

Lawful interception of IP networks

SAFE-NL

ir. F. Fransen
KPN Research

November 29, 2002



1

Agenda

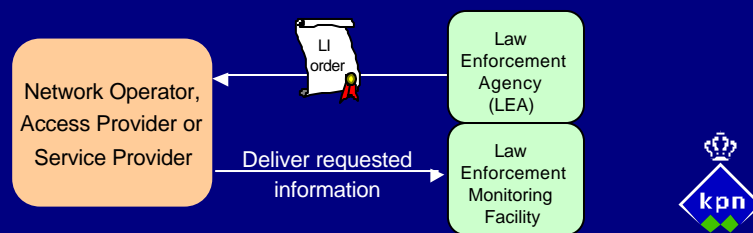
- Introduction on Lawful Interception
- Interception of Internet services
- WAI & TIIT specifications
- Interception techniques
- Reliability & Future issues



2

Introduction on Lawful Interception

- ETSI definition of (lawful) interception:
 - **interception:** action (based on the law), *performed by* an network operator/access provider/service provider (NWO/AP/SvP), of making available certain information and providing that information to a law enforcement monitoring facility.



Planet MultiMedia - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address http://www.planet.nl/multimedia2/pink/1,,101_1498_594415,00.html Go Links

Planet Multimedia

Justitie tapt kinderporno, rechtzaak gaande

De eerste rechtzaak waarbij gebruik is gemaakt van het aftappen van internetverkeer in Nederland dient deze dagen voor de rechtbank in Alkmaar. Zes verdachten staan terecht voor het maken en verkopen van kinderporno.

Het onderzoek naar de zes verdachten is al sinds 1998 aan de gang, vandaag en morgen staan ze terecht. Ze worden ervan verdacht via een aantal internetzites kinderporno te hebben aangeboden. Een van die sites is Dutchteen.com. De site is niet meer actief, het domein is in handen van een bedrijf in Nieuwegein dat zich in professionele sex bakwaamd lijkt te hebben.

De kinderporno's waren niet vrij te downloaden. In opdracht van justitie kochten rechercheurs in 1998 toegang tot de site. Vervolgens werd gekeken waar het geld naartoe ging: naar een Luxemburgse bankrekening van een 28-jarige Nederlander.

De politie Haaglanden, die het onderzoek leidde, maakte ook gebruik van internettaps. In welke mate dit bij heeft gedragen aan het sluitend krijgen van het bewijs is niet transparant.

De kwaliteit van de internettaps liet te wensen over. Het materiaal afkomstig uit de taps was moeilijk te ontziferen door justitie. Teksten waren veel te lezen, afbeeldingen kwam niet als herkenbaar over.

(Bron: ANP)

Introduction on Lawful Interception

Legal framework for LI in The Netherlands

- Telecommunicatiewet (Telecommunications act)
- Wetboek van Strafvordering (Code of Criminal Proceedings)
 - art. 126m & art. 126t = Content interception
 - art. 126n & art. 126u = Traffic data interception
- Wet Inlichtingen en Veiligheidsdiensten (Intelligence and Security Services Act)
 - art. 25 = Content interception
 - art. 27 = Traffic data interception
- Wet Bijzondere Opsporingsbevoegdheden (The Special Investigation Powers Act)
 - streamlines criminal investigation method

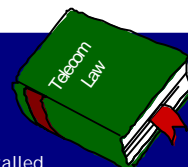


6



Introduction on Lawful Interception

- Telecommunicatiewet (TW, 1998)
- Art. 13.1
 - NWO/AP/SvP may only enter market when LI capability is installed
- Art. 13.2
 - NWO/AP/SvP obliged to assist authorities with interception
- Art. 13.4
 - NWO/AP/SvP obliged to offer information needed by the LEA to draft LI order
 - NWO/AP/SvP obliged to store traffic data for 3 months in order to facilitate data analyses
- Art. 13.6
 - Initial costs and maintenance costs are for the NWO/AP/SvP
 - Government only pays labour costs
- Until 15th of April, 2001 ISPs could have exemption



