IPSEC

Internet Protocol SECurity

Thomas Bader

<thomasb@trash.net>

Einführung

- Schreibweisen: IPsec oder IPSEC
- Bereitstellen von Sicherheitsfunktionen auf dem IP Layer
- Framework, bestehend aus drei Protokollen

Alternativen

- OpenPGP
- SSH
- SSL/TLS

Vor- und Nachteile

- IPSEC ist der allgemeinste Weg
- IPSEC ist für Benutzer transparent
- IPSEC ist nicht sicherer als die Systeme, die es benutzen
- Kein Ersatz für Protokolle auf höherem Level
- Anfällig gegen Traffic Analysis

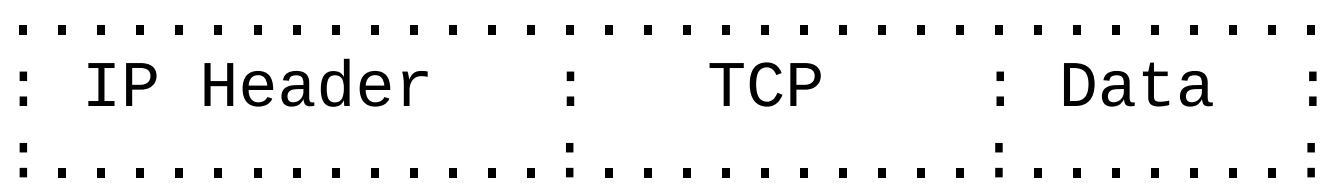
Ziele

- Authentifizierung
  Empfangene Daten kommen von der angegebenen Quelle
- Integrität
  Daten sind auf dem Sendeweg nicht manipuliert worden
- Vertraulichkeit
  Unbeteiligte Personen können Daten nicht entziffern

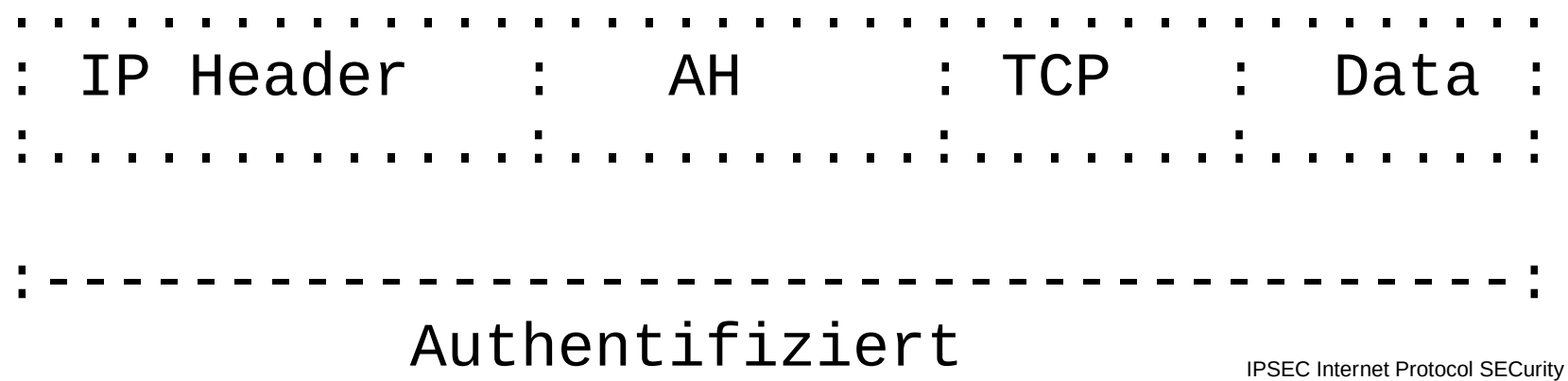
IP Authentication Header

- Kurz AH, authentifiziert Packete
- RFC 2402

Vor der Benutzung von AH:

