

Mobile IP Security

Sicherheit mobiler Systeme, WS 2007/2008
Rene Schneider, rs034@hdm-stuttgart.de

Agenda

- ▶ Einführung in Mobile IP
 - ▶ Was kann Mobile IP?
 - ▶ Wie funktioniert Mobile IP?
- ▶ Angriffsszenarien auf Mobile IP
- ▶ Security-Funktionen in Mobile IP
- ▶ Schutz der übertragenen Daten: ESP



Einführung in Mobile IP

- ▶ Mobile IP ist ein IETF-Standard
- ▶ Das Protokoll ermöglicht „Roaming“ auf IP-Ebene
- ▶ Mobile IP ist transparent: Die Applikationen erfahren nichts über die Position eines Knotens bzw. einen Positionswechsel
- ▶ Die Kompatibilität zu bestehenden Endgeräten bleibt erhalten – Mobile IP basiert auf dem normalen IP-Protokoll



Mobile IP - Funktionsweise

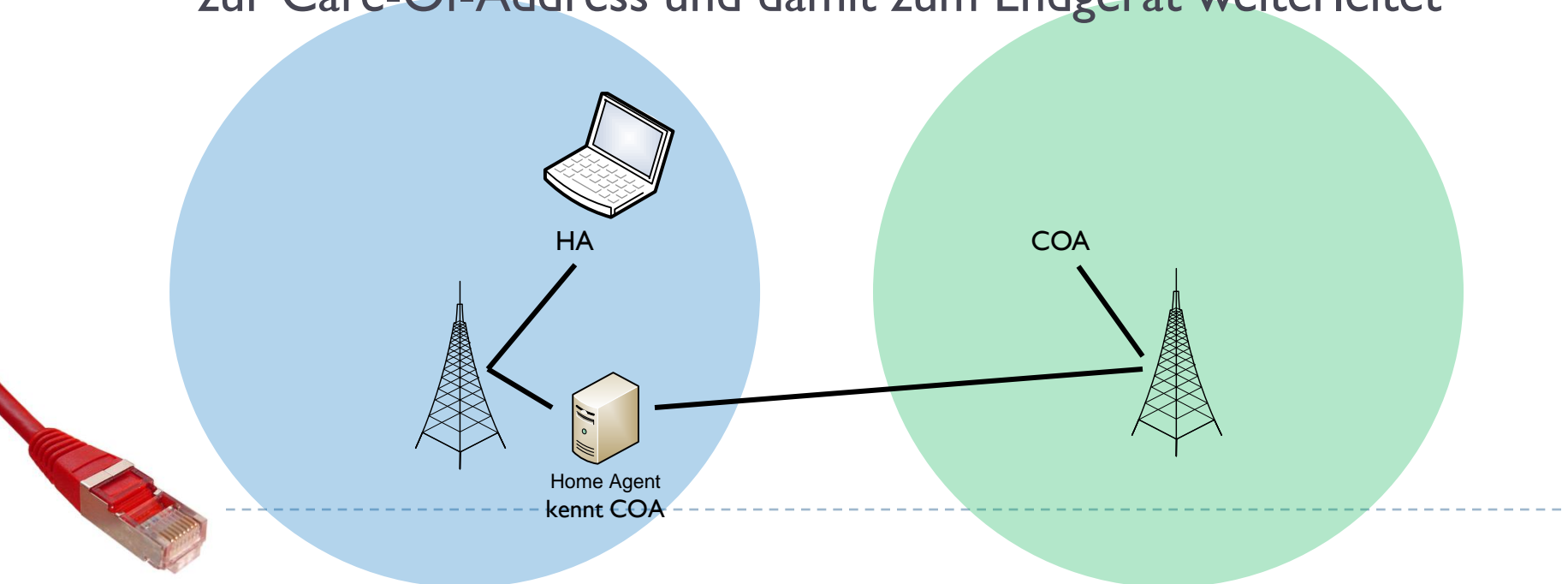


- ▶ Bei Mobile IP erhält das Endgerät (Mobile Host) zwei Adressen:
 - ▶ Home Address (HA)
 - ▶ Diese Adresse ist die statische Adresse des Endgeräts. Sie bleibt konstant erhalten, selbst wenn sich ein Endgerät bewegt.
 - ▶ Diese Adresse wird von anderen Geräten zur Kommunikation mit dem Endgerät genutzt
 - ▶ Care-Of-Address (COA)
 - ▶ Die COA wird von einem fremden Netz zugewiesen, wenn ein Rechner sich aus seinem Heimatnetz entfernt und an einem anderen Netz anmeldet



