Attacking the IPSec Standards in Encryption-only Configurations

Ein Vortrag von Martin Skrodzki

Nach dem Paper von

Jean Paul Degabriele und Kenneth G. Paterson

1 Einführung ins Thema

- Encryption-only Systeme sind als angreifbar bekannt
- Statt einer Neuauflage des IPsec Standards gibt es mehr Warnungen bei Encryption-only
- Warnungen bleiben vielfach unbeachtet
- Paterson & Yau: Ohne Post-Processing Policy-Checks ist System angreifbar
- Hier: generelle Anwendbarkeit, d.h. Angriff auf Standard
- Voraussetzung: in RFC‘s empfohlene Padding-Checks (sonst sind andere Attacken möglich → Bellovin)
- IPsec bei Encryption-only IMMER angreifbar (Bsp. OpenSolaris)

1.1 Kurzbeschreibung der Attacken

- Attacken möglich bei neuester IPsec Generation: RFCs: 4301-4309 und zweiter Generation: RFCs: 2401-2411
- Alle Inhalte werden entschlüsselt
- Nicht gesamter Verkehr eines Hosts (P&Y), sondern nur Verkehr des Tunnels muss gelesen werden können
- Fokus auf ESP im Tunnel-Mode, Transport-Mode analog

1.1 Kurzbeschreibung der Attacken (2)

- Idee der Attacken: wie in P&Y, 2006: Manipulation der Header-Fields, Erzeugen von ICMP-Nachrichten
- Ausnahme (zu Annahmen von P&Y): Padding-Checks werden korrekt ausgeführt
- Idee: falsches Padding führt zu ICMP-Nachrichten, damit wird ESP Padding Orakel gebaut
- Wichtig bei den Attacken: praktische Ausführbarkeit

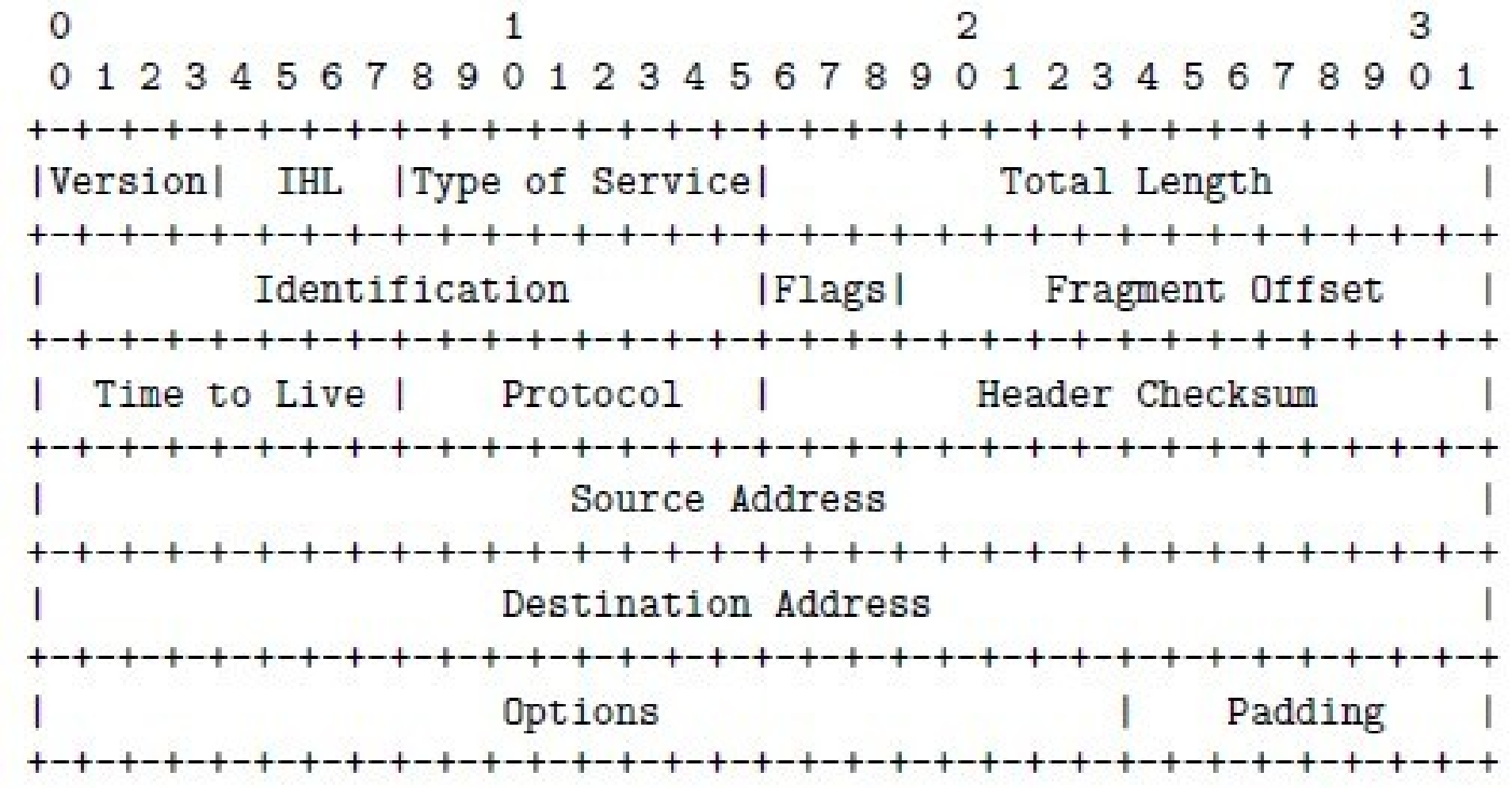
2.1 Padding und Depadding bei Tunnel-Mode ESP

