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

Dipl.-Inf. Ali Fessi

Übungen zur Vorlesung „Netzsicherheit“
Übungsblatt 5, WS08/09

Abgabe: 07. Jan. 2009
Besprechungstermin: 14. Jan. 2009

Aufgabe 1: IPSec: Allgemein

a) Welche Sicherheitsdienste bietet jeweils das Authentication Header (AH) Protokoll und das Encapsulation Secure Payload (ESP) Protokoll an?
b) Erklären Sie den Begriff „Security Association“. Durch welche Parameter kann eine Security Association eindeutig definiert werden?
c) Erklären Sie die Aufgaben der beiden konzeptionellen Datenbanken Securiy Association Database (SAD) und Security Policy Database (SPD).
d) Erklären Sie den Unterschied zwischen „Transport Mode“ und „Tunnel Mode“.
e) Welche der beiden Modi kann „Ende-zu-Ende“ bzw. „Ende-zu-Gateway“ oder „Gateway-zu-Gateway“ verwendet werden?

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) Beschreiben Sie den Unterschied zwischen der Datenintegrität, die das AH bzw. das ESP Protokoll bietet?
d) Abbildung 1 zeigt 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?
   - Welcher Wert würde im AH-Header bei dem Feld "`Next Header"', wenn das Paket nicht mit ESP geschützt ist und der Inhalt des IP-Pakets ein TCP-Segment ist?
e) 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?

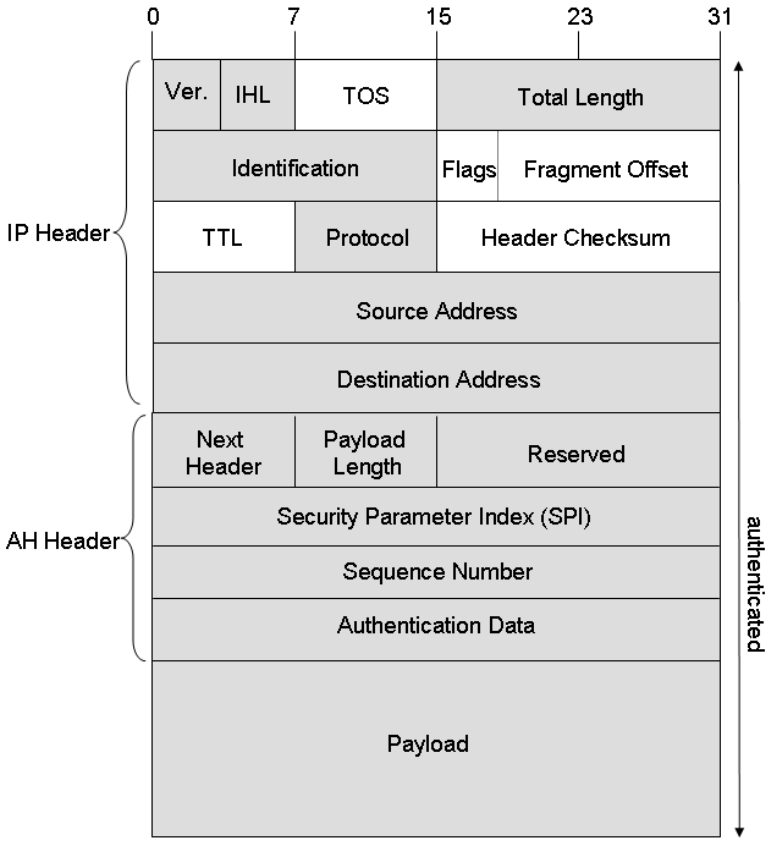

Abbildung 1: Aufbau eines IP-Pakets mit AH-Header

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 2). Im fremden Netz werden ausschließlich private IP Adressen vergeben[1]. Die Verbindung ins Internet geschieht durch einen Network Address Translator (NAT), der 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 dem Transport Header (Layer 4) eines Pakets[2]. Welcher Konflikt entsteht hier mit dem ESP Protokoll, falls der ausgehandelte Verschlüsselungsalgorithmus ungleich „NULL“ ist?

[1] 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.
[2] 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.

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.

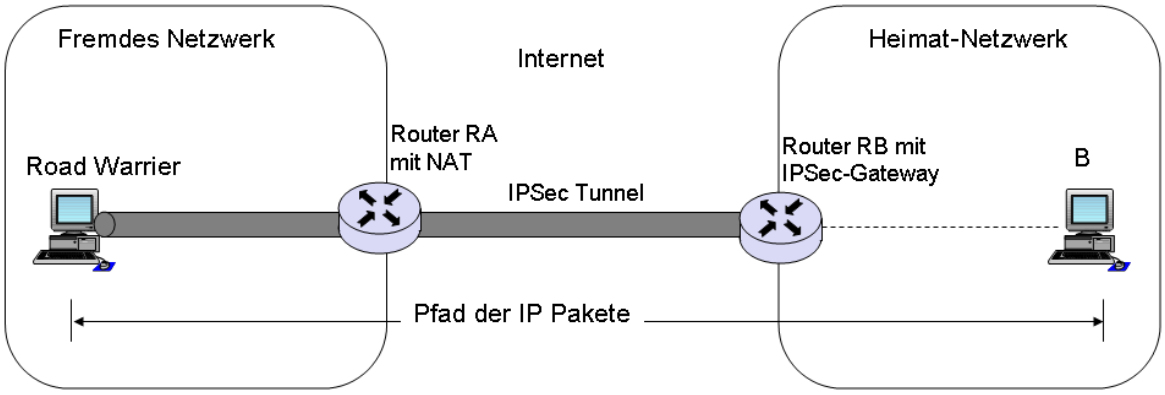

Abbildung 2: Road-Warrier hinter einem NAT