in: Bernd Holznagel, Ursula Nelles, Bettina Sokol (Hg.): Die neue TKÜV (Telekommunikations-Überwachungs-Verordnung) – Die Probleme in Recht und Praxis, Schriftenreihe Information und Recht, Bd. 27,Verlag C. H. Beck, München 2002, 115-123.

Schwachstelle Schnittstelle — Angriffspunkt für Datenspione?

Beitrag zum Symposium „Die neue TKÜV — Innere Sicherheit auf Kosten von Netzbürgern und Providern?" am 11. Mai 2001 in Münster

Dr.-Ing. Hannes Federrath, Freie Universität Berlin, Institut für Informatik

1 Einleitung

Ziel der Strafverfolgungsbehörden ist es, den Bürger vor Verbrechen zu schützen. Wenn Kriminelle die moderne Telekommunikationstechnik nutzen, um Verbrechen zu begehen, darf Technik auch helfen, Kriminelle zu enttarnen. Über speziell für die Strafverfolgung geschaffene Einrichtungen, so genannte Überwachungsschnittstellen, soll dieses Ziel erreicht werden.

Ziel beim Design von Überwachungsschnittstellen muss es auch sein, Verbrechen, die über bzw. mittels Überwachungsschnittstellen durch Kriminelle verübt werden könnten, mit allen Mitteln zu verhindern. Im engeren Sinn bedeutet dies, dass eine Überwachungsschnittstelle sicher sein muss vor Missbrauch. In diesem Papier soll erstens untersucht werden, ob dieses Schutzziel von den existierenden technischen Spezifikationen von Überwachungsschnittstellen erreicht wird, zweitens sollen Empfehlungen für die technische Ausgestaltung künftiger Überwachungsschnittstellen gegeben werden.

Überwachungsschnittstellen sind sowohl von Netzbetreibern als auch Dienstanbietern zu implementieren. Zur Vereinfachung der Darstellung wird der Begriff Netzbetreiber als Synonym für beide Betroffene verwendet.

2 Begriffsbestimmung

Eine Überwachungsschnittstelle ist der physische Ort innerhalb einer Telekommunikationseinrichtung des Netzbetreibers, an dem der überwachte Fernmeldeverkehr und verbindungsrelevante Daten den gesetzlich ermächtigten Behörden (Bedarfsträger) bereitgestellt werden. Eine Überwachungsschnittstelle ist nicht notwendigerweise ein einzelner fester Punkt (nach Glos. Abl. 96/C 328/019).

In englischsprachigen Dokumenten, konkret dem Meta-Standard ETSI ES 201 671 V1.1.1 (1999-07) des European Telecommunications Standards Institute, wird unterschieden nach Handover Interface und Interception Interface.

Die Definition von Handover Interface entspricht in etwa der oben genannten Begriffsbestimmung von Überwachungsschnittstelle.

Ein Interception Interface ist der physische und logische Ort innerhalb der Anlagen des Netzbetreibers, an dem die

- Ereignisdaten (Verbindungsversuche, Konfigurationsänderungen, Wechsel der Funkzelle etc.) und
- Inhaltsdaten

dem Bedarfsträger zur Verfügung gestellt werden.

3 Handover Interface

Nach dem Standard ETSI ES 201 671, auf dessen Grundlage auch die deutschen Überwachungsschnittstellen realisiert sein sollen, hat eine Überwachungsschnittstelle drei Sub-Schnittstellen: Über eine administrative Schnittstelle wird dem Netzbetreiber die Überwachungsanordnung zugestellt. Die beiden anderen Schnittstellen dienen der Übermittlung der Ereignisdaten und Inhaltsdaten zum Bedarfsträger.

