Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Heiko Niedermayer
Dipl.-Inf. Ali Fessi

Exercises for lecture „Netzsicherheit“
Assignment 4, WS09/10

Hand-out:	Wednesday December 16th 2009
Deadline:	Thursday January 7th 2010
Exercise course:	Thursday January 14th 2010

Task 1: Trust models in Public Key Infrastruktures (PKI)

a) Figure 1 show a PKI that is structured as tree[1]. Let *N* be the number of nodes in the tree and *d* the height of the tree (i.e. the longest path from a leaf to the root node). Furthermore, we assume that each CA can decide given the user name if a certificate may be in its subtree or not.
The certificates of Alice and Bob are now in this PKI each attached to a leaf in the tree. What is the “best case” and what is the “best case” complexity to find a certificate chain from Alice to Bob with respect to *d*?

b) Figure 2 is a PKI that is based on a “user-centric” as in *Pretty Good Privacy (PGP)*. For the sake of simplicity we assume that the graph is undirected.In our case this means that when the public key of Alice is signed by a friend of Alice, Alice also signed the public key of her friend. The certificates are stored in a central PGP server. It is now the task of the server to find a certificate chain from Alice to Bob. Such a chain may not necessarily exist.

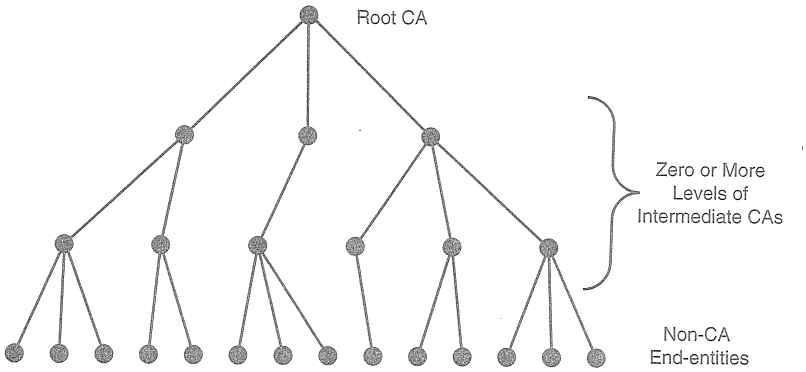

Figure 1: PKI with strict hierarchy

Let *V* be the set of nodes („Vertices“) and *E* be the set of links („Edges“) in the graph $G = (V, E)$.

[1] A tree is a graph that is fully connected, but does not contain any cycle (in undirected graph identical with circle).

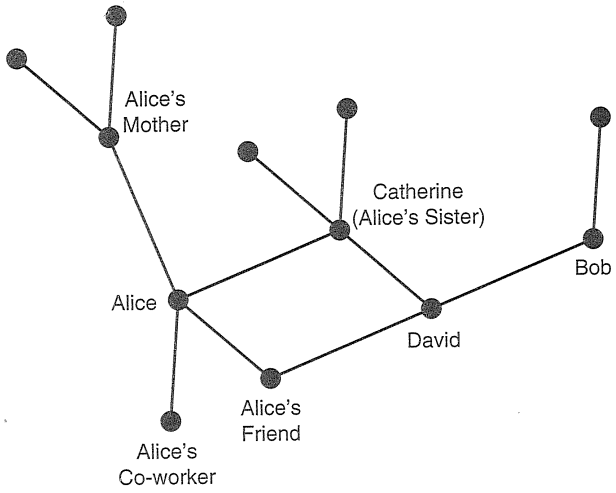

Figure 2: PKI like PGP

The following algorithm (~ Algorithm of Dijkstra) computes the shortest path from Alice to Bob. Let *U* ("unvisited") be the set of yet unprocessed nodes (at the start *U = V*). When the algorithm terminates, the value *Distance*(*Bob*) the length of the path between Alice and Bob.

```
FOR all v in V DO
   Distance(v):=infinite; Predecessor(v):=null;
END FOR;

Distance(Alice):=0; Predecessor(Alice):=Alice; U:=V;

WHILE(U not empty) DO
   Select u in U with minimum Distance(u);
   U:=U – u;
   IF (u=Bob) STOP
   FOR ALL (u,v) in E with v in U DO
         IF Distance(u)+1 < Distance(v) THEN
               Distance(v):=Distance(u)+1;
               Predecessor(v)=u;
         END IF
   END FOR
END WHILE
```

What is the complexity to find a certificate chain between two users Alice and Bob? Use nodes *N* and edges *M* as parameters..

c) Figure 3 is a third variant how a PKI can be structured: the graph contains multiple trees, yet the root nodes of the trees are interconnected in an arbitrary way (not necessary that all roots are connected).

