COUNTER STRIKE
LAWFUL INTERCEPT

FX of Phenoelit / 30C3
@41414141

Derived From: Half-Life Engine
Dated: Yes
Declassify: When Leaked

Agenda

- Justification and regulation of lawful interception
- Inherent problems
- The game map
- Playing one side
- Playing the other side
- Conclusions

Disclaimer

- This talk is IP network centric
  - Lawful interception is also in place for email, wired phone lines, mobile phone networks, …
- I'm just a concerned amateur, but I can read
  - Standards
  - Documentation
  - Books
  - Assembly
  - Regulation
  - Resolutions

Justification and Regulation

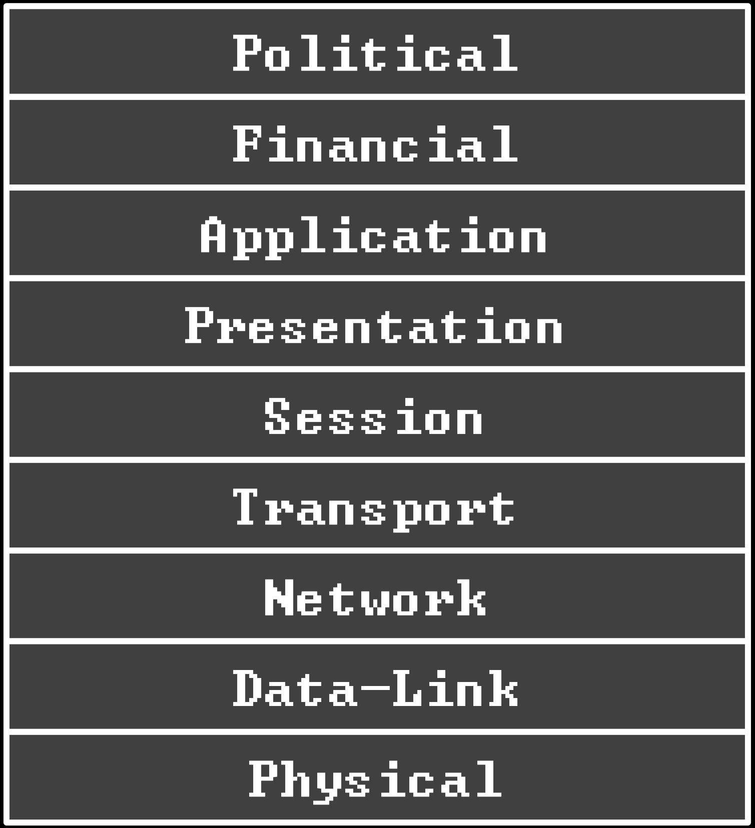
- Lawful interception is meant to be used by law enforcement agencies (LEA)
  - Legally rooted in concepts derived from snail mail [1]
- Wiretapping and targeted surveillance have very legitimate use-cases
  - If your child is kidnapped and the ransom note arrives via email, you will ask for it
- EU adopted "Council Resolution of 17 January 1995 on the lawful interception of telecommunications"
  - Regards to "Treaty on European Union" (Maastricht Treaty), Article K.1 (9): "police cooperation for the purposes of preventing and combatting **terrorism**, **unlawful drug trafficking** and other serious forms of international crime […]"
  - Also regarding to Article K.2 (2) [3]
- National legislation differs in implementation requirements (e.g. how much network operators are allowed to see)

THE MAP

OMFG! 3.724.541.951 spawn points!

IETF vs. LEA

- IETF demand for un-tampered encryption (RFC 1984):
  - "Cryptography is the most powerful single tool that users can use to secure the Internet. Knowingly making that tool weaker threatens their ability to do so, and ***has no proven benefit***."
- IETF Policy on Wiretapping (RFC 2804):
  - "[…] tools which are effective for a purpose tend to be used for that purpose." (By anyone who can)
  - "[…] tools designed for one purpose that are effective for another tend to be used for that other purpose too, no matter what its designers intended." (aka HTTP)
  - "[…] if a vulnerability exists in a security system, it is likely that someone will take advantage of it sooner or later." (e.g. right now)



Political

Financial

Application

Presentation

Session

Transport

Network

Data-Link

Physical

The real-world OSI model

by Evi Nemeth

An IETF Refusal Sums Up Security: RFC 2804 Security Considerations

- The system is less secure than it could be had this function not been present.
- The system is more complex than it could be had this function not been present.
- Being more complex, the risk of unintended security flaws in the system is larger.