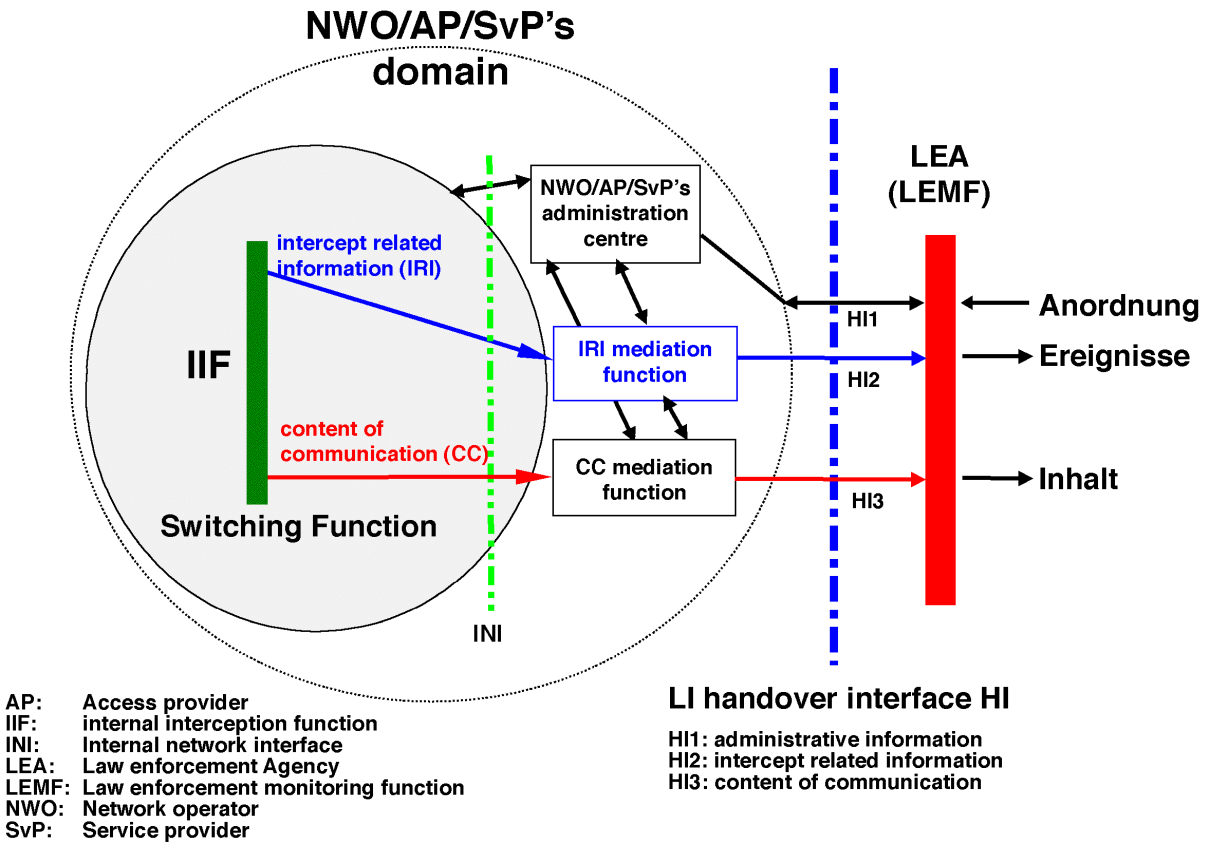

Abbildung 1. Handover Interface

In der Technischen Richtlinie zur Fernmeldeüberwachungsverordnung (TR FÜV, Ausgabe 2.2, Dezember 2000) sind folgende Netze betroffen, d.h. die Netzbetreiber müssen eine Überwachungsschnittstelle auf ihre eigenen Kosten zur Verfügung stellen:

- Leitungsvermittelte Netze: Der Fokus liegt hier in der Überwachung der klassischen Telefonie (einfaches analoges Telefon, ISDN, Mobilfunknetze etc.) und von Telefax.
- Paketvermittelnde Netze: Hier liegt das Interesse der Strafverfolger im Abhören von Datenübertragungen.
- Funkrufnetze,
- ATM-Netze, sowie
- Zugang zum Internet: Dies betrifft die Zugangsvermittlung zum Internet, d.h. so genannte Access Provider.

Nach dem Entwurf der neuen TKÜV vom 25.01.2001 sollen künftig auch Internet Service Provider (ISP) eine Überwachungsschnittstelle bereitstellen, selbst dann, wenn sie nicht als Access Provider tätig sind.