6



Introduction on Lawful Interception

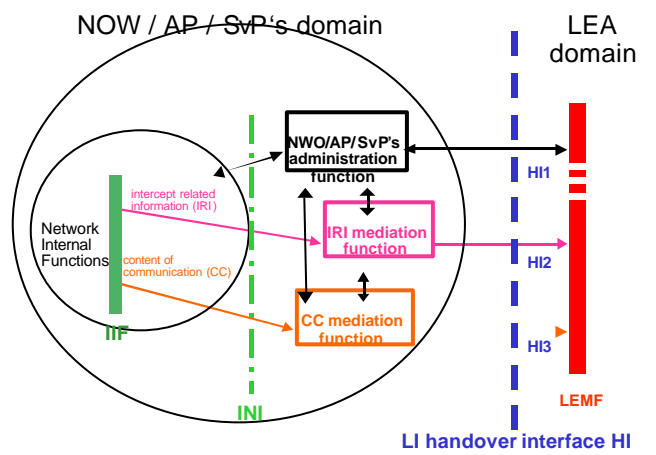
- Wet Bescherming Persoonsgegevens (Privacy Law)
 - exceptions for investigation by authorised LEAs
- Note that NWO/AP/SvP also have to comply to privacy laws
 - they are liable? check validity of LI order
 - company's public image



7



Introduction on Lawful Interception – ETSI model



IIF: internal interception function
 INI: internal network interface
 H1: administrative information
 H2: intercept related information
 H3: content of communication

8



Agenda

- Introduction on Lawful Interception
- **Interception of Internet services**
- WAI & TIIT specifications
- Interception techniques
- Reliability & Future issues

9



Interception of Internet services

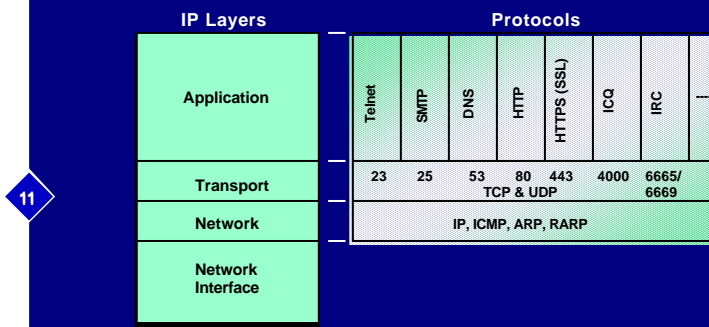
What are Internet services?

- access to the Internet
- the services that go over the Internet, such as:
 - World Wide Web (e.g. http),
 - e-mail,
 - chat and ICQ,
 - VoIP, FoIP,
 - Peer2Peer networks (e.g. KaZaA, eDonkey)
 - ftp, telnet,
 - etc.

10



IP stack and applications



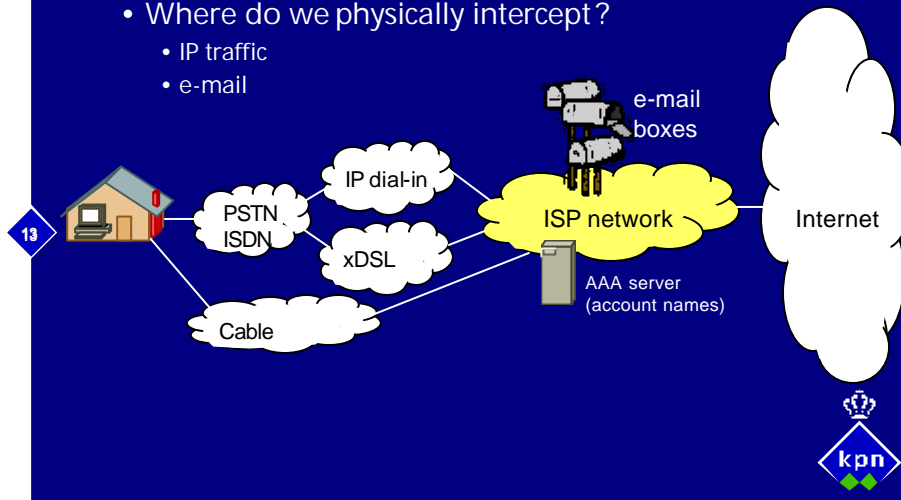
Interception of Internet services

- 12
- So what service should we intercept?
 - interception of a specific Internet services (e-mail, http, chat, etc) is not efficient and more complex
 - manipulate traffic of target
 - Dutch conclusion from WAI-T:
 - full IP interception (IPv4, IPv6, ICMPv4, ICMPv6)
 - e-mailbox interception (target identity in RCPT TO:
 - like an electronic Post Office box