Mobile IP - Funktionsweise

- ▶ Wenn ein Mobile Host sein Heimatnetz verlässt und ein anderes Netz betritt...
- ▶ ...erhält er von diesem eine Care-Of-Address...
- ▶ ...die er seinem Home Agent mitteilt...
- ▶ ...welcher daraufhin sämtliche Pakete an die Home Address zur Care-Of-Address und damit zum Endgerät weiterleitet



Mobile IP - Funktionsweise

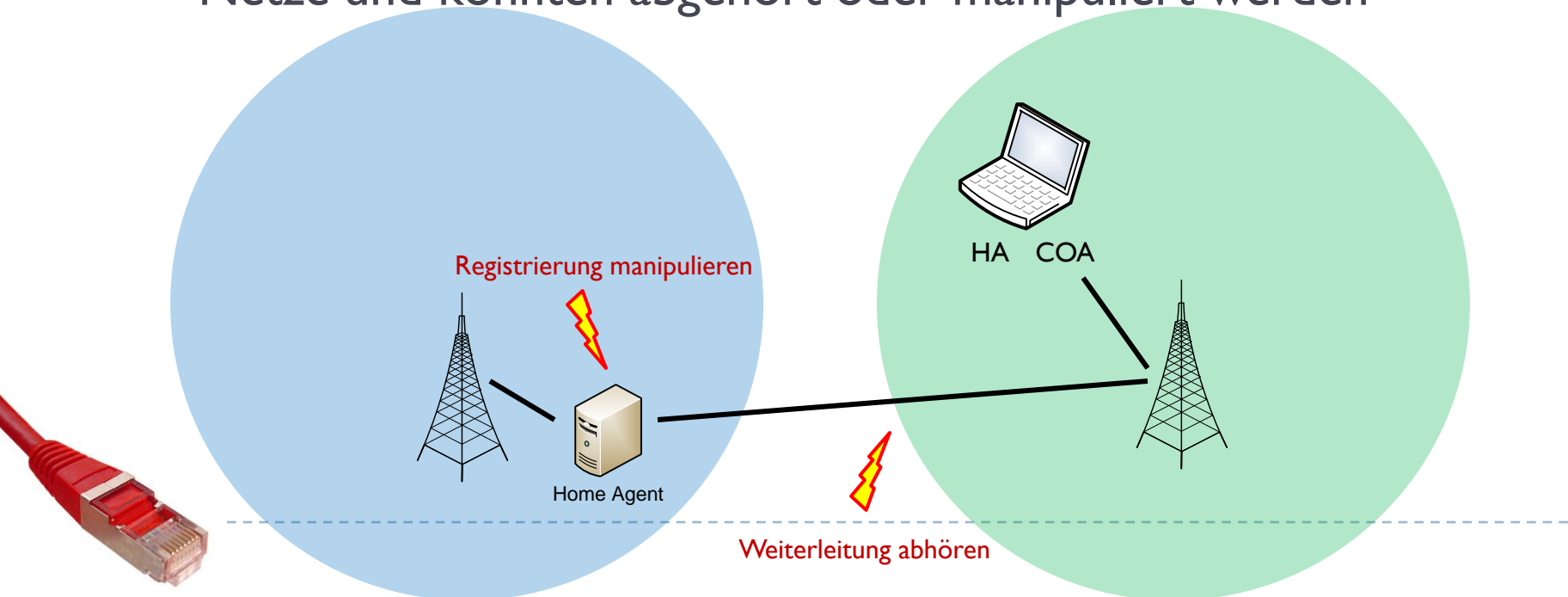
- ▶ Alternativ zur eben gezeigten Variante gibt es die Möglichkeit, einen Foreign Agent zur Weiterleitung der Daten im Zielnetz einzusetzen
 - ▶ Dabei meldet sich der Mobile Host beim Foreign Agent an und erhält keine echte IP-Adresse im fremden Netz
 - ▶ Der Foreign Agent kümmert sich anschließend um die Umleitung der Daten über den Home Agent zum Foreign Agent und schließlich zum Mobile Host, seine Adresse wird dazu als COA beim Home Agent registriert
- ▶ Nachteil dieser Variante: Foreign Agent in jedem potentiellen Zielnetz erforderlich