- Padding: Inneres Datagramm als Sequenz von Bytes, wird gefüllt, mit Padding-Length- (PL) und Next-Header- (NH) Byte versehen
- Verschiedene Padding-Methoden, meistens jedoch benutzt:
  - 1: Gesamtzahl der Bytes (inklusive PL und NH) wird an eine Blockgröße angepasst
  - 2: Das Padding ist ein Null-String oder t Bytes mit 1,2,…,t und 1<= t <= 255

2.1 Padding und Depadding bei Tunnel-Mode ESP (2)

- NH-Byte: Protokoll-Implementation, der die Daten übergeben werden
- Tunnel-mode: NH=4 (IP-in-IP encapsulation)
- Depadding: Das Padding wird abgeschnitten, sollte jedoch geprüft werden
- Rekonstruktion des inneren Datagramms: Policy Checks, Drop des Pakets bei Fehler

2.2 IP Datagram Header



2.3 ICMP & IPSec

- Zwei Fälle für ICMP-Messages wurden bereits aufgezeigt: „time exceeded“ und „protocol unreachable“ (s. P&Y 2006, Vortrag André)
- Format, Länge und Inhalt der ICMP-Msg hängen vom Fehler und der ICMP-Implementation ab
- Zwei Arten von ICMP-Messages:
  - Error – Message
  - Non-Error – Message (mit eigener Security Association (SA))

2.3 ICMP & IPSec (2)

- Zwei Fälle von Error-Messages:
  - Fehler bei Abarbeitung vom IPsec Paket
  - Transitfehler (Übertragungsfehler)
- Zwei Fälle beim Auftritt einer ICMP-Msg:
  - SA existiert oder es wird eine erstellt, alles läuft normal weiter
  - SA existiert nicht, es darf keine erstellt werden: Es muss die SA für Antworten auf dem Kanal verwendet werden, auf dem der Fehler auftrat

2.3 ICMP & IPSec (3)

- Eine ICMP-Message wird also wie andere Payloads als Datagramm über IP im gesamten Netzwerk verschickt
- Problem: wie erkenne ich eine verschlüsselte ICMP-Message?
- Erkennbar ist eine ICMP-Message an der Länge oder durch andere Techniken (s. Kapitel 4)

3 Padding Oracle Attacks

- Der Angreifer hat in dieser Attacke Zugang zu einem „Padding Orakel“, das bei Erhalt eines Chiffreblocks ein einzelnes Bit ausgibt, das die Korrektheit des Paddings angibt
- Geht man von der Existenz eines passenden Padding Orakels aus, kann man in CBC-Mode Encryption ein Decryption Orakel bauen.
- (s. S. Vaudenay, Security Flows induced by CBC Padding ..., Eurocrypt 2002)

3 Padding Oracle Attacks (2)

- o.B.d.A. ist das NH Byte nicht präsent, das PL Byte ist das least significant Byte eines Blocks
- *[siehe hier das Beispiel aus dem Paper]*

3.1 Applicability to IPSec

- Die obige Attacke funktioniert leider nicht ohne Modifikation gegen IPSec
- Zunächst ist kein solches Padding Orakel bekannt
- Weiter wird das NH-Byte nicht beachtet und dessen Effekt auf die weitere Abarbeitung der Daten
- IPSec verwirft die Daten (im Tunnel-Mode) nur dann nicht, wenn das NH-Byte gleich 4 ist, also die Daten weiter an IP gehen
- Es wird nun davon ausgegangen, dass ein Paket gedroppt wird, falls $NH \neq 4$ ist.

