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

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

Übung zur Vorlesung „Netzsicherheit“
Übungsblatt 4, WS09/10

Ausgabe:	Mi 16. Dez. 2009
Abgabe:	Do 7. Jan. 2010
Besprechungstermin:	Do 14. Jan. 2010

Aufgabe 1: Vertrauensmodelle in Public-Key-Infrastrukturen (PKI)

a) Abbildung 1 stellt eine PKI dar, die in einem Baum strukturiert ist[1]. Sei dabei *N* die Anzahl der Knoten in diesem Baum und *d* die Höhe des Baums (d.h. der längste Pfad zwischen einem Blatt und dem Wurzelknoten). Weiterhin gilt, dass jede CA an Hand des Namen eines Benutzers feststellen kann, ob der jeweilige Zertifikat in ihrem Unterbaum liegt.
Angenommen die Zertifikate von Alice und Bob sind in dieser PKI jeweils in einem Blatt des Baumes eingetragen. Schätzen Sie den Aufwand in Abhängigkeit von *d* im „Best case“ und „Worst Case“ ab, um einen Zertifikatskette zwischen Alice und Bob zu bilden.

b) Abbildung 2 stellt eine PKI in einem Graphen im so genannten „User-Centric“ Model dar, sowie es bei *Pretty Good Privacy (PGP)* der Fall ist. Der Einfachheit halber gehen wir davon aus, dass der Graph ungerichtet ist, d.h. wenn z.B. der öffentliche Schlüssel von Alice durch „Alice’ Friend“ signiert ist, dann ist der öffentliche Schlüssel von „Alice’s Friend“ auch durch Alice signiert. Die Zertifikate werden hier in einem zentralen PGP Server gespeichert, der auf Anfrage von einem Benutzer Alice eine Zertifikatskette von Alice zu einem anderen Benutzer Bob liefern kann.

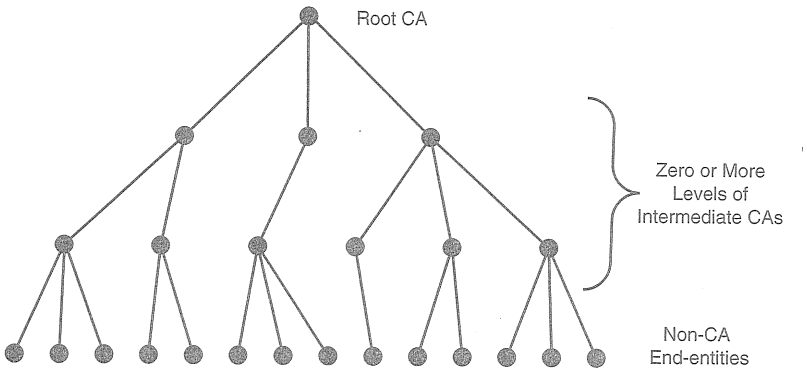

Abbildung 1: PKI mit einer strikten Hierarchie

Sei *V* die Menge der Knoten („Vertices“) und *E* die Menge der Kanten („Edges“) in dem Graphen $G = (V, E)$.

[1] Ein Baum wird in der Graphentheorie als ”ein zusammenhängender Graph, der keine Zyklen enthält“ definiert.