Ob Internet-Dienste (sog. Teledienste, im Gegensatz zu Telekommunikationsdiensten) davon betroffen sind, geht nicht klar aus den Formulierungen hervor. So ist beispielsweise unklar, ob Freemail-Anbieter, Internet-Kaufhäuser ohne ISP-Funktion etc. ebenfalls Überwachungsschnittstellen implementieren müssen. Da Teledienste nicht explizit genannt werden, ist davon auszugehen, dass sie nicht betroffen sind. Insgesamt sind die Formulierungen in den Regelwerken (TR FÜV, ETSI ES 201 671) noch sehr „telefonielastig" und darüber hinaus könnte der Eindruck entstehen, die Formulierungen wurden (wenigstens aus der Sicht des Technikers) scheinbar diffus genug gewählt, um den staatlichen Stellen nicht womöglich vorab Überwachungsmöglichkeiten zu nehmen. Dies führt – zumindest für Nicht-Experten im juristischen Bereich – zu erheblicher Rechtsunsicherheit.

Es stellt sich beispielsweise die Frage, ob ein Mehrwertdienst-Betreiber auf dem Gebiet Sicherheit im Internet unter die Regelungen fällt: Anbieter von Software und Dienstleistungen zum Verwischen von Datenspuren zum Selbstschutz der Bürger im Internet würden dann ihrer geschäftlichen Grundlage beraubt, weil sie Spuren, die sie ja verschleiern wollen, nun ausnahmslos zum Zwecke der Strafverfolgung erheben

(und ggf. speichern) müssten. Diese Benachteiligung dürfte ein erheblicher Eingriff in die Grundrechte der Bürger und die freie Entfaltung eines Marktes für solche Sicherheits- und Selbstschutz-Technologien sein.

4 Bereitzustellender Überwachungsumfang

Die TR FÜV nennt eine Empfehlung, welchen Umfang an Übertragungskanälen ein betroffener Netzbetreiber zum Bedarfsträger vorzuhalten hat. Die Gleichung $M = 0{,}75 \cdot x^{0{,}45} + p$ mit M als Anzahl der aktivierbaren Maßnahmen und x als Gesamtzahl an analogen Anschlüssen, B-Kanälen im ISDN oder Mobilfunkanschlüssen pro Netzknoten bestimmt dabei den Aufwand. Die Konstante p ist 0, wenn der Netzbetreiber seinen Kunden keine Primärmultiplexanschlüsse anbietet, andernfalls ist p = 30.

Beispiel: Mit p=0:

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

+ (p = 30), falls Primärmultiplexanschlüsse

Obwohl diese Zahlen noch keinerlei „Sockelaufwand" berücksichtigen, lässt sich bereits ablesen, dass kleinere Anbieter durch diese Anforderungen viel stärker belastet sind als große.

Die skizzierte Gleichung betrifft vornehmlich die Telefonüberwachung. Für die Beurteilung der vorzuhaltenden Überwachungskapazitäten im Bereich des Internet ist die o.g. Empfehlung völlig untauglich. Gründe hierfür sind:

Die Bandbreiten im Teilnehmeranschlussbereich sind deutlich uneinheitlicher.

Die künftig zu erwartenden Übertragungskapazitäten mehrerer Überwachungsmaßnahmen im Internet sind selbst beim besten Willen nicht mehr komplett speicher-, verarbeit- und analysierbar. So besteht z.B. die Möglichkeit, dass die Intelligenteren unter den Überwachten derart viel unsinnige Kommunikation betreiben werden, wodurch die relevanten Daten in einem völlig unübersichtlichen „Datenwust" untergehen.

Darüber hinaus bietet die Anwendung kryptographischer und steganographischer Techniken weiteren Schutz gegen Überwachung. Entsprechende Software ist im Internet frei verfügbar und einfach einsetzbar.

5 Bedrohungen durch Überwachungsschnittstellen

Grundsätzlich unterscheidet man in informationstechnischen Systemen nach Angriffen auf die *Vertraulichkeit, Integrität und Verfügbarkeit* von Diensten und Daten.