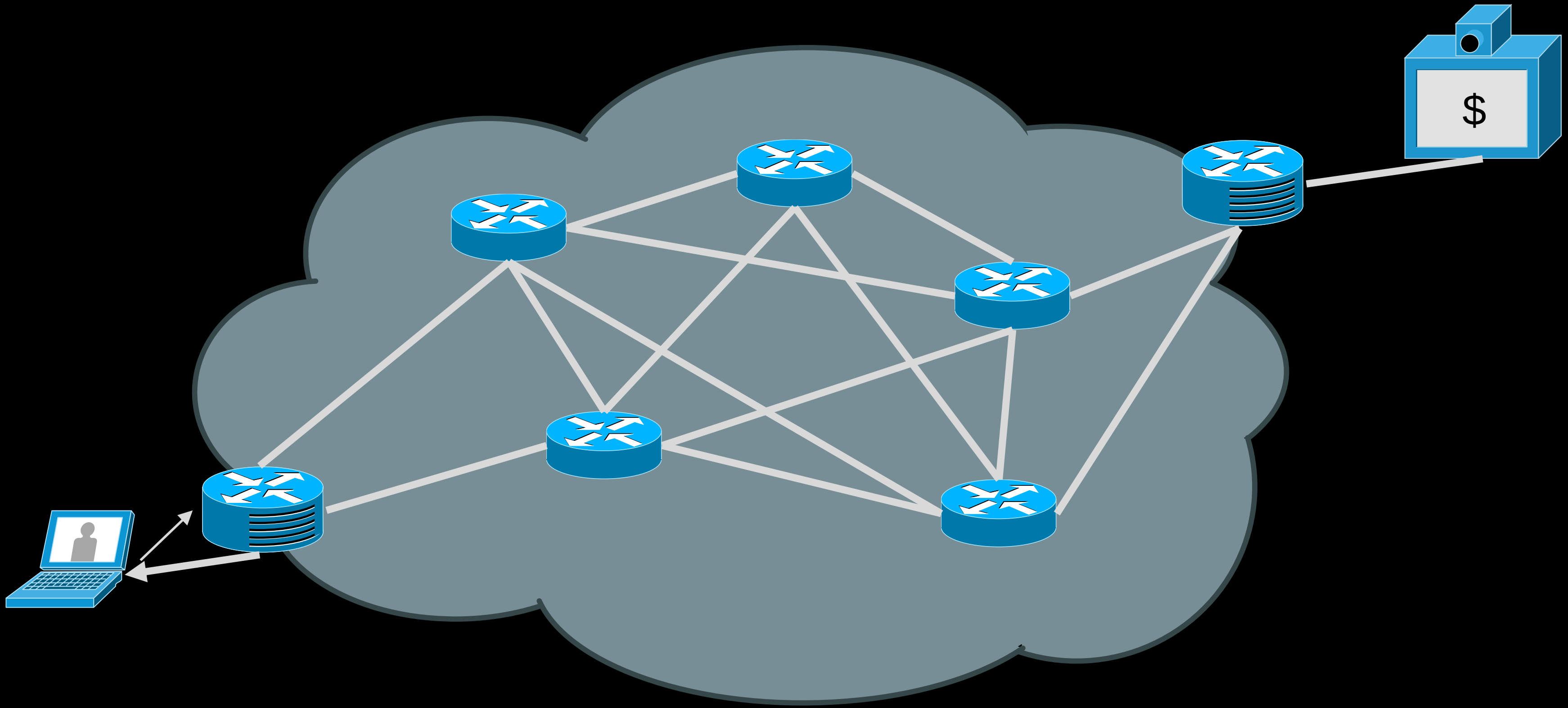
➔Wiretapping, even when it is not being exercised, therefore lowers the security of the system.