Location of interception

- Where do we physically intercept?
 - IP traffic
 - e-mail



Interception of Internet services

- 14
- What about encrypted traffic?
 - Secure e-mail (e.g. PGP, S/MIME)
 - Secure surfing with HTTPS (e.g. SSL, TLS)
 - VPNs (e.g. IPSec)
 - Encrypted IP Telephony (e.g. pgp-phone and Nautilus)
 - etc.
 - If applied by NWO/AP/SvP then
 - encryption should be stripped before sending to LEMF or
 - key(s) should be made available to LEA
 - else
 - *a challenge for the LEA*

Agenda

- Introduction on Lawful Interception
- Interception of Internet services
- **WAI & TIIT specifications**
- Interception techniques
- Reliability & Future issues

15



WAI & TIIT specifications

- Two Dutch specifications for LI of Internet traffic:

Functional
Specification for
lawful interception
of Internet traffic in
the Netherlands.

WAI/GT/FuncSpecs
V1.0.1 (2000-06)
GovTech (WAI)

**WAI Functional
Specification**

Transport of
Intercepted IP
Traffic (TIIT)

Version 1.0.0 (2002-09)

DGTP
Ministry of
Economic Affairs

TIIT

16



WAI & TIIT specifications

WAI Functional Specification contains:

- User (LEA) requirements for Lawful Interception
 - General requirements
 - Results of Interception
 - Location Information
 - Time Constraints
 - Information Protection Requirements
 - Unchanged State of Service, etc.
 - Technical Interface(s) and Format Requirements
 - Multiple points for delivery
 - Temporary Obstacles to Transmission
 - Identification of the identity to be intercepted
 - Multiple interception measures
- Interception scenarios
 - IP interception
 - Email interception

17



WAI & TIIT specifications

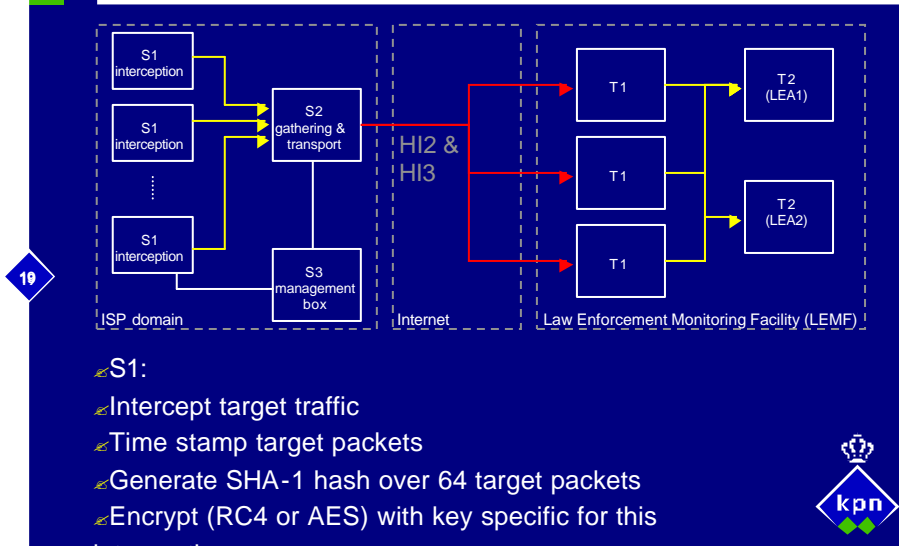
TIIT Specification contains:

- User (LEA) Requirements for transport
- Description of Handover Interface
 - HI1: method depends on LEA, but also contains crypto keys
 - HI2: events like login, logout, access e-mailbox, etc.
 - HI3: Content of Communication and additional generated information (hash results and NULL packets)
- Description of General Architecture for HI2 and HI3
- Handover Interface specification
 - Global data structures
 - S1 – T2 Traffic Definition
 - Data structures and message flows for HI2 and HI3
 - Use of cryptography