Im Zusammenhang mit Überwachungsschnittstellen interessieren hier beispielsweise folgende Angriffe:

- Ein Angreifer könnte erfahren wollen, welche Anschlüsse bzw. Kennungen derzeit überwacht werden.
- Er könnte unberechtigt auf überwachte Anschlüsse zugreifen wollen,
- könnte die zum Bedarfsträger übermittelten Inhalte und Ereignisse mithören und/oder verändern wollen,
- selbst unberechtigt Überwachungsmaßnahmen „einleiten" wollen und
- Überwachungsmaßnahmen stören, verhindern und verzögern.

Als potentielle Angreifer kommen z.B. in Frage:

- fremde Geheimdienste,
- Personen aus dem Umfeld des organisierten Verbrechens,
- Hacker.

Welche Maßnahmen und Sicherheitsfunktionen in den technischen Dokumenten vorgeschrieben sind, um den Bedrohungen zu begegnen, wird im folgenden Abschnitt untersucht.

6 Sicherheitsfunktionen

6.1 Verbindung zwischen Netzbetreiber und Bedarfsträger

Die Anschlüsse zwischen Netzbetreiber und Bedarfsträger sollen beim Netzbetreiber nur für gehende Verbindungen konfiguriert sein (siehe auch Abbildung 1). Beim Bedarfsträger dürfen die Anschlüsse nur für kommenden Verkehr konfiguriert sein, um die Übermittlung der zu überwachenden Kommunikation jederzeit zu gewährleisten.

Eine solche unidirektionale Kommunikation soll außerdem verhindern, dass über die Überwachungsschnittstelle Anfragen an den Netzbetreiber von außen gestellt werden können. Somit ist es eigentlich auch ausgeschlossen, dass der Bedarfsträger beliebige Online-Anfragen auf den Datenbanken des Netzbetreibers durchführt.

Leider passt das Konzept der unidirektionalen Verbindung vom Netzbetreiber zum Bedarfsträger nicht besonders gut zu den Kommunikationsprotokollen im Internet. Es ist deshalb zweifelhaft, ob das gut gedachte Konzept auf die Überwachung von Internet-Kommunikation übertragbar ist. Zwar existieren in Firewalls, die in diesem Kontext eingesetzt werden könnten, entsprechende Funktionen zur Bestimmung der Kommunikationsrichtung, allerdings wurden in den letzten Jahren auch Tunneling-Techniken entwickelt, um die Filter wieder zu umgehen. Es ist deshalb nicht auszuschließen, dass bei der Komplexität heutiger Systeme die ggf. geschalteten Filter unbemerkt überbrückt werden können.

6.2 Übermittlung der Überwachungsanordnung

Für die Zukunft darf man davon ausgehen, dass das Konzept der unidirektionalen Verbindung selbst für zu überwachende Telefonverbindungen nicht konsequent beibehalten werden wird. Ein Grund dafür liegt in der für die Zukunft vorgesehenen elektronischen Übermittlung der Überwachungsanordnung. Bisher wird die Überwachungsanordnung manuell erstellt und basiert auf Papier, die dann per Fax bzw. Post den Netzbetreiber erreicht.

Die bisher öffentlich zugänglichen Dokumente enthalten leider noch keine technischen Details, weshalb die Sicherheit der elektronischen Übermittlung der Anordnungen noch nicht beurteilt werden kann. Aus Sicherheitssicht sollte aber die Überwachungsanordnung auf jeden Fall eine digitale Signatur tragen.