CounterStrike LI | Hot fork my dongle ... | Hypocrisy - Wikipedi... | 08:15

Inherent Problems

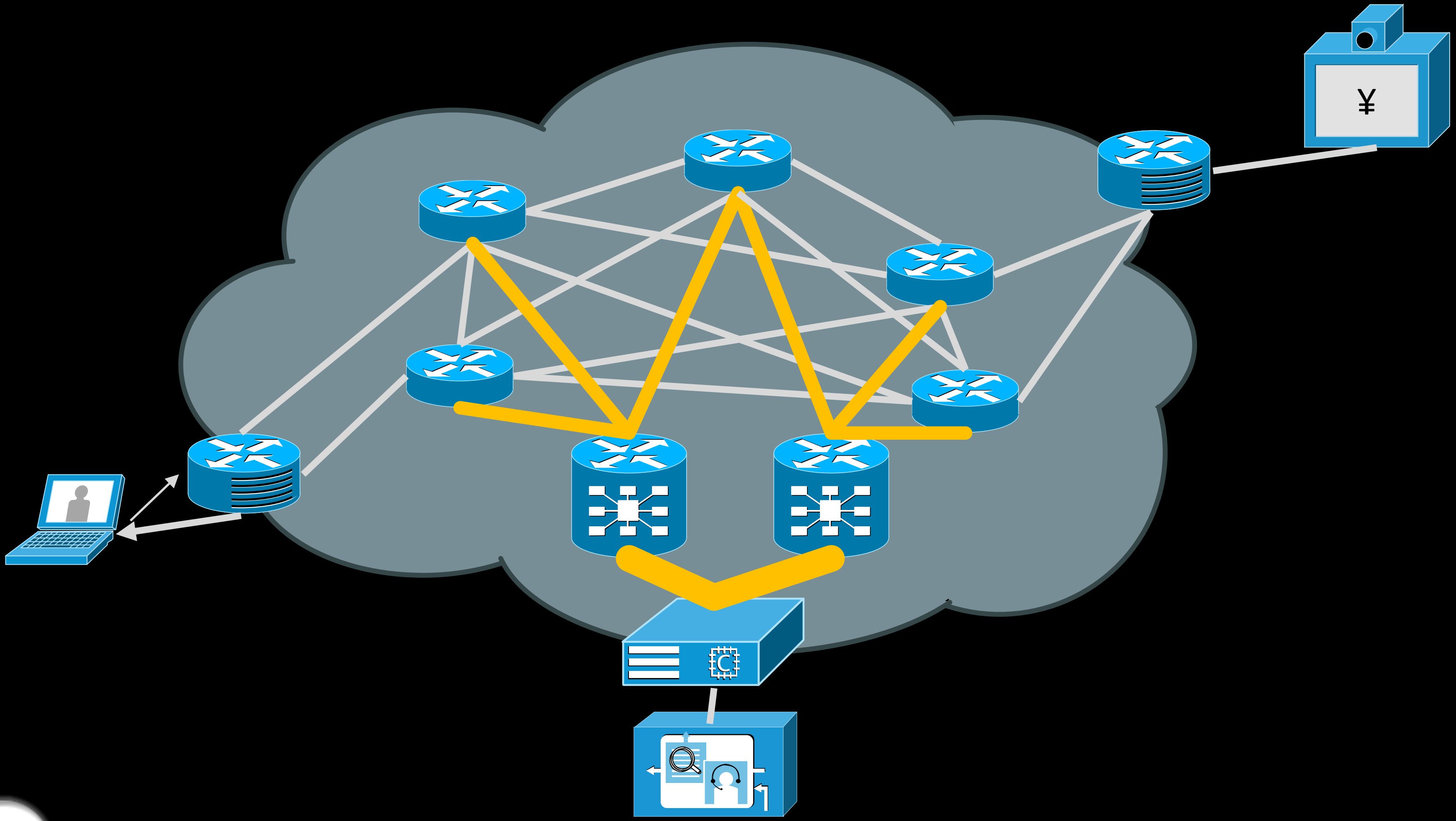
- Lawful intercept is a cost center
  - Tier-2 service provider case study ([2] 9.1.3):
    - One-time cost: $7,905,000
    - Annual recurring costs in 1st year: $38,657,000
    - Reimbursements $25,000,000
  - Business models based on user surveillance profit from LI
- Performance and Operation
  - "[…] the operation of the target service must appear unchanged to the interception subject"
  - "During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers […]"
  - "[…] telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope […]"
- Bandwidth
  - "[…] transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators"

Internet Topology



Initially conceived by the "Members and Affiliates of the Intergalactic Computer Network" at US DoD DARPA IPTO, SDC, Berkeley and MIT – 1962

Sensor Network



GAMEPLAY

A first-person game, in which players join either the terrorist team or the counter-terrorist team – to become spectators.