Mobile IP - Sicherheit

▶ Mögliche Angriffsszenarien

- ▶ Die Registrierung beim Home Agent könnte gefälscht werden, um Pakete zu einem Angreifer umzuleiten
 - ▶ Zweck: Paketinhalt mitlesen oder Denial-of-Service
- ▶ Weitergeleitete Pakete passieren evtl. unbekannte fremde Netze und könnten abgehört oder manipuliert werden

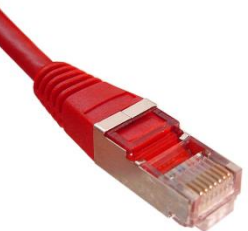


Mobile IP - Sicherheit



▶ Manipulation der Registrierung

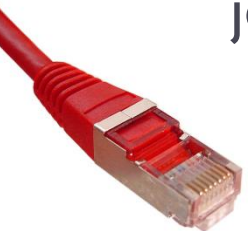
- ▶ Wichtig: Dieser Angriff kann potentiell von jedem Netz aus durchgeführt werden, welches sich als fremdes Netz für den Mobile Host eignet!
- ▶ Angreifer sendet eine gefälschte Registrierung in einem fremden Netz an den Home Agent, wobei er sich als das Opfer ausgibt und seine eigene IP-Adresse als Care-Of-Address spezifiziert
- ▶ Folge: Angreifer erhält sämtliche Netzwerkpakete des Opfers



Mobile IP - Sicherheit



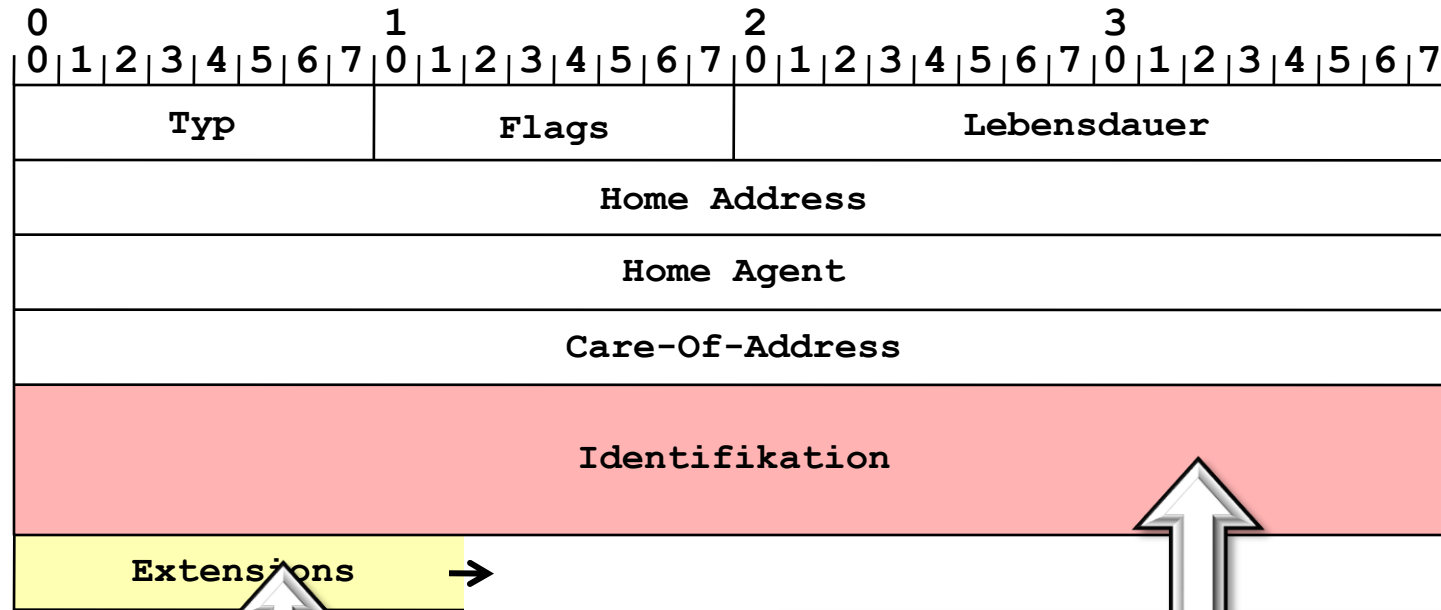
- ▶ Zur Unterbindung von gefälschten Registrierungen kann eine beidseitige Authentifizierung erzwungen werden
 - ▶ Im Mobile-IP-Standard vorgeschrieben: mindestens HMAC-MD5 mit 128 Bit Schlüssellänge (preshared key)
 - ▶ Ein MD5-Schlüssel von 64 Bit Länge wurde im distributed.net-Projekt nach 1757 Tagen verteilter Brute-Force-Attacke geknackt
 - ▶ Seit 2021 Tagen läuft ein verteilter Brute-Force-Angriff auf MD5-72, bislang ohne Erfolg nach Abdeckung von 0,5% des gesamten Keyspace
 - ▶ Daher: Authentifizierungsprozess auf Basis von MD5 kann zum jetzigen Zeitpunkt als ausreichend sicher angesehen werden