4 A Tutorial Chosen Plaintext Attack

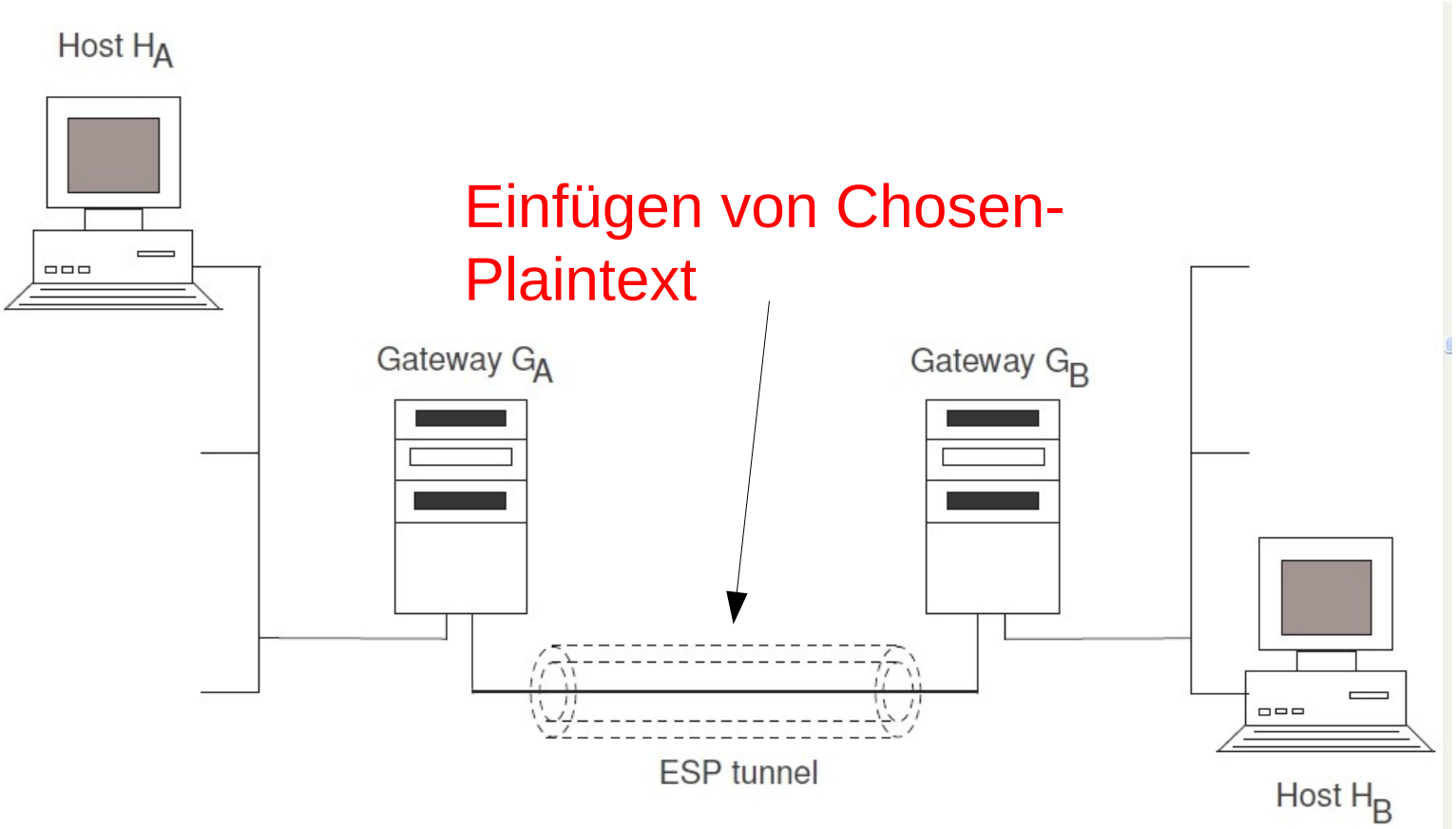
- o.E. Block-Größe von 64 Bit
- Voraussetzungen:

1. Encryption-only ESP, wie in Fig 3 (typische VPN-Konstellation)
2. Der Schlüssel K ist konstant während der Attacke
3. Der Angreifer hat Zugriff auf ESP-gesicherte Pakete zwischen den zwei Gateways
4. Der Angreifer kann modifizierte Pakete in das Netzwerk zwischen A und B einfügen

- Folgt: Konstruktion einer adaptiven Chosen-Plaintext Attacke, um ICMP-Nachrichten zu generieren und zu detektieren und damit schrittweise Plaintext-Bytes zu erhalten
- Komplexität: O(2^16)