Interception Points

- Acquisition at source (Quellen-TKÜ)
- CPE
- Access layer
- SS7 probes
- Data Retention
- DNS triggered interception
- Global Observer

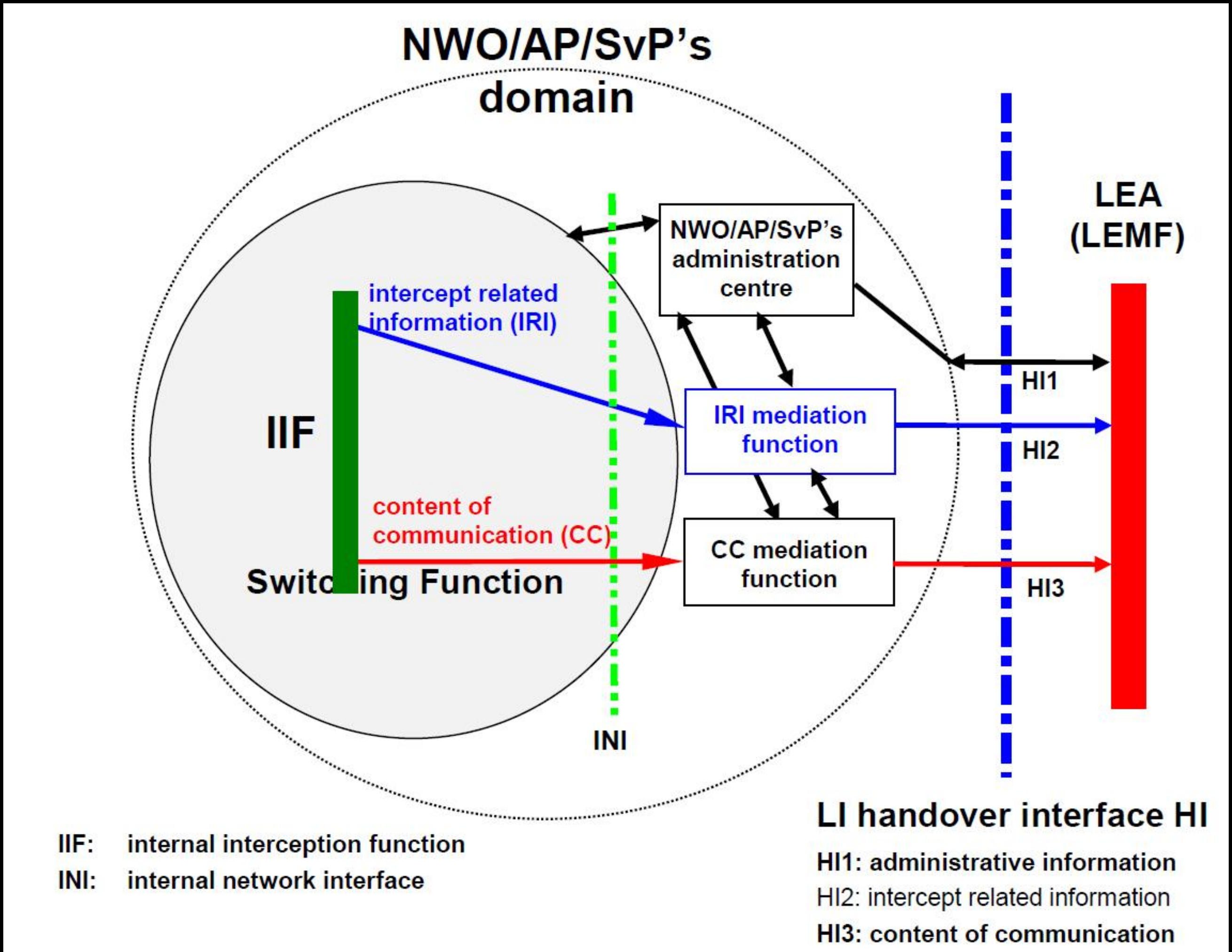
Let's go and get them!

COUNTER-TERRORISTS

Because we are the good girls/guys/anything-in-between
(incl. at least one android entity)

LI Architecture

ETSI Model ([4], section 5)



NWO/AP/SvP's domain

IIF

intercept related information (IRI)

content of communication (CC)

Switching Function

INI

NWO/AP/SvP's administration centre

IRI mediation function

CC mediation function

HI1

HI2

HI3

LEA (LEMF)

IIF: internal interception function

INI: internal network interface

LI handover interface HI

HI1: administrative information

HI2: intercept related information

HI3: content of communication

CounterStrike LI

Hot fork my dongle ...