6.3 Gegenseitige Identifizierung und Authentifizierung

Eine Authentifizierung wird sowohl in TR FÜV als auch in ETSI ES 201 671 ausdrücklich gefordert. Als Lösung wird jedoch leider nur eine schwache Lösung angegeben: Die jeweiligen Anschlüsse von Netzbetreiber und Bedarfsträger müssen sich über die Protokolle COLP/CLIP (Connected Line Identification Presentation, Calling Line Identification Presentation) ihrem Gegenüber identifizieren. Es handelt sich bei den Protokollen im Wesentlichen um die Übermittlung der Rufnummer der Gegenstelle. Die relevanten Datenfelder sind nicht gegen Verfälschung durch intelligente Angreifer geschützt. Es handelt sich deshalb *nicht* um eine Authentifizierung im kryptographischen Sinn. Nach der Anwendung von so genannten Message Authentication Codes oder einer Digitalen Signatur sucht man leider vergeblich, obwohl entsprechende Produkte für starke Authentisierung im Internet und ISDN existieren.

6.4 Geheimhaltung der Zielrufnummer

Für jede Überwachungsmaßnahme wird vom Bedarfsträger eine individuelle Zielrufnummer angegeben, die der Netzbetreiber als Geheimsache „VS–Nur für den Dienstgebrauch“ aufzubewahren hat.

Natürlich schadet es nicht, die Rufnummer geheim zu halten, es nützt aber auch vergleichsweise wenig, insbesondere wenn dadurch so genannte Denial-of-Service-Angriffe, d.h. Angriffe auf die Verfügbarkeit der Überwachungsmaßnahme verhindert werden sollen. Schließlich könnte ja ein Fremder einfach die Rufnummer des Bedarfsträgers wählen, wodurch dessen Anschluss besetzt wäre und währenddessen keine Überwachung stattfinden kann.

Bei der Vorschrift handelt es sich wohl mehr um eine Vorschrift der Kategorie „security-by-obscurity“ als um eine ernsthafte Sicherheitsfunktion.

6.5 Verhindern von Denial-of-Servcie-Angriffen

Die geringe Verhinderungswirkung der Geheimhaltung der Rufnummer war den Autoren der Richtlinie durchaus bewusst, weshalb sie vorsorglich noch eine explizite Vorschrift zur Verhinderung von Angriffen

auf die Verfügbarkeit aufnahmen. In der TR FÜV heißt es deshalb: „Es ist zu verhindern, dass unberechtigte Benutzer die Einrichtungen beim Bedarfsträger anwählen können und diesen stören, blockieren oder überwachten Verkehr simulieren."

Als technische Lösung hierfür wird das Konzept der Closed User Group (CUG) angegeben. Auch diese Lösung ist sehr telefonie-lastig. Technologien dieser Art existieren für das Internet bzw. für IP-basierte Kommunikation nicht bzw. nur in Ansätzen. Darüber hinaus gestaltet sich gerade im Internet die Abwehr von Denial-of-Servcie-Angriffen außergewöhnlich schwierig. Wenn die Bedarfsträger also künftig auch im Internet überwachen können wollen, wäre eine der ersten Forderungen, Projekte im Bereich der Abwehr von Denial-of-Service-Angriffen zu fördern, bevor weiter über Überwachungsschnittstellen im Internet nachgedacht wird. Dies wäre außerdem für die Internet-Wirtschaft von Vorteil, da die Forschungsergebnisse auch ihnen zugute kämen.

6.6 Verschlüsselte Datenübermittlung zum Bedarfsträger

Man würde erwarten, dass aus Vorsorge vor externen Angreifern jegliche Kommunikation zwischen Netzbetreiber und Bedarfsträger verschlüsselt ablaufen muss. Leider formuliert die TR FÜV aber folgendes: „Der Inhalt der Datensätze ist dem Bedarfsträger unkodiert im Klartext zu übermitteln." Diese Formulierung hat nichts damit zu tun, dass ein Netzbetreiber die ggf. verschlüsselte Kommunikation vor der Übermittlung zum Bedarfsträger entschlüsseln muss, sofern er über die entsprechenden Schlüssel verfügt. Es ist grundsätzlich völlig unproblematisch, die zu übermittelnden Ereignisdaten und (unverschlüsselten) Inhalte auf der Verbindung zwischen Netzbetreiber und Bedarfsträger zusätzlich zu verschlüsseln. Entsprechende Soft- und Hardware sowohl für ISDN als auch Internet ist preiswert und problemlos einsetzbar. Für künftige technische Richtlinien sollte unbedingt die Verschlüsselung vorgeschrieben werden. Schließlich birgt das Abfangen unverschlüsselter Kommunikation zwischen Netzbetreiber und Bedarfsträger auch die Gefahr, dass intelligente Kriminelle so frühzeitig erfahren, dass sie im Fadenkreuz einer Ermittlung stehen. Darüber hinaus dürfte das unverschlüsselte Übertragen von Kommunikationen Unbeteiligter, die zufällig einen überwachten Anschluss benutzen, gegen den Datenschutz verstoßen.