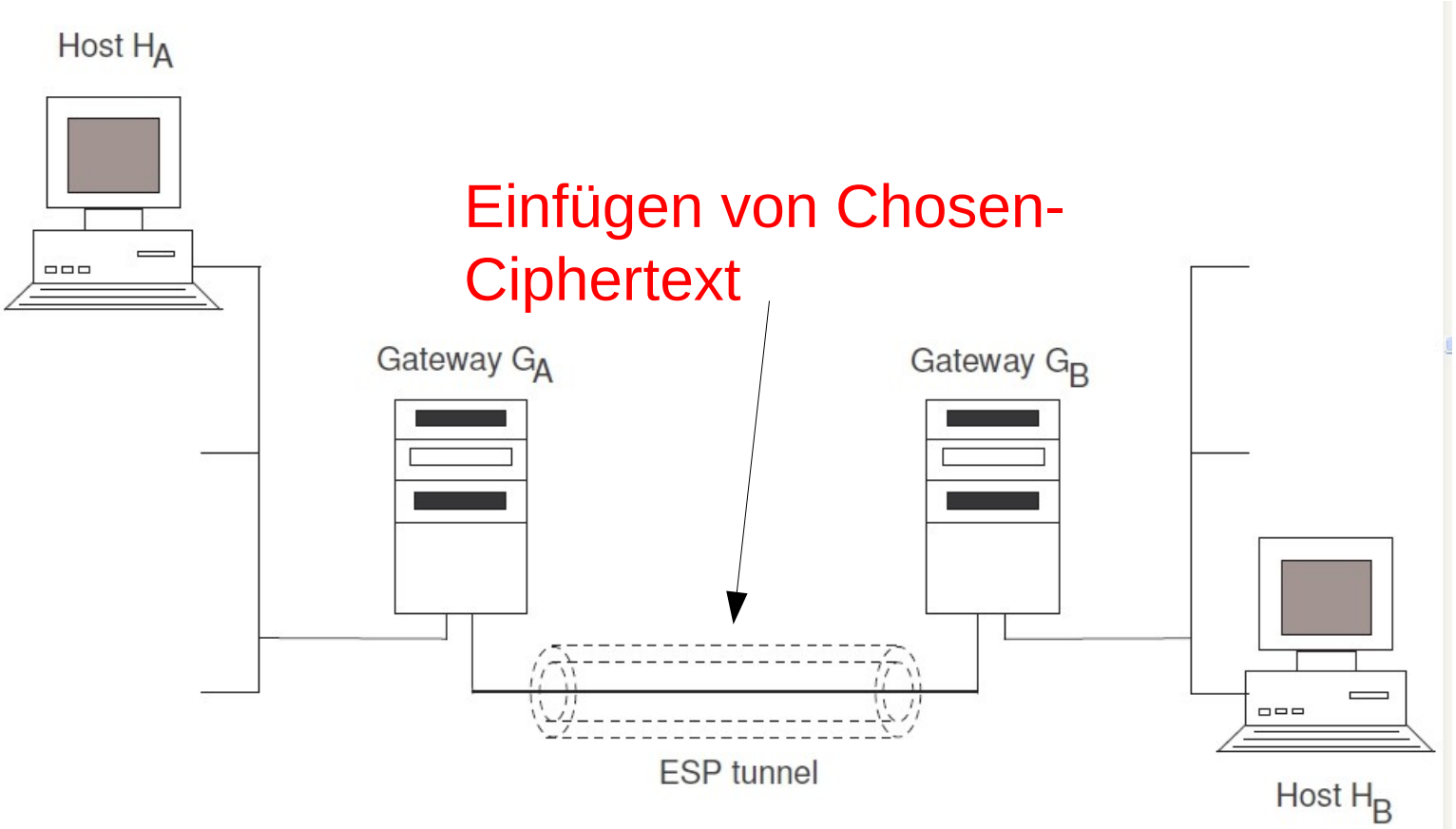
4 A Tutorial Chosen Plaintext Attack (2)

- Das VPN-Netz für die Attacke:



5 An Attack based on Options processing

- Das VPN-Netz für die Attacke:



5 An Attack based on Options processing (2)

- Idee: Änderung eines Chiffrentexts, so dass eine ICMP auf Grund von falscher Optionen-Abarbeitung entsteht, dieser Chiffrentext bildet Padding Orakel, wie in 4
- Verfahren funktioniert wie analoges Verfahren bei P&Y und Kapitel 4
- Statt des Options-Field kann analog das Protocol-Field benutzt werden

Conclusion

- Wir sind nicht auf alle technischen Details eingegangen, aber:
- Ipsec in Encryption-only ESP tunnel-Mode (und transport-Mode) ist bei CBC-Mode Encryption selbst bei standardkonformer Implementierung praktisch angreifbar
- Encryption-only bei aktiven Angreifern ist UNSICHER!