Mobile IP - Sicherheit



- ▶ Blick auf die Protokollebene: „Registration Request“
 - ▶ UDP-Paket auf Zielport 434



Eine Authentifizierungs-Extension ist Pflicht; der MAC umfasst die gesamte UDP-Payload bis zur Extension

Dient dem Schutz vor Replay-Attacken: Ein 64-Bit-Timestamp im NTP-Format oder Nonces

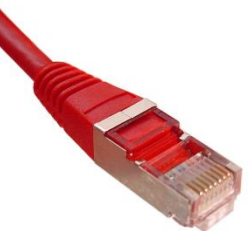
Mobile IP - Sicherheit

- ▶ Die Registration Requests können auf zwei Arten gegen Replay-Attacken geschützt werden
 - ▶ Möglichkeit I (verpflichtend): Timestamps
 - ▶ Sowohl Request als auch Reply werden mit aktuellen Timestamps im NTP-Format versehen
 - ▶ Die ersten 32 Bit des 64-Bit-Timestamps decken Sekundenbruchteile ab und müssen nicht zwingend korrekt sein, etwa wenn kein ausreichend genauer Zeitgeber vorhanden ist. In diesem Fall sollten sie mit Zufallswerten belegt werden.
 - ▶ Der Timestamp dient gleichzeitig als Sequence Number: nur wenn der Timestamp eines Requests weniger als (default) 7 Sekunden von der Uhrzeit des Home Agents abweicht und der Home Agent noch keinen Request mit höherem Timestamp erhalten hat, wird er akzeptiert.



