>Schwachstelle Schnittstelle

Angriffspunkt für Datenspione?

Hannes Federrath • TU Dresden / Freie Universität Berlin

- Begriffsbestimmung
- Handover Interface
- Betroffene Netze
- Bereitzustellender Überwachungsumfang
- Bedrohungen durch Überwachungsschnittstelle
- Sicherheitsfunktionen und deren Bewertung
- Zusammenfassung

> Begriffsbestimmung

- Überwachungsschnittstelle:
  - Der physische Ort innerhalb einer Telekommunikationseinrichtung des Netzbetreibers bzw. Dienstanbieters, an dem der überwachte Fernmeldeverkehr und verbindungsrelevante Daten den gesetzlich ermächtigten Behörden (Bedarfsträger) bereitgestellt werden.
  - Nicht notwendigerweise ein einzelner, fester Punkt

nach Glos. Abl. 96/C 328/019

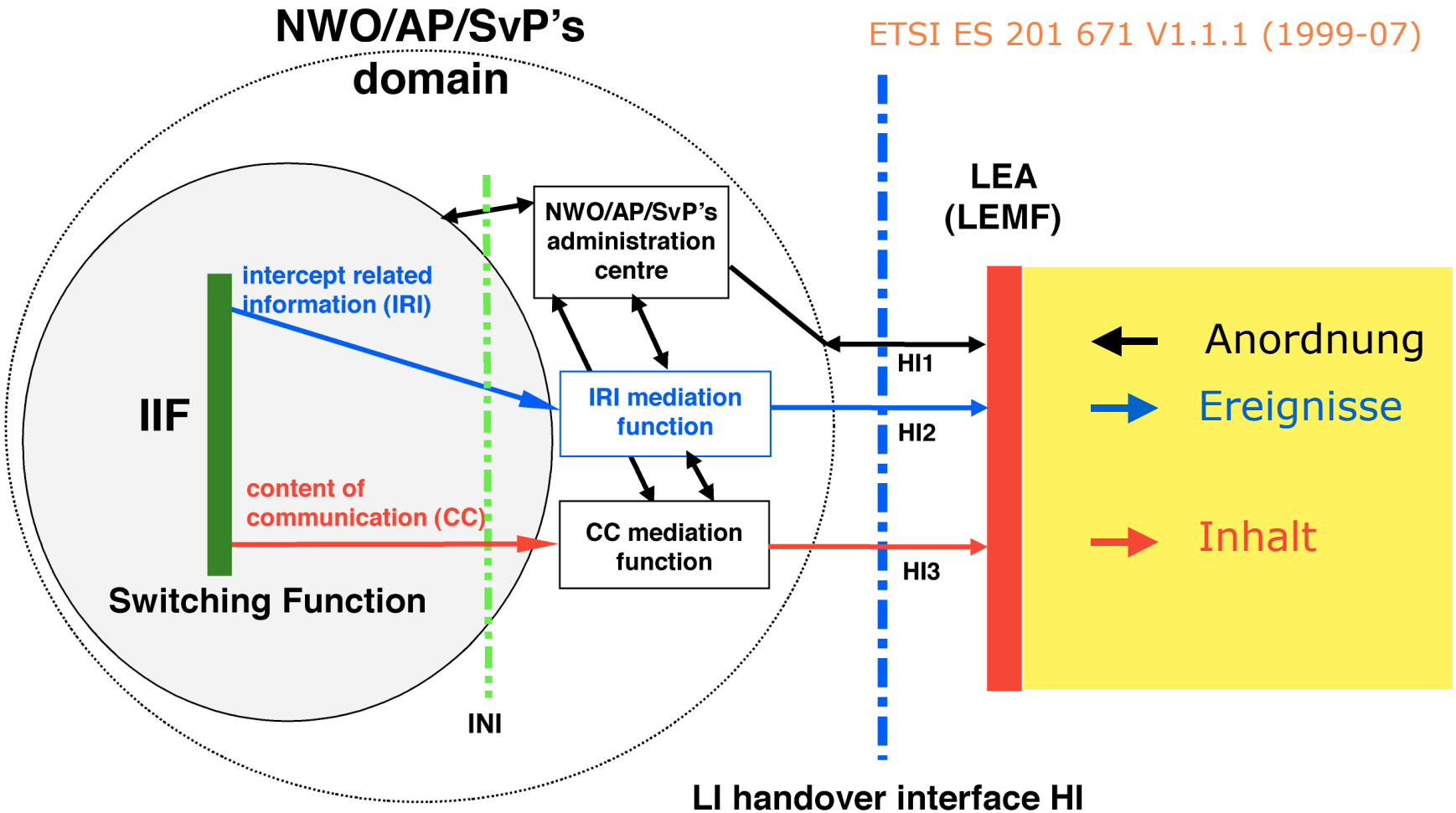
- In englischsprachigen Dokumenten Unterscheidung nach:
  - Handover interface: entspricht etwa der o.g. Begriffsbestimmung von Überwachungsschnittstelle
  - Interception interface: physischer und logischer Punkt innerhalb der Anlagen des Netzbetreibers/Dienstanbieters, an dem die
    - Ereignisdaten (Verbindungsversuche, Konfigurationsänderungen etc.)
    - Inhaltsdaten