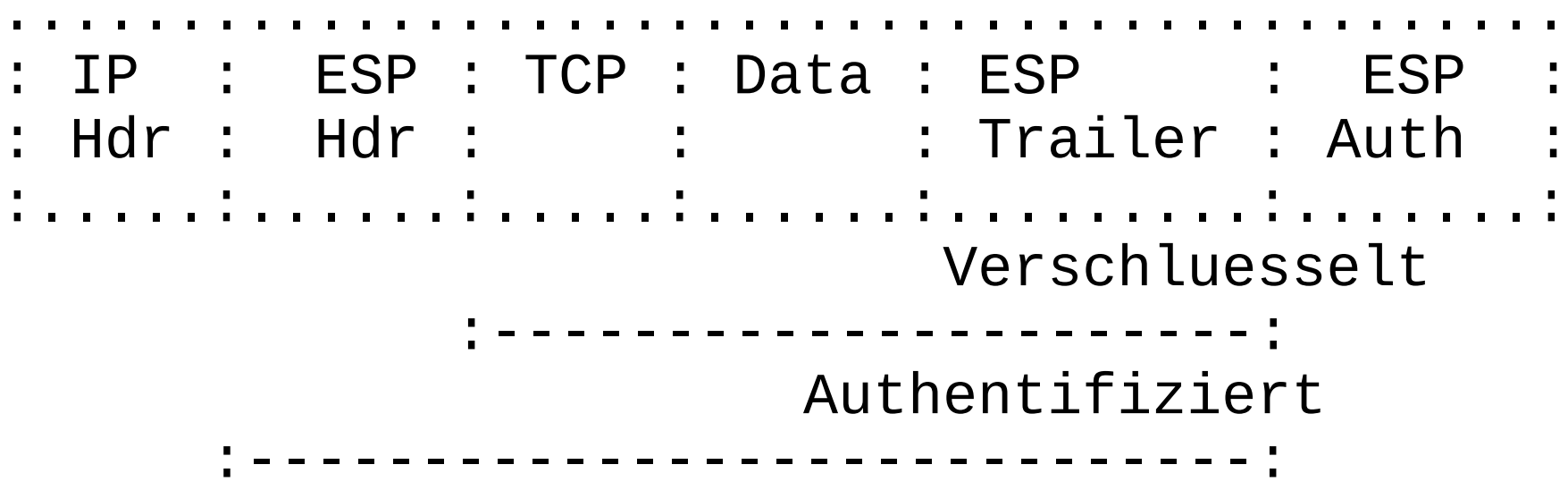


Nach der Benutzung von AH:



IP Encapsulating Security Payload

- Kurz ESP, verschlüsselt und/oder authentifiziert Daten
- RFC 2406



Internet Key Exchange

- Kurz IKE
- RFC 2409
- Handelt Verbindungsparameter aus:
  Algorithmen
  Schlüssel
  Verbindungsdauer
- Benutzt Diffie-Hellman Key Agreement
- Tauscht Daten über Port 500/udp aus

Kryptografische Komponenten

- Block Cipher
  Symetrische Verschlüsselung
  DES bzw. 3DES sind bekannte Block Cipher
- Hash Funktionen
  Stellt Integrität fest
  Im Fall IPSEC: HMAC
  Andere, bekannte Hash Funktionen: MD5, SHA

Kryptografische Komponenten (2)

- Diffie-Hellman Key Agreement
  Schlüssel zwischen zwei Parteien aushandeln
  Mithörer kann Key nicht in Erfahrung bringen
- RSA
  Public Key Algorithmus
  Benannt nach Erfindern (Rivest, Shamir, Adleman)

Links

- http://www.ietf.org/html.charters/ipsec-charter.html
- http://www.tml.hut.fi/Tutkimus/IPSEC/

```
$Id: ipsec.slides.tex,v 1.4 2002/07/17 20:10:00 thomasb Exp $
```