6.7 Protokollierung der Überwachungsmaßnahme

Einiges Durcheinander und Unsicherheit herrscht bei der Frage der Protokollierung der Kommunikation, die über die Überwachungsschnittstelle erfolgt. Die Protokollierung hilft, Schwachstellen in und Angriffsversuche auf Überwachungsschnittstellen zu erkennen. In der Vergangenheit war das Protokollieren von Überwachungsmaßnahmen nicht vorgeschrieben bzw. die Formulierungen verboten dem Netzbetreiber sogar, Funktionen zur (technischen) Nachvollziehbarkeit zu implementieren. Der Chaos-Computer-Club formulierte deshalb zurecht in einer Presseerklärung vom 31. Juli 1996 zum § 90 TKG: „Diese Situation ist der Traum eines jeden Hackers." In den Entwürfen zur Schnittstellenbeschreibung für Überwachungsschnittstellen nach § 90 TKG führten unter anderem Formulierungen wie „Ein Aufzeichnen bzw. Anzeigen der Anfragen darf nicht erfolgen" zu erheblicher Verunsicherung.

Der Gesetzgeber hat inzwischen das Problem erkannt und im § 18 des Entwurfs zur TKÜV Vorschriften zugunsten einer vorgeschriebenen Protokollierung festgelegt. Leider existieren bisher noch keine technischen Richtlinien, wie die Protokollierung erfolgen soll. Es ist deshalb zu klären, wer die Protokollierung durchführt, vor wem die Protokolle zu sichern sind, gegen welche Angriffsformen (z.B. Angriffe auf Vertraulichkeit und Verfügbarkeit) sie schützen soll und wie Manipulationen an Protokollen verhindert werden. Da die Protokolle sensitive (auch personenbezogene) Daten enthalten werden, ist eine verschlüsselte Ablage der Protokolle angeraten.

7 Zusammenfassung

Zusammenfassend kann festgestellt werden, dass die in den Richtlinien geforderten Sicherheitsfunktionen bei weitem nicht dem entsprechen, was technisch möglich und zumutbar ist. Die vorhandenen Sicherheitsfunktionen schützen allenfalls vor Angriffsversuchen durch Unbedarfte, sie gefährden dadurch schlimmstenfalls sogar Unbeteiligte.

Die Hauptrisiken sind die fehlende starke Authentifizierung z.B. mit digitalen Signaturen und die fehlende bzw. zwingend vorgeschriebene Verschlüsselung der Ereignisdaten und Inhalte zwischen Netzbetreiber und Bedarfsträger.

Kein System ist von Anfang an sicher. Dies gilt auch für Überwachungsschnittstellen. Daraus folgt (zumindest theoretisch): Wer (unberechtigt und möglicherweise sogar organisiert kriminell) über eine Über-

wachungsschnittstelle in fremde Systeme eindringen will, dem wird dies über kurz oder lang gelingen, aber er wird den betroffenen Netzbetreibern und Bedarfsträgern bestimmt nicht von den Schwächen berichten. Folglich sollten möglichst viele „gutwillige“ Experten die Überwachungsschnittstelle genau untersuchen können: Fehler im Design und im Betrieb werden am Schnellsten durch Offenlegung und Nachvollziehbarkeit der Nutzung gefunden.

Überwachungsschnittstellen sollten nach dem besten Stand der Forschung und Technik arbeiten. Sie müssen sich wenigstens am Sicherheitsstand der am Markt verfügbaren Produkte orientieren. Dies ist leider derzeit noch nicht der Fall.