    dem Bedarfsträger zur Verfügung gestellt werden.

ETSI ES 201 671 V1.1.1 (1999-07)

> Handover Interface

ETSI ES 201 671 V1.1.1 (1999-07)



LI handover interface HI

HI1: administrative information
HI2: intercept related information
HI3: content of communication

IIF: internal interception function
INI: internal network interface

> Welche Netze und Dienste sind betroffen?

- Leitungsvermittelnde Netze
  - Fokus: klassische Telefonie
  - ISDN, einfaches analoges Telefon, Mobilfunknetze, …
- Paketvermittelnde Netze
  - Fokus: Datenübertragung
- Funkrufnetze
- ATM-Netze
- Zugang zum Internet (nur Zugangsvermittlung)

Quelle: TR FÜV, Ausgabe 2.2, Dezember 2000

- Auch Internet-Dienste selbst?
  - Beispiele: Freemail-Anbieter, Internet-Kaufhäuser ohne ISP-Funktion
  - Keine explizite Nennung …
- Regelwerk (TR FÜV, ETSI ES 201 671) ist (noch) sehr Telefonie-lastig

> Bereitzustellender Überwachungsumfang

- TR FÜV nennt hierzu eine Empfehlung: $M = 0{,}75 \quad x^{0{,}45} + p$

  M: Zahl der aktivierbaren Maßnahmen

  x: Gesamtzahl an analogen Telefonanschlüssen, B-Kanäle im ISDN, Mobilfunkanschlüsse pro Netzknoten

  p: p=30, wenn Primärmultiplexanschlüsse vorhanden, sonst p=0

- Mit p=0:

x =	100	1.000	10.000	100.000
M =	6	17	48	134

  + (p=30), falls Primärmultiplexanschlüsse

- Kleinere Anbieter sind durch diese Anforderungen viel stärker belastet als große.

> Bedrohungen durch Überwachungsschnittstelle

Angriffe auf

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

der Überwachungsmaßnahme.

Angreifer z.B.:

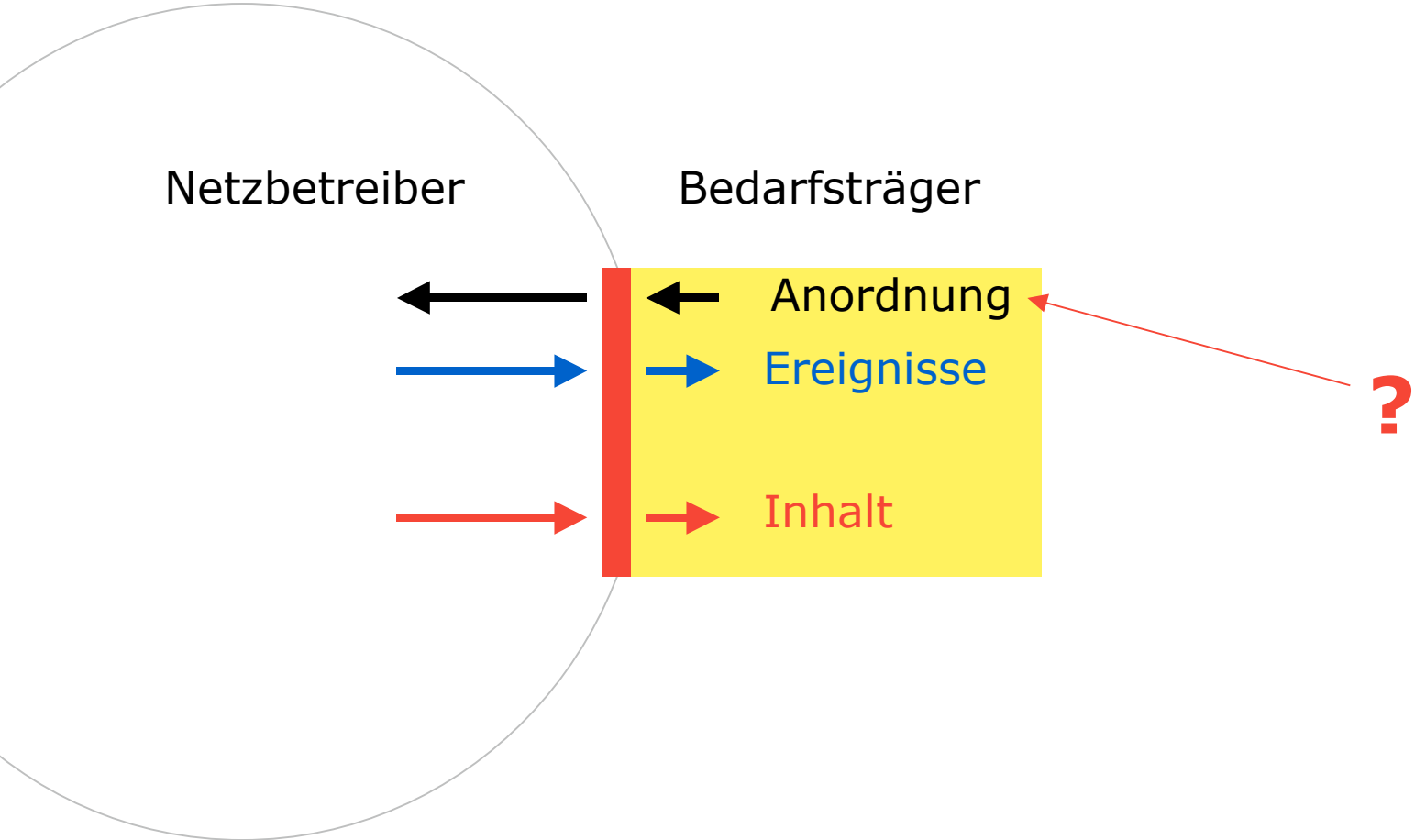
- Fremde Geheimdienste
- Organisiertes Verbrechen
- Hacker

Angreifer könnte z.B

- Erfahren wollen, welche Anschlüsse derzeit überwacht werden,
- Unberechtigt auf überwachte Anschlüsse zugreifen,
- Zum Bedarfsträger übermittelte Daten mithören, verändern,
- Unberechtigt Überwachungsmaßnahmen „einleiten".
- Überwachungsmaßnahmen stören, verhindern, verzögern.

Verbindung zwischen Netzbetreiber und Bedarfsträger

- Anschlüsse beim Netzbetreiber nur für gehende Verbindungen
- Anschlüsse beim Bedarfsträger nur für kommende Verbindungen



Übermittlung der Überwachungsanordnung

- Bisher manuell und basiert auf Papier

- Angedacht:
  - Elektronische Übermittlung
- Unbedingt notwendig:
  - **Digitale Signatur**

Digitale Signatur

Gegenseitige Identifizierung und Authentisierung?

- Authentifizierung wird in der Richtlinie ausdrücklich gefordert!
- Schwache Lösung:
  - Überprüfung der Rufnummern durch COLP/CLIP (Connected Line Identification Presentation/ Calling Line Identification Presentation)
  - Relevante Datenfelder sind in nicht gegen Verfälschung geschützt.
- *Message Authentication Codes oder Digitale Signatur?*
  - Fehlanzeige !
- Produkte für starke Authentisierung im ISDN existieren!