18



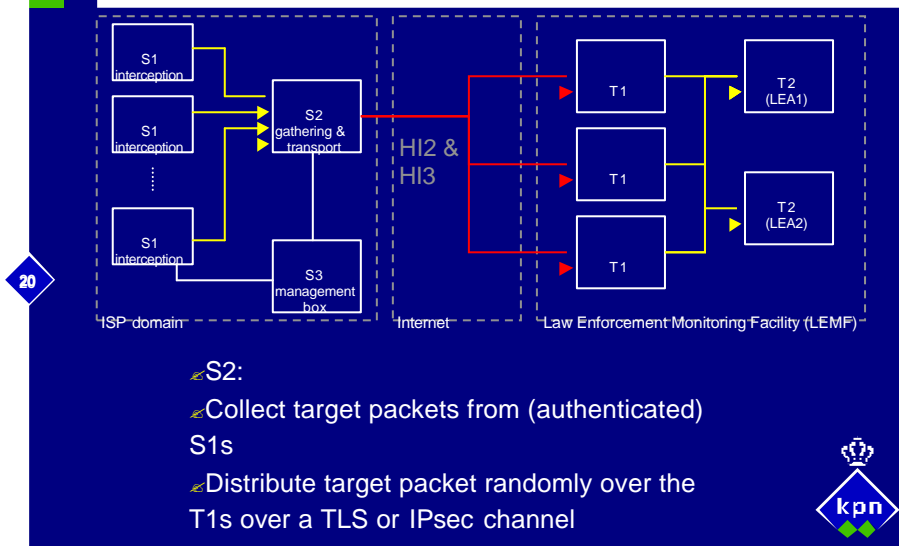
TIIT - General Architecture for HI2 and HI3



- ⚡ S1:
- ⚡ Intercept target traffic
- ⚡ Time stamp target packets
- ⚡ Generate SHA-1 hash over 64 target packets
- ⚡ Encrypt (RC4 or AES) with key specific for this



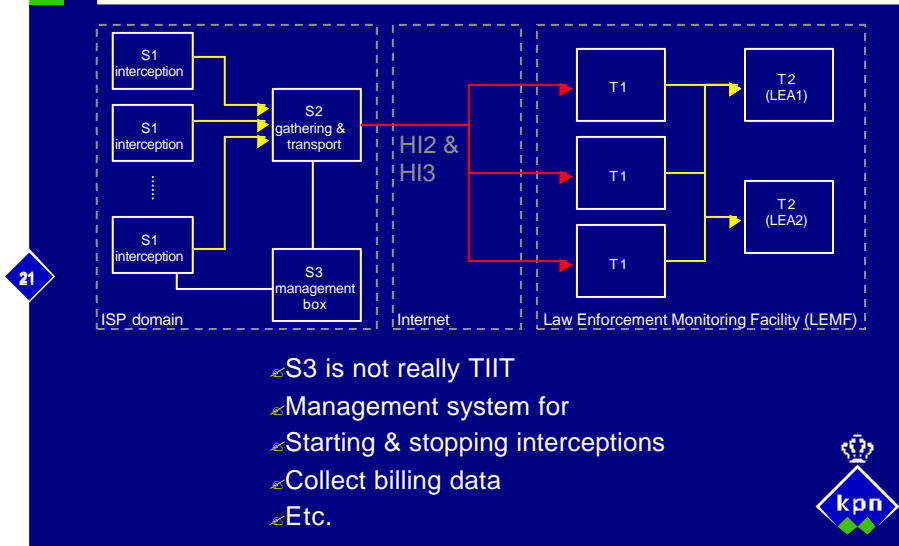
TIIT - General Architecture for HI2 and HI3