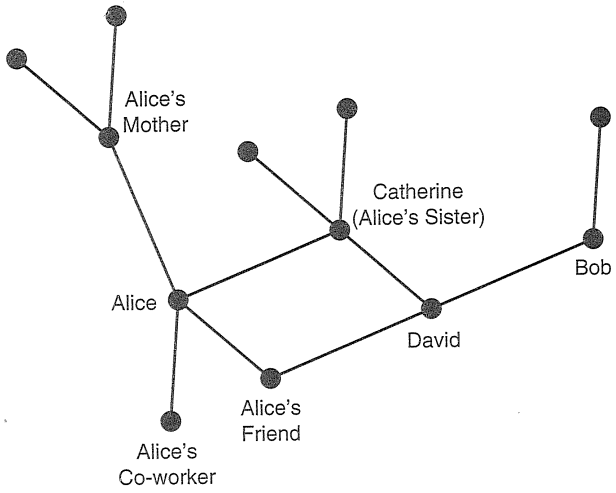

Abbildung 2: PKI mit PGP

Folgender Algorithmus berechnet den kürzesten Pfad von Alice nach Bob. Dabei ist *U* (”unvisited“) die Menge der noch zu bearbeitenden Knoten (am Anfang gilt also *U = V*). Wenn der Algorithmus terminiert, dann liefert der Wert *Distanz*(*Bob*) die Länge des Pfades zwischen Alice und 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
```

Schätzen Sie den Aufwand ab, um die Zertifikatskette zwischen 2 Benutzern Alice und Bob zu bilden, in Abhängigkeit von der Anzahl der Knoten *N* und der Anzahl der Kanten *M*.

c) Abbildung 3 stellt eine dritte Möglichkeit dar, wie eine PKI strukturiert sein kann: der Graph besteht aus mehreren Bäumen, wobei die Wurzelknoten dieser Bäume untereinander beliebig mit einander verbunden sein können (aber es sind auch nicht alle unbedingt mit einander verbunden).

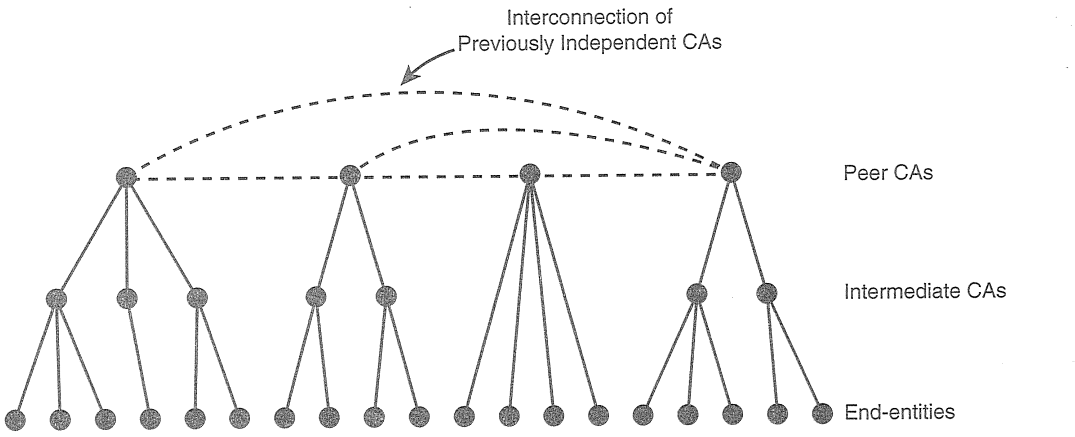

Abbildung 3: Teilweise hierarchische PKI

Sei *n* bei dieser Struktur die Anzahl der obersten CAs, *m* die Anzahl der Kanten, welche die obersten CAs miteinander verbinden und d_{max} die maximale Höhe eines Baumes. Schätzen Sie hier auch den Aufwand im „Worst Case" ab, um eine „Chain of Trust" zwischen Alice und Bob zu bilden, in Abhängigkeit von d_{max}, *n* und *m*.

Aufgabe 2: IPSec: AH und ESP

a) Aus welchem Grund kann der Authentication Header nicht alle Felder des äußeren IP-Headers schützen?
b) Begründen Sie, warum bei der Verarbeitung von ankommenden Paketen, mit dem AH oder ESP Protokoll, erst alle Fragmente eines IP-Pakets zusammengesetzt werden müssen, bevor weitere Verarbeitung erfolgen kann.
c) Betrachten wir den IP-Header und den AH-Header eines geschützten IP-Pakets.
   - Welcher Wert steht im IP-Header bei dem Feld „Protocol"? (Hinweis: siehe http://www.iana.org/assignments/protocol-numbers)
   - Welcher Wert würde im AH-Header bei dem Feld "`Next Header"', wenn das Paket zusätzlich mit ESP geschützt ist?
d) In welchen Fällen wird der ESP-Trailer nicht benötigt?

Aufgabe 3: IPSec - Schutz vor „Replay-Angriffen"

a) Welche Maßnahme wird bei dem AH bzw. ESP Protokoll verwendet, um einen „Replay-Angriff" zu erkennen?
