futureZone ORF.at

Die missbrauchten Vorratsdaten

Während EU-weit die Richtlinie zur verpflichtenden Speicherung von Verkehrsdaten aus Telefonie und Internet ["Data Retention"] umgesetzt wird, zeigen drei europäische Telekom-Skandale, wie Verkehrs- und Standortdaten, sowie die Überwachungsschnittstellen für “Lawful Interception” systematisch missbraucht werden.

Hochschule München 2008 11 27

Erich Moechel

Abriss der EU-weiten Überwachungsstandardisierung

futureZone ORF.at

- 1995 Ein EU-Ministerratsbeschluss zur Überwachung der digitalen Telefonienetze passiert den EU-Fischereiausschuss [sic!]
- 1996 Arbeit an den Überwachungstandards im European Telecom Standards Institute beginnt
- 1998/99 ein EU-Aufreger namens ENFOPOL
- 1999 Jahre vor Fertigstellung der UMTS-Netze wird der erste UMTS-Überwachungsstandard im ETSI publiziert.

ETSI ES 201 671 - Schema der Überwachungsschnittstelle

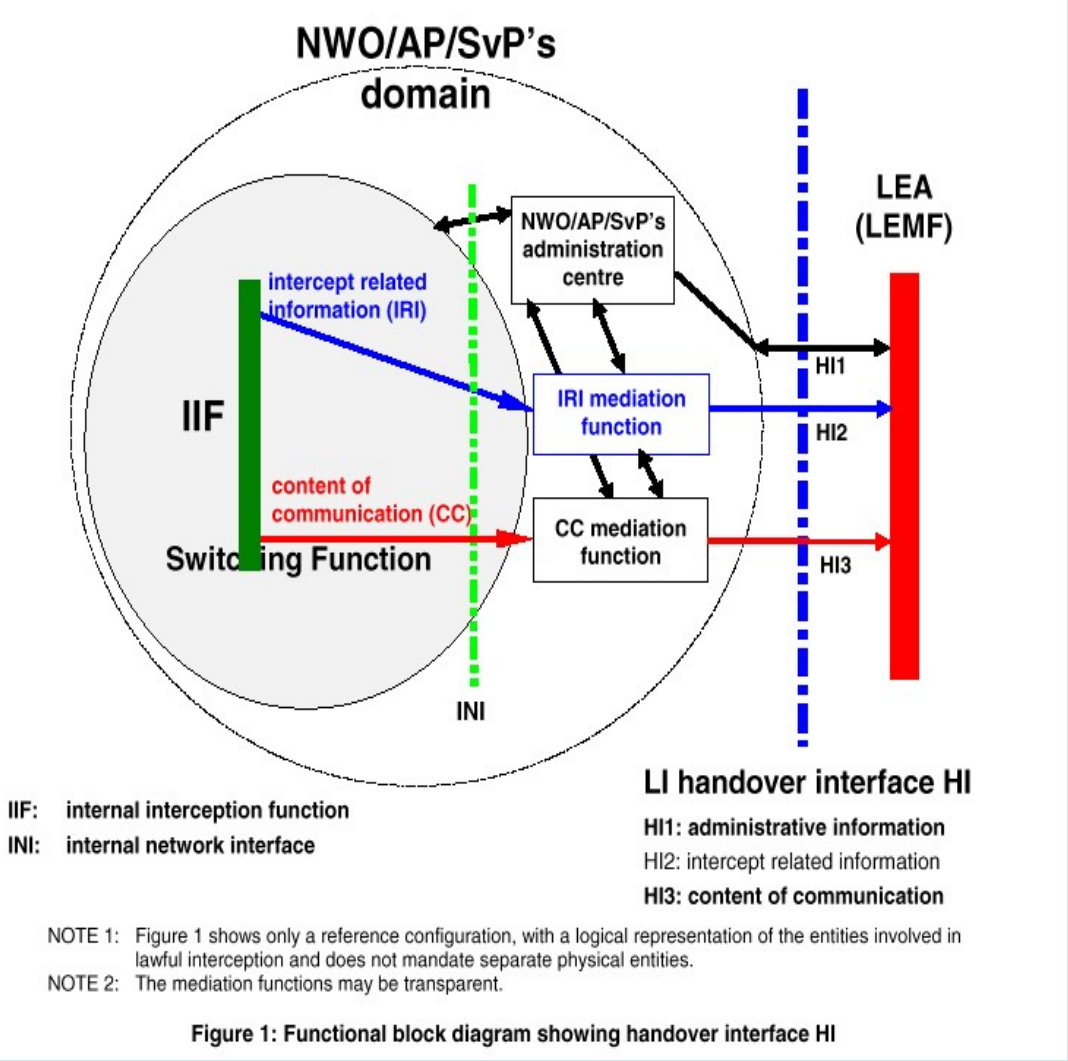

Figure 1: Functional block diagram showing handover interface HI

- LEA = Law Enforcement agency
- HI1 Anfrage LEA
- HI2 Verkehrsdaten
- HI3 Call Content
- Strichpunktierte Linien - Grenze zwischen Rechts- und Polizeistaat

Die neue Schnittstelle für “Vorratsdaten”

futureZone ORF.at

- Das Technische Komitee ETSI TC LI [Lawful Interception] setzt die EU-Richtline ([Data Retention] um.
- Das Pflichtenheft [Requirements] stammt vom holländischen Geheimdienst PIDS.
- Das Bundesamt für Verfassungsschutz, das britische Home Office/MI5, Verisign, das FBI, die israelischen Spezialfirmen Verint und Nice als weitere Beteiligte an einem Standard, der die Daten aller EU-Normalbürger betrifft.

Zwischenbilanz des Skandals in der Deutschen Telekom

futureZone ORF.at