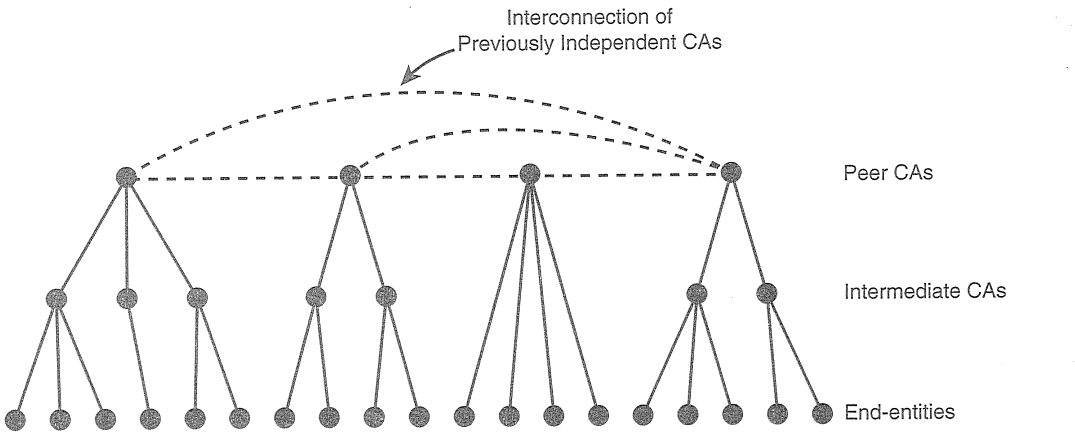

Abbildung 3: Teilweise hierarchische PKI

Let n be the number of root CAs, m the number of edges between the root Cas and d_{max} the maximum height of a tree. What is the "worst case" complexity to find a chain of trust between Alice and Bob in this model, with respect to parameters d_{max}, n and m.

Task 2: IPSec: AH and ESP

a) Why is it not possible that the Authentication Header can protect all header fields of the outer IP header?
b) Argue why the processing of incoming packets requires all fragments of an IP packet to be reassebles before the further processing of IPSec can proceed..
c) Let us now look at the IP header and the AH header of a protected IP packet.
   - What value stands in the (outer) IP header field „Protocol" when AH is used? (Note: cf http://www.iana.org/assignments/protocol-numbers)
   - Which value stands in the header field „Next Header" of HA, when the packet is additionally protected by ESP?
d) When is the ESP trailer unnecessary?

Task 3: IPSec – Protecting against „Replay- Attacks "

a) What measures are taken in the AH or ESP protocol to prevent a replay attack?
b) Why is it reasonable to check for incoming IPSec packets if the sequence number is not too old before the cryptographic checkes are performed?
c) Why is it necessary that the authenticity of an AH or ESP is checked before the sliding window is slided?
d) What is the difference (operation, functionality) between the sliding window in TCP and IPSec (AH/ESP)?

Task 4: IPSec – Incompatibility with Network Adress Translation (NAT)

An employee („Road Warrier") visiting a costumer or partner company becomes a part of foreign network (cf. Figure 4). The foreign network only assigns private IP addresses[2] to the network devices, including the computer of our road warrior. The connection to the Internet is done via a so-called Network Address Translator (NAT) that is located in router RA in the given figure. NAT changes the IP addresses of incoming and outgoing IP packets. This is also true to the IP packets from the computer of the road warrior and the IPSec gateway RB. IPSec is used in Tunnel Mode.

[2] Private IP adress ranges are in the ranges 10.x.x.x, 172.16.x.x oder 192.168.x.x. For more details, see RFC1918.

a) What is the resulting conflict when the packets between the computer of the Road Warrier und RB are protected with Authentication Header (AH)?
b) Now assume that the NAT does additionally change port numbers of the transport layer protocol (Layer 4)[3]. Why does this also conflict the use of ESP, if the encryption algorithm is not „NULL“?
c) RFC3948 describes a solution for the problem with NAT and ESP (section 3.4). Why does this solution solve the problem of b). Please explain it by using exemplary IP adresses and port numbers in the inner and outer IP headers / payload.

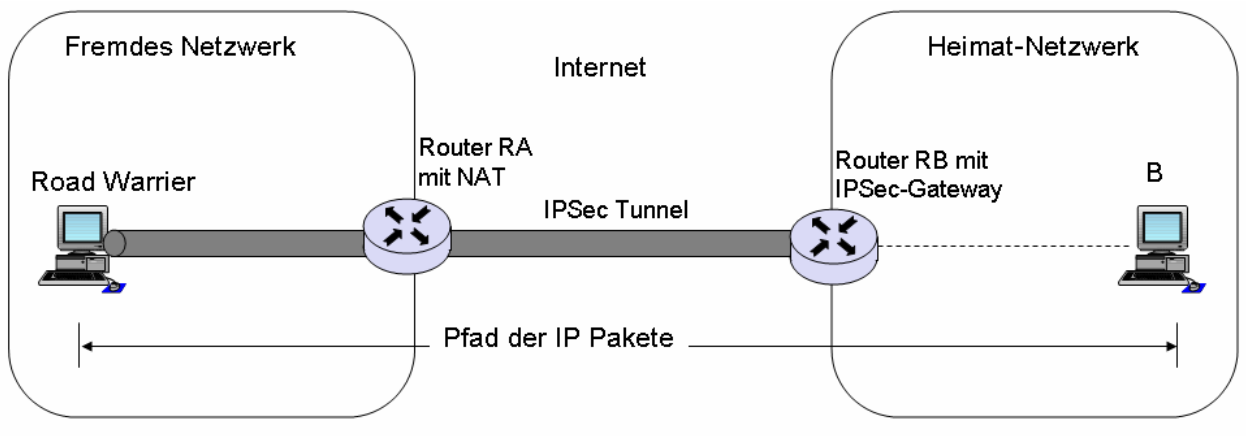

Figure 4: Road-Warrier behind NAT

[3] This kind of NAT, also called NAPT (Network Address and Port Translator), is very common and can be found in DSL routers as well as at the border of company networks with private addresses. While this is the most common one, there are also other NATs, e.g. IPv6-IPV4 NAT, Twice-NAT.