Geheimhaltung der Zielrufnummer

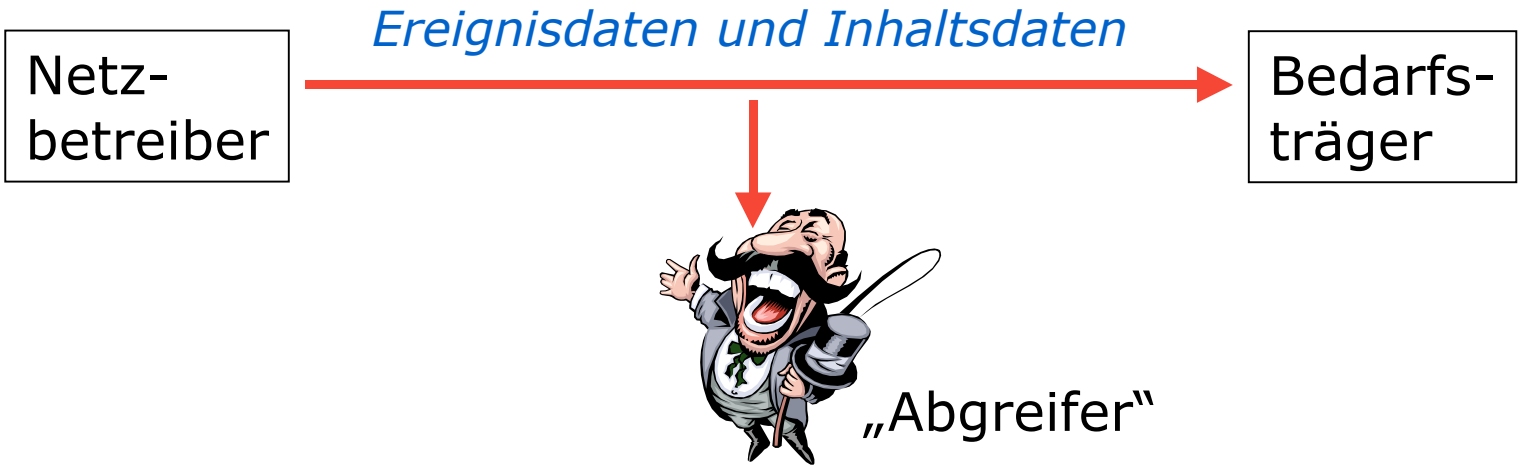
- Für jede Überwachungsmaßnahme wird von Bedarfträger individuelle Zielrufnummer angegeben.
  - Rufnummer: „VS–Nur für den Dienstgebrauch“
  - *Security-by-obscurity*

Denial-of-Service-Angriffe

- Schutz vor Denial-of-Service-Angriffen auf Überwachungsmaßnahme
- TR FÜV:
  - „Es ist zu verhindern, daß unberechtigte Benutzer die Einrichtungen bei Bedarfsträger anwählen können und diesen stören, blockieren oder überwachten Verkehr simulieren“
- Closed User Group, verwaltet durch die Regulierungsbehörde

Vertrauliche Datenübermittlung?

- *Verschlüsselte Übermittlung von Ereignisdaten und Inhaltsdaten?*
  - Fehlanzeige!
- TR FÜV:
  - „Der Inhalt der Datensätze ist dem Bedarfsträger unkodiert im Klartext zu übermitteln.“



- Produkte für starke Verschlüsselung im ISDN und Internet existieren!

> Zusammenfassung

- Die geforderten Sicherheitsfunktionen
  - entsprechen bei Weitem nicht dem, was technisch möglich und zumutbar ist,
  - schützen allenfalls vor Angriffsversuchen durch Unbedarfte,
  - gefährden dadurch schlimmstenfalls Unbeteiligte.

- Hauptrisiken:
  - fehlende starke Authentisierung,
  - fehlende (bzw. nicht vorgeschriebene) Verschlüsselung zwischen Netzbetreiber und Bedarfsträger,

  - fehlendes (bzw. nicht vorgeschriebenes) Logging und fehlende technische Nachvollziehbarkeit der Überwachungsmaßnahme
    - „Diese Situation ist der Traum eines jeden Hackers“

      aus: CCC-Presseerklärung 31. Juli 1996 zum §90 TKG