- 2005/6 T-Aufsichtsräte, T-Gewerkschafter, Journalisten von T-Vorstand bespitzelt
- 2006 Verkehrsdatensätze von 17 Millionen T-Kunden landen im "Erotik-Milieu"
- Zugriff auf Daten über Konzern-Security
- "Ertragswert" der Daten 50 Mio. Euro jährlich
- Geheimnummern und Kommunikationsprofile von Promis, Sportlern, Politikern...

Telecom Italia: Massives Data-Mining in Kunden-Verkehrsdaten

futureZone ORF.at

- Februar 2006 “Data Warehouse Population Platform” der TI analysiert und vergleicht 20 Millionen Verkehrsdatensätze pro Stunde. Gesamt: 3 Milliarden.
- Das “RADAR” System: Eigenkonstruktion aus Datenbanken und Data-Mining-Tools. Früherkennung von Betrug und Abwanderung [Churn] usw.
- Juli 2006: Vodafone Italia klagt TI wegen unzulässigem Datamining in Verkehrsdaten und Abwerbung von Kunden.

Mafiajäger, CIA-Renditions, Verkehrsdaten und der Tod

futureZone ORF.at

- 2003/4 Ex-Mafiajäger Adamo Bove liefert als Sicherheitschef der Telecom Italia Mobile Verkehrsdaten, die zur Anklage gegen zwei Dutzend CIA-Mitarbeiter wegen Verschleppung eines Imams nach Ägypten führen.
- Frühjahr 2006 Bove untersucht Lücken im TI-Sicherheitsystem: RADAR hat Hintertüren.
- Juli 2006, Adamo Bove stürzt in Neapel von einer Brücke, der Vizechef des Militärgeheimdienstes SISMI wird verhaftet.

Zwischenbilanz des Skandals in der Telecom Italia

futureZone ORF.at

- September 2006 Boves Vorgänger als TI-Sicherheitschef, Giovanni Tavaroli, wird des systematischen Missbrauchs der ETSI-Schnittstellen beschuldigt: Illegaler Datenhandel und Erpressung.
- Die Verkehrsdatensätze wurden über eine eigene Agentur verkauft, auch auf Bestellung.
- Januar 2007 : Zwei Dutzend Telekomtechniker, Polizisten und SISMI-Agenten sind in Haft. 14 Millionen Euro beschlagnahmt.