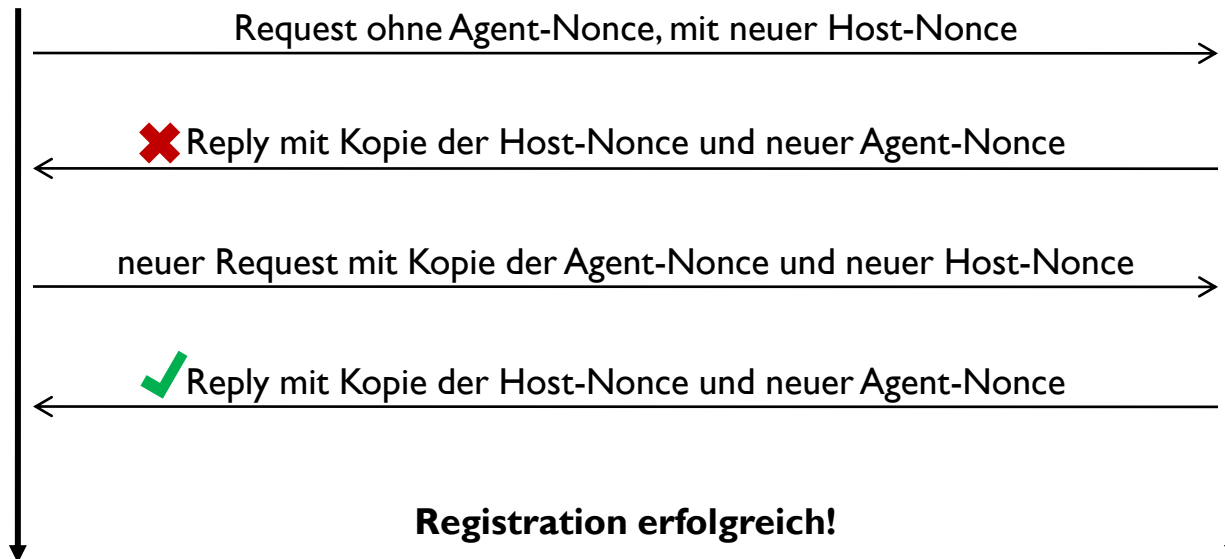
Mobile IP - Sicherheit

- ▶ Die Registration Requests können auf zwei Arten gegen Replay-Attacken geschützt werden
 - ▶ Möglichkeit 2 (optional): Nonces
 - ▶ Nonces sind Zufallszahlen, die von einem Teilnehmer einer Kommunikation einem anderen zugesendet werden, welcher durch das Einfügen der Nonce in seine nächste Nachricht beweist, dass er die Nachricht unmittelbar erstellt hat und nicht zuvor mitgehört und erneut abgesendet
 - ▶ Nonces funktionieren grundsätzlich nur, wenn sie innerhalb der Nachricht gegen Manipulation geschützt sind
 - Dies ist bei Mobile IP der Fall



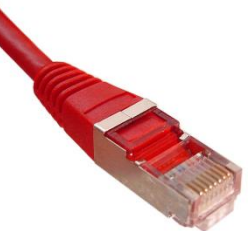
Mobile IP - Sicherheit

- ▶ Die Registration Requests können auf zwei Arten gegen Replay-Attacken geschützt werden
 - ▶ Möglichkeit 2 (optional): Nonces



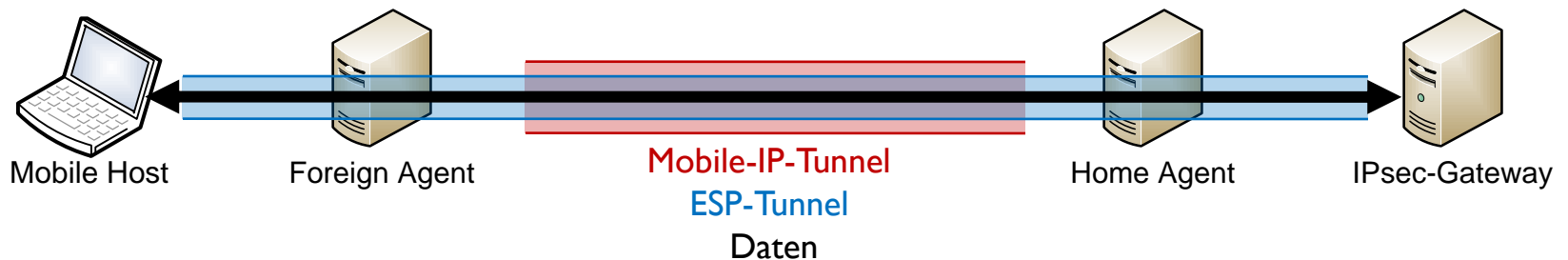
Mobile IP - Sicherheit

- ▶ Die Weiterleitung von Home Agent zu Mobile Host erfolgt via IP-in-IP-Tunneling (optional: IP-in-UDP)
 - ▶ Der Mobile-IP-Standard (RFC 3344) beschreibt keinerlei Absicherung dieses Tunnels!
 - ▶ Stattdessen müssen entweder die einzelnen Verbindungen (wie etwa bei SSH) verschlüsselt werden oder anderweitig ein verschlüsselnder Tunnel vorhanden sein
 - ▶ Eine solche Möglichkeit bietet etwa IPsec mit dem ESP-Protokoll