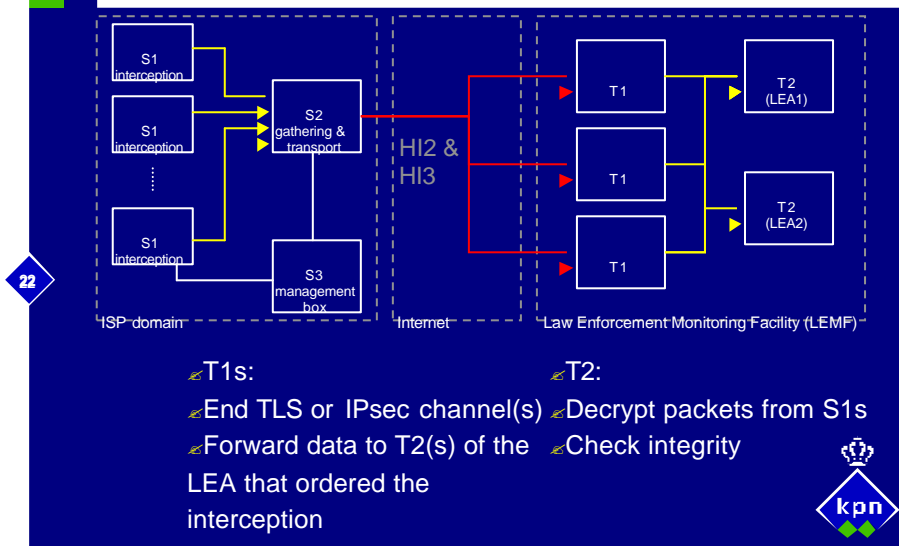
- ⚡ S2:
- ⚡ Collect target packets from (authenticated) S1s
- ⚡ Distribute target packet randomly over the T1s over a TLS or IPsec channel
- ⚡ Use X.509 certificates for authentication



TIIT - General Architecture for HI2 and HI3



TIIT - General Architecture for HI2 and HI3



Agenda

- Introduction on Lawful Interception
- Interception of Internet services
- WAI & TIIT specifications
- **Interception techniques**
- Reliability & Future issues

23



Interception techniques

Constraints for the LI solution:

- Confidentiality
 - Participants in communication **MUST NOT** be able to detect the interception
 - Unauthorised employees **MUST NOT** be able to get any information on the interception
- Impact on infrastructure
 - ISP infrastructure is very dynamic and **SHOULD NOT** be limited by the LI solution
- Cost efficient
- Reliable

24



Interception techniques – IP traffic

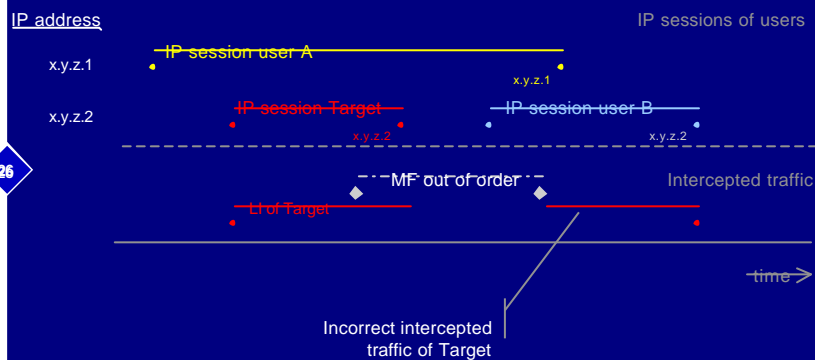
- Identification of target traffic
 - Target ID = account name
- Fixed IP address
 - derive fixed IP address from account name is easy
- Dynamic IP addressing
 - monitor Radius traffic for account name and deduct the IP address for this session
 - conversion MUST be fast enough to prevent missing packets
 - don't miss Radius tickets