Vodafone Hellas: Schnittstelle gehackt, Sicherheitschef erhängt

futureZone ORF.at

- März 2005 Nach Problemen im Netz von Vodafone Hellas finden Techniker des Ausrüsters Ericsson die ETSI-Schnittstelle “gehackt” vor.
- Zwei Tage später wird Netzwerksicherheitschef Kostas Tsalikidis erhängt aufgefunden.

Fakten zum Abhörskandal in Athen

- Premier Kostas Karamanlis und sein Kabinett wurden monatelang abgehört.
- Eine Software unbekannter Herkunft aktivierte am ETSI-Interface illegal Ericssons Überwachungssuite IMS. Programmiersprache PLEX, 6500 Zeilen mit “Rootkit” Funktion, 16 [!] Remote-Updates mit Patches
- Ericsson vor Gericht: Vodafone hat auf Verlangen des britischen Geheimdiensts MI6 agiert.
- Dezember 2005 MI6 Stationsleiter in Athen enttarnt, 76+ Mio Euro Strafe für Vodafone, 7,3 Mio. Ericsson.

Die Spuren zurück ins ETSI

- Der Skandal in Athen flog durch eine Kollision von Überwachungsprotokollen am ETSI-Interface auf.
- In der AG 3GPP SA LI treffen Techniker von Vodafone , Ericsson und Home Office/MI5, Deutscher Telekom und FBI et al. regelmäßig zusammen.
- April 2006 Ericsson-Techniker in 3GPP SA LI mit Eil-Antrag um Protokoll-Problem zu beseitigen.
- In Italien wurde die “Live”-Schnittstelle vom obersten Lawful-Interception-Verantwortlichen missbraucht.

Was beide Fälle gemeinsam haben

- Involvierung von nationalen Militärgeheimdiensten und CIA bzw. MI6.
- Missbrauch der ETSI-Überwachungsschnittstelle zum Mitschnitt von Telefongesprächen.
- Sicherheitschefs in den kompromittierten Netzen enden durch Selbstmord, Angehörige zweifeln.
- “Anti-Terror-Maßnahmen”. In Italien waren es CIA-Entführungen, in GR wurde dem MI6 und dem griechischen Geheimdienst EYP vorgeworfen, Pakistanis gefoltert zu haben.

Was all das für die EU-weite “Vorratsdatenspeicherung” bedeutet

futureZone ORF.at

- Durch die den Telekoms vorgeschriebene Bereithaltung genau definierter Verkehrsdatensätze im System wird Data-Mining für “Staatsicherheitsagenturen” weitaus einfacher.
- Analog zu den Angriffen auf das “Live-Interface” ES 201 671 wird es systematische Attacken von Geheimdiensten auf das neue Interface und damit auf historische Verkehrsdaten geben.
- Neue Datensätze, neue “Incentives” für Begehrlichkeiten innerhalb der Telekoms.

Das Metanetz – Anatomie des modernen Überwachungsstaats

futureZone ORF.at

Das Überwachungsszenario in den Telefonienetzen der näheren Zukunft wird eine permanente Rasterfahndung nach Kommunikationsmustern sein, die über das Data-Retention-Interface als Routine in den Kommunikationsdaten aller Bürger läuft. Bei Alarm wird die Überwachungsschnittstelle nach ES 201 671 automatisch aktiviert und live aufgezeichnet.

Erich Moechel

Tod an der Überwachungsschnittstelle

- Kostas Tsalikidis, Netzwerkarchitekt von Vodafone Hellas, im Januar 2005 erhängt aufgefunden.
- Seine Angehörigen sind überzeugt, dass Tsalikidis ermordet wurde. [foto tsalikidis family]

Tod an der Überwachungsschnittstelle

- Adamo Bove, Netzwerksicherheits-chef der Telecom Italia, gestorben im Juli 2006.
- Wie Tsalikidis hinterließ Bove keinen Abschiedsbrief. [Foto: Reuters]

Die missbrauchten Vorratsdaten

futureZone ORF.at

2009 – who is next?

erich.moechel@orf.at
secure: me@quintessenz.org
Key ID: 0x007DB429
Fingerprint:
9F49 57E7 8824 26C8 78B5 F3B6 F416 7AFB 007D B429