Hypocrisy - Wikipedi...

08:15

Examples of LI Framework Solutions

Vendor	Product	Notes
SS8 Networks	Xcipio	• Famous configuration templates for Cisco IOS **snmp-server user ss8user tapGrp v3 auth md5 ss8passwd** • Sun Solaris/Windows
Aqsacom	ALIS Lawful Interception Management Solution	• IRI via FAX and SMS • Billing System for "new revenue Streams" • Windows/UNIX/Linux
GTEN AG	"a solution"	• German Federal Ministry of Economics and Technology (BMWi) certified (supposedly) • Data collection and filter unit [DCFU] placed • Add-ons, e.g. Posidon VoIP→ISDN call (wait, what?)
Utimaco Safeware AG	Lawful Interception Management System (LIMS)	• Remote administration of other LI systems • Integrated billing capabilities
Siemens AG	Monitoring Center	• FAX, SMS, DTMF in-band, Modem, GIS, …

WYSIWYG Right?

- List of features advertised for a LI solution:
  - "It includes optimal granularity to preserve privacy."
  - "Its flexible architecture allows for configurations based on country specific regulations."
  - "It captures only the traffic to or from the entity listed on the warrant; the privacy of all non-warrant-defined IP traffic is preserved."
    - "[…] provided to the exclusion of any telecommunications that do not fall within the scope […]" – legal requirements for the SP
  - "It operates at high speeds without service disruption."
  - "The high operation speed (measured in Gbps) ensures interception of all IP traffic for a specific warrant-defined suspect."
  - "Traffic is intercepted in the core of the network, minimizing the number of devices that need to be used and reducing the required investment for IP-interception deployments."

CounterStrike LI
Hot fork my dongle ...
Hypocrisy - Wikipedi...
08:15

Cisco's LI

- "Cisco Architecture for Lawful Intercept in IP Networks" (RFC 3924)
  - IESG Note: "This RFC is not a candidate for any level of Internet Standard. The IETF disclaims any knowledge of the fitness of this RFC for any purpose, and in particular notes that the decision to publish is not based on IETF review for such things as security, congestion control or inappropriate interaction with deployed protocols."
    - IETF in full "I don't talk to you"-mode
- This is the only LI architecture published
  - WTF? Cisco is the one vendor who did the right thing?
- At least they kept their tradition of authentication design failures. As usual, by design ;)
  - LEA-authentication and authorization happens at the MD
  - The tap and traffic copy destination… on the router

RFC 3924 Reference Model

```
                       +--------------------+               +-----+
                       |  LI Administration |     HI1(a)    |     |
                       |      Function      |<--------------|     |
                       +--------------------+               |     |
                              |                             |     |
                              | MD Provisioning             |     |
                              | Interface(b)                | LEA |
                              v                             |     |
+-----------+           +--------------------+              |     |
|           |<---(c)----|                    |              |     |
|  IRI IAP  |--IRI(e)-->|      Mediation     |----HI2(g)--->|     |
|           |           |      Device (MD)   |              |     |
+-----------+           |                    |----HI3(h)--->|     |
                        +--------------------+              +-----+
                             |         ^
                   Intercept |         | Intercepted
                  Request(d) |         | Content(f)
                             |         |
                             v         |
                           +--------------------+
                     User  |       Content      |  User
                   -------->|         IAP        |--------->
                   Content +--------------------+  Content
```

CounterStrike LI

Hot fork my dongle ...

Hypocrisy - Wikipedi...

08:15

RFC 3924 Reference Model

- LI functionality is controlled via SNMPv3
  - Common and well understood in SP networks
  - Authentication required, encryption optional
  - Registering a mediation device (MD) is done with one UDP packet
  - Starting to intercept a communication is done with one UDP packet
- The mediation device performs all the voodoo
  - Separation of LEAs
  - Management of multiple interceptions
  - Format according to $country requirements
- The router does what is already implemented

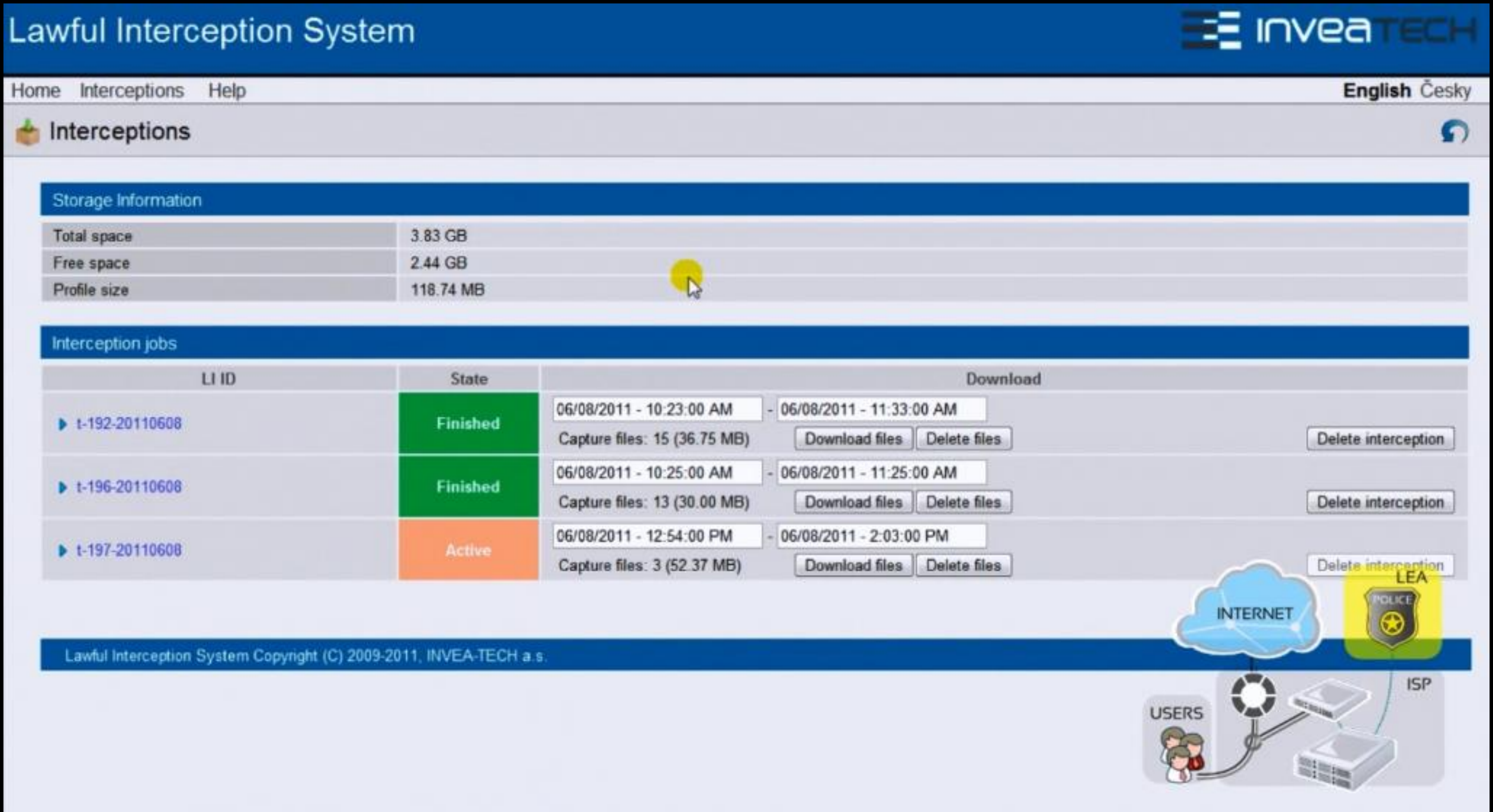
… or so it seems

But how?

- LI matching must happen in what is called the "critical path": The forwarding code!
  - Either a router moves packets from the incoming to the outgoing interface as fast as it can
  - Or the router looks at the packets
- Routers are not meant to look at packets
  - The closest to "looking at the packet" are Access Control Lists (ACL)
    - 12 major ACL bypass vulnerabilities are documented for Cisco IOS
  - For interception purposes, Cisco IOS builds Access Control Lists on the fly

Mediation Device Example

Ease of use



Lawful Interception System

Interceptions

Storage Information

Total space	3.83 GB
Free space	2.44 GB
Profile size	118.74 MB

Interception jobs

LI ID	State	Download				
t-192-20110608	Finished	06/08/2011 - 10:23:00 AM - 06/08/2011 - 11:33:00 AM Capture files: 15 (36.75 MB)	Download files	Delete files		Delete interception
t-196-20110608	Finished	06/08/2011 - 10:25:00 AM - 06/08/2011 - 11:25:00 AM Capture files: 13 (30.00 MB)	Download files	Delete files		Delete interception
t-197-20110608	Active	06/08/2011 - 12:54:00 PM - 06/08/2011 - 2:03:00 PM Capture files: 3 (52.37 MB)	Download files	Delete files		Delete interception

Lawful Interception System Copyright (C) 2009-2011, INVEA-TECH a.s.

