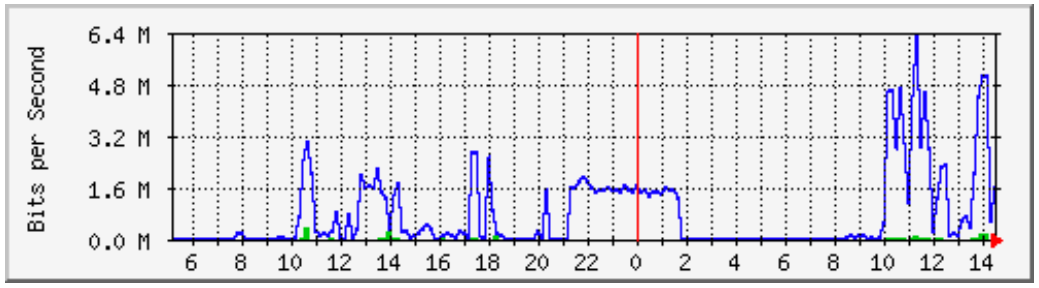
- Upon reception of a peer certificate, a VPN client will try to get an updated Certificate Revocation List from the URI(s) listed in the crlDistributionPoints field.
- Version 1.1.0 of X.509 patch for Linux FreeS/WAN 2.00 supports URI-based dynamic CRL fetching.

Deployment – University of Freiburg, Germany

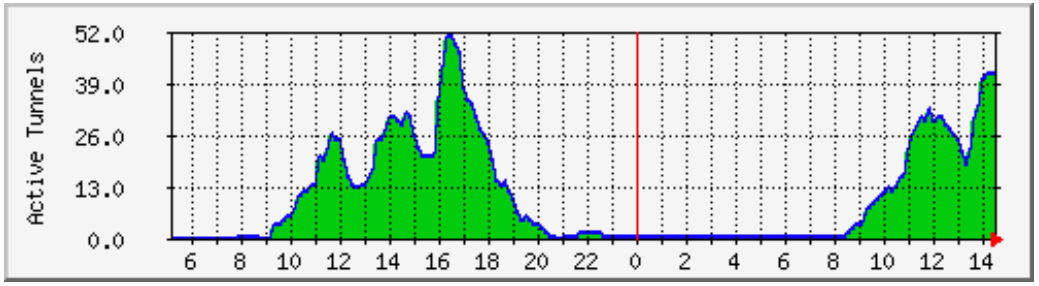
Zürcher Hochschule Winterthur



Campus



IPsec throughput at VPN gateway



Active VPN tunnels

- 44 WLAN access points, 1 Linux VPN gateway, no DHCP-over-IPsec
- 202 active and 88 revoked X.509 certificates
- FreeS/WAN Linux clients / SSH Sentinel Windows clients
- Further information: http://mopoinfo.wlan.informatik.uni-freiburg.de

Zürcher Hochschule Winterthur

IPsec Policies
Coping with Complexity

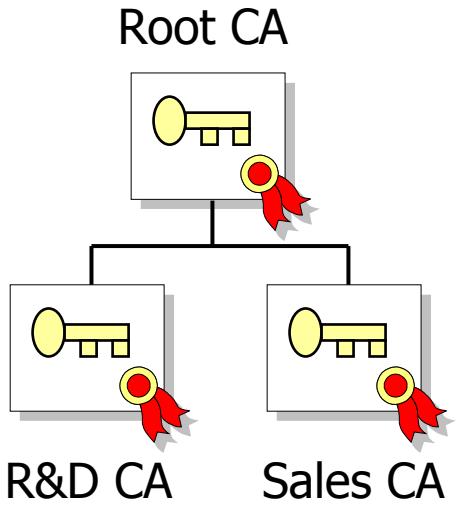
IPsec Policy Model - Intermediate CAs

Zürcher Hochschule Winterthur

```
conn research
     right=%any
     rightca="C=CH, O=Rolex, CN=R&D CA"
     leftsubnet=10.1.1.0/24
```

```
conn sales
     right=%any
     rightca="C=CH, O=Rolex, CN=Sales CA"
     leftsubnet=10.1.2.0/24
```

- Advantage: decentralized management of access control rights possible
- Drawback: user or host certificate is bound to intermediate CA
- Linux FreeS/WAN:
  Access control based on intermediate CAs might be implemented in 2003



IPsec Policy Model - Identity Wild Cards

Zürcher Hochschule Winterthur

```
conn research
     right=%any
     rightid="C=CH, O=Rolex, OU=R&D, CN=*"      /* DN */
     leftsubnet=10.1.1.0/24
```

```
conn sales
     right=%any
     rightid=*@sales.rolex.ch              /* USER FQDN */
     leftsubnet=10.1.2.0/24
```

```
conn it-hosts
     right=%any
     rightid=@*.it.rolex.ch                    /* FQDN */
     leftsubnet=10.1.3.4/32
```

- Wild cards as defined by draft-ietf-ipsp-config-policy-model-06.txt
- Drawback: Identity is strongly bound to user or host certificate
- Linux FreeS/WAN: wild cards will be introduced in 1Q 2003

IPsec Policy Models – Attribute Certificates

Zürcher Hochschule Winterthur

- X.509 Attribute Certificates (AC)
  - ACs separate the tasks of authentication (based on user certificates) and authorization (based on attribute certificates).
  - Attribute certificates grant short-term access control rights but are themselves bound to long-lived user certificates.
  - Due to the short lifetime of attribute certificates, revocation will usually not be necessary.
- Kerberos V5 tickets with Privilege Attribute Certificates (PAC)
  - For its Windows 2000 authentication and authorization solution Microsoft added a proprietary PAC containing group memberships to Kerberos V5 tickets. Kerberos can be used to authenticate IPsec connections and to grant access control rights.
- Linux FreeS/WAN:
  - Solutions based on Attribute Certificates and/or Kerberos Tickets are being studied at the Zurich University of Applied Sciences.