25



Interception techniques – IP traffic

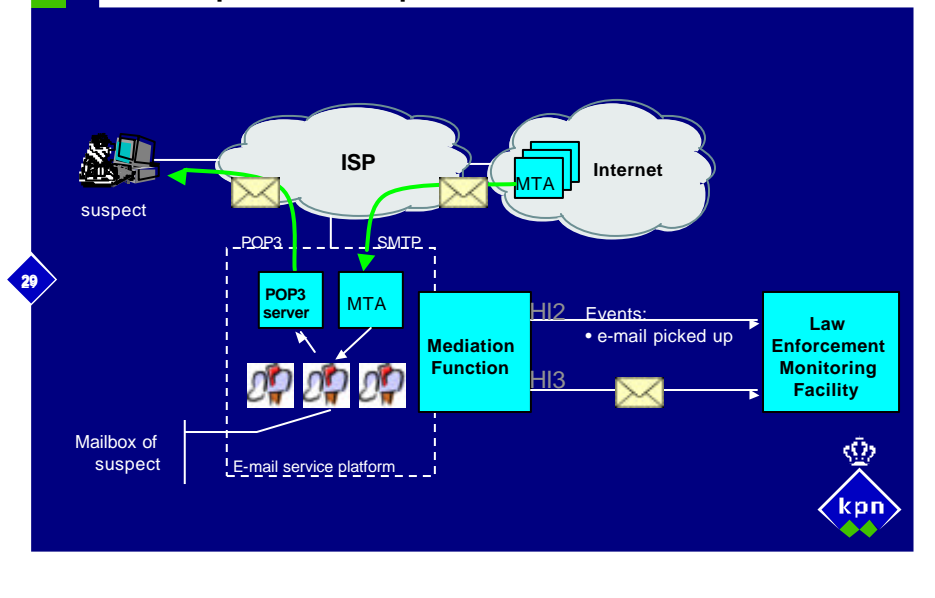
- Don't miss Radius tickets because:



26



Interception techniques – e-mail

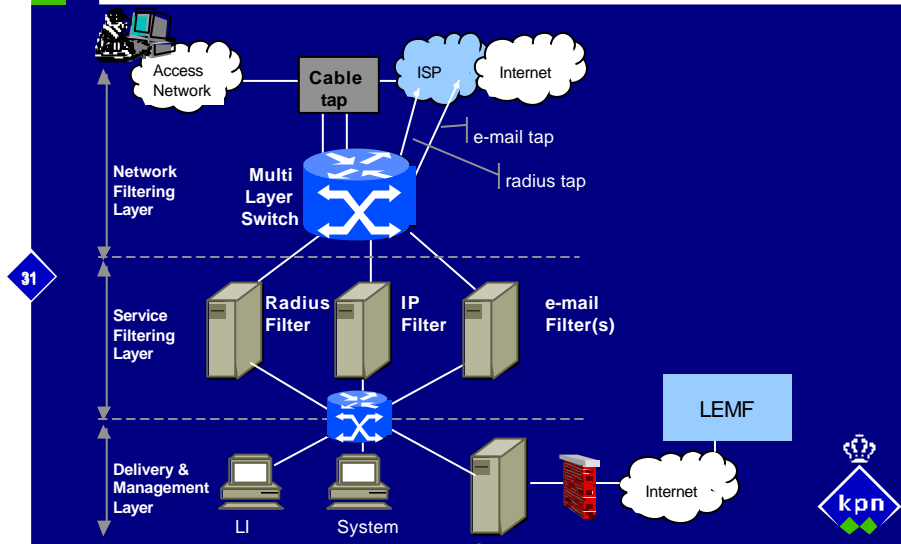


Interception techniques – e-mail

Possible IIF methods for e-mail interception:

- 30
- Add a BCC: LEA@LEMF.nl to target e-mail at the MTA
 - Change state of service
 - Confidentiality problem when LEA mailbox is full
 - Interception function in mail server copies e-mails addressed to target
 - Need to modify mail server (not preferred)
 - LI information on mail system needs to be protected from unauthorised administrators
 - Cable tap and filter for SMTP and POP3 traffic
 - Best solution
 - Reliability issue - Filter needs to perform IP packet defragmentation, tcp sequence reordering, handle retransmission, etc. It is a target for DoS attack.

Interception techniques – basic concept



Agenda

- Introduction on Lawful Interception
- Interception of Internet services
- WAI & TIIT specifications
- Interception techniques
- Reliability & Future issues

32



Some reliability issues

- IP spoofing
- Intra-pop traffic
- Tricks with IP packet fragmentation
- Tricks with TTL
- Bugs in S1 and S2 implementation
 - should S1 and S2 be evaluated by third party?
(e.g. Common Criteria)

33



Some future issues

- Constant increase in bandwidth
 - LEAs and LEMF will have to keep up
- WLAN / HotSpots
 - free & anonymous access
- UMTS: IP Multimedia Subsystem
 - HI2: interception of SIP messages
 - HI3: RTP/RTCP traffic

34



Questions



35