Cisco IOS LI Protection

- Authentication is required
  - "Use of security level other than authNoPriv and authPriv prohibited"
  - SNMPv3 engine values must be known as well to calculate the authentication hash (MD5 or SHA1)
    - Changing the Engine-ID is probably a good idea
- Access Control Lists matching source IP addresses are commonly deployed ("infrastructure ACLs")
- SNMP user-groups can have individual ACLs
  - Nobody uses this
- SNMPv3 encryption
  - LI works without it, so nobody cares
- IPv6 is a topic of its own
- The SNMPv3 notifications provided are meant for the Mediation Device, not to notify a third party (like network operators)
  - The MD can disable SNMPv3 notification traps when registering by cTap2MediationNotificationEnable = false

REPUBLIC
U.S. KILLS BIN LADEN
al-Qaida leader killed in raid in Pakistan
Arkansas Democrat-Gazette
U.S. kills bin Laden

COUNTER-TERRORISTS WIN

That was the point, right?

CHANGING SIDES

Just as a thought experiment, mind you!

Options

- Don't use the Internet
- Use traffic that is not intercepted
- Detect interceptions monitoring you
- Take over the LI infrastructure
- Take over the Intercept Access Point (IAP)

Traffic Not Intercepted: #fail

- IOS XE: "The enforced lawful intercept license allows the Lawful Intercept (LI) feature to be used."
  - What if this license expires?
- VRF-based interception
  - That's how "secure" your "SP-VPN" is. MPLS-Cloud anyone? [1]
  - Causes packet drop and interface shutdowns with:
    - DHCP snooping, IP recirculation, Policy Based Routing (PBR), Reverse path forwarding (RPF), Server load balancing (SLB), WCCP
- LI is prioritized, and documented as doing so, causing side-effects with:
  - Optimized ACL logging (OAL): not functioning
    - Ooops, LI is implemented via ACLs! ☺
  - VLAN access control list (VACL) capturing: not function properly
  - Intrusion detection system (IDS): not function properly
  - IDS cannot capture traffic on its own, but captures traffic that has been intercepted by lawful intercept only [12]

Traffic Not Intercepted: #fail

- CSCty06990 [9]
  - Symptoms: Intercepted packets are not forwarded to MD.
  - Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.
  - Workaround: Remove and reapply TAP.
- CSCse80032 - Resolved in 12.2(18)ZY1 [10]
  - Symptoms: An SNMP Manager that uses SNMPv3 may not resynchronize the timer for the SNMP engine after the router has been reloaded.
  - Conditions: This symptom is observed on Cisco Catalyst 6500 series switch and Cisco 7600 series router that have been reloaded and occurs because a parameter is incorrectly set in the REPORT message, causing a mediation device to register an SNMP timeout instead of a reload.
  - Workaround: You may be able to restart the SNMP Manager to force the timer for the SNMP engine to resynchronize. Note, however, that doing so causes a 100-percent outage for all wiretaps that are served by the SNMP Manager. If you cannot restart the SNMP Manager, there is no workaround.

Traffic Not Intercepted: #mkfail

- "Stateful SwitchOver (SSO) and NonStop Forwarding (NSF) are not supported for wiretaps. When a switchover occurs between the active and standby supervisor engines, information about active wiretaps is deleted."[7]
  - Causing a switch-over is not considered a functional or security issue, as long as it worked
    - Anything crashing the SUP works
- "The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS)."[8]
  - Tell me Dan, what could possibly go wrong with that?

Traffic Not Intercepted: Size Does Matter

- LEA bandwidth and equipment might not measure up to the target
  - From the "Careful With That Axe Eugene"-department
- "To maintain router performance, lawful intercept is limited to no more than 2% of active calls." (e.g. 8 out of 4000) [11]
- 12.3(7)XI on a Cisco 10000 supports 6.4 Mbps active taps in total

  ➔The less predictable any traffic burst of the target is, the more likely it is that interception requests are expanded

    - The intercepting entity hates you for going out to party while you keep those mirror jobs running