Mobile IP – Sicherheit – ESP

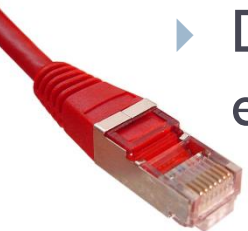
- ▶ ESP ist Teil der IPsec-Suite
- ▶ Das Protokoll bietet
 - ▶ Authentifizierung
 - ▶ Integritätsschutz
 - ▶ Vertraulichkeit
- ▶ ESP baut einen verschlüsselnden Tunnel zwischen zwei Kommunikationspartnern auf



Mobile IP - Sicherheit

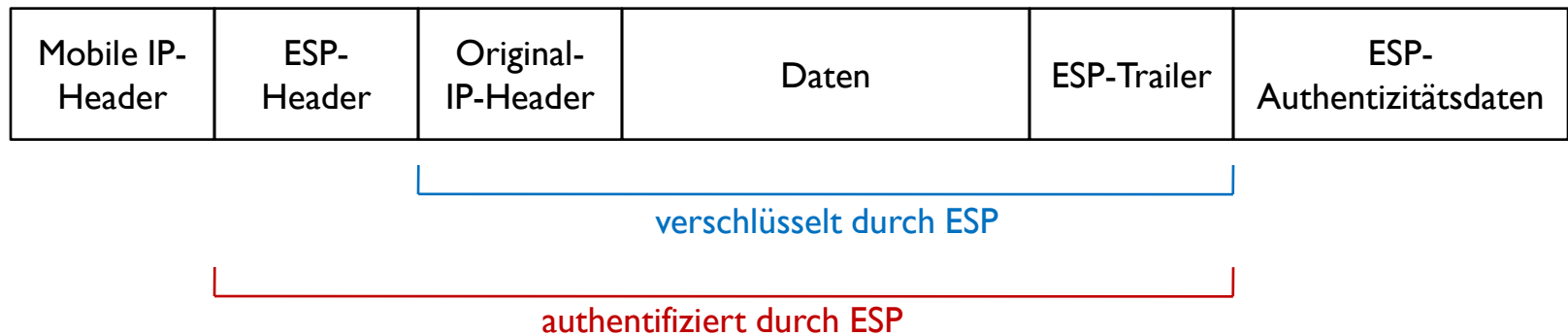


- ▶ **ESP bietet einen sogenannten Transport- und einen Tunnelmodus**
 - ▶ Im Transportmodus bleibt der IP-Header des Pakets unverändert, während der ESP-Header zwischen IP-Header und Nutzdaten (hier: das von Mobile IP gekapselte Datenpaket) eingefügt wird. Der Transportmodus wird für Host-zu-Host-Verbindungen genutzt.
 - ▶ Im Tunnelmodus kapselt ein neues IP-Paket mit eigenem IP-Header das zu tunnelnde IP-Paket.
- ▶ **Für die Rundum-Absicherung einer Mobile-IP-Session ist der Tunnelmodus geeignet**
 - ▶ Der Tunnel wird vom Mobile Host bis zum Home Agent oder einem separaten IPsec-Gateway im Heimatnetz aufgebaut



Mobile IP - Sicherheit

- ▶ ESP im Tunnelmodus kombiniert mit Mobile IP



Mobile IP - Sicherheit

- ▶ Mobile IP in Kombination mit IPsec/ESP bietet Sicherheit sowohl beim Management des Roamings selbst als auch bei der Datenweiterleitung
 - ▶ Vorteile
 - ▶ Roaming in beliebige andere Netzwerke möglich, ohne dass dort spezielle Hardware vorhanden sein muss
 - ▶ Sicherheit der Daten ist dabei jederzeit gewährleistet
 - ▶ Nachteile
 - ▶ erheblicher Protokoll-Overhead speziell bei kleinen Paketgrößen
 - ▶ Home Agent sowie IPsec-Gateway im Heimatnetz erforderlich
 - ▶ Probleme mit NAT -> NAT-Traversal erforderlich!
-