b) Warum ist es sinnvoll, bei der Verarbeitung eingehender IPSec-Pakete zunächst zu prüfen, ob die Sequenznummer nicht zu alt ist, bevor mit weiteren kryptographischen Überprüfungen fortgefahren wird?
c) Warum wird stets erst die Authentizität eines AH- oder ESP-Pakets überprüft, bevor das Sliding Window verschoben wird?
d) Beschreiben Sie den Unterschied zwischen der Funktion des Sliding-Windows-Verfahrens bei TCP und bei AH bzw. ESP.

Aufgabe 4: IPSec – Inkompatibilität mit Network Adress Translation (NAT)

Ein externer Firmenmitarbeiter („Road Warrier") befindet sich gerade mit seinem PC in einem fremden Netz (Siehe Abbildung 4). Im fremden Netz werden ausschließlich private IP Adressen vergeben[2]. Die Verbindung ins Internet geschieht durch einen Network Address Translator (NAT), der

[2] Private Adresse Räume können aus den Bereichen 10.x.x.x, 172.16.x.x oder 192.168.x.x ausgewählt werden. Mehr Details dazu kann man z.B. in RFC1918 finden.

sich im Router RA befindet. Der NAT verändert die IP Adressen, der ein- und ausgehenden IP-Pakete. Insbesondere gilt das auch für die IP-Pakete, die zwischen dem PC des Road Worriers und des IPSec-Gateways im RB. Es wird IPSec im Tunnel Mode betrieben.

a) Welcher Konflikt entsteht falls die Pakete zwischen dem PC des Road-Warriers und RB mit dem Authentication Header Protocol (AH) geschützt werden sollen?
b) Angenommen, der NAT ändert zusätzlich die Port-Nummern im Transport Header (Layer 4) eines Pakets[3]. Welcher Konflikt entsteht hier mit dem ESP Protokoll, falls der ausgehandelte Verschlüsselungsalgorithmus ungleich „NULL“ ist?
c) RFC3948 beschreibt eine Lösung für das Problem mit dem NAT und dem ESP-Protokoll. (Siehe z.B. Abschnitt 3.4). Begründen Sie, warum das in Aufgabe b) diskutierte Problem mit dieser Lösung behoben wird. Erläutern Sie Ihre Begründung mit beispielhaften IP-Adressen (für die inneren und äußeren IP-Header) und Port-Nummern.

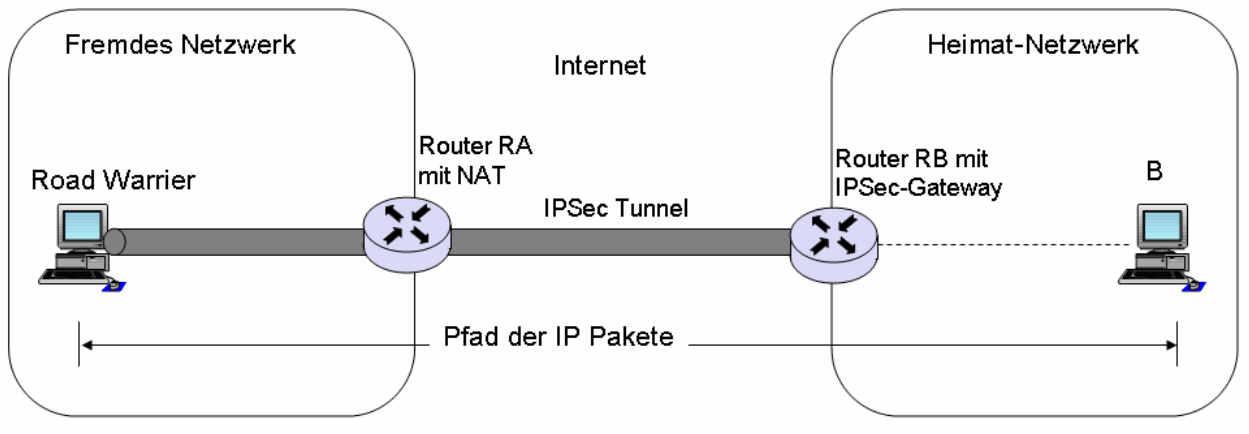

Abbildung 4: Road-Warrier hinter einem NAT

[3] Dieser Art vom NATs, auch NAPT (Network Address and Port Translator) genannt, ist eine häufige Art von NATs, die sich z.B. öfter in kommerziellen DSL-Routern befindet. Es gibt allerdings andere Arten von NATs, z.B. IPv6-IPV4 NAT, Twice-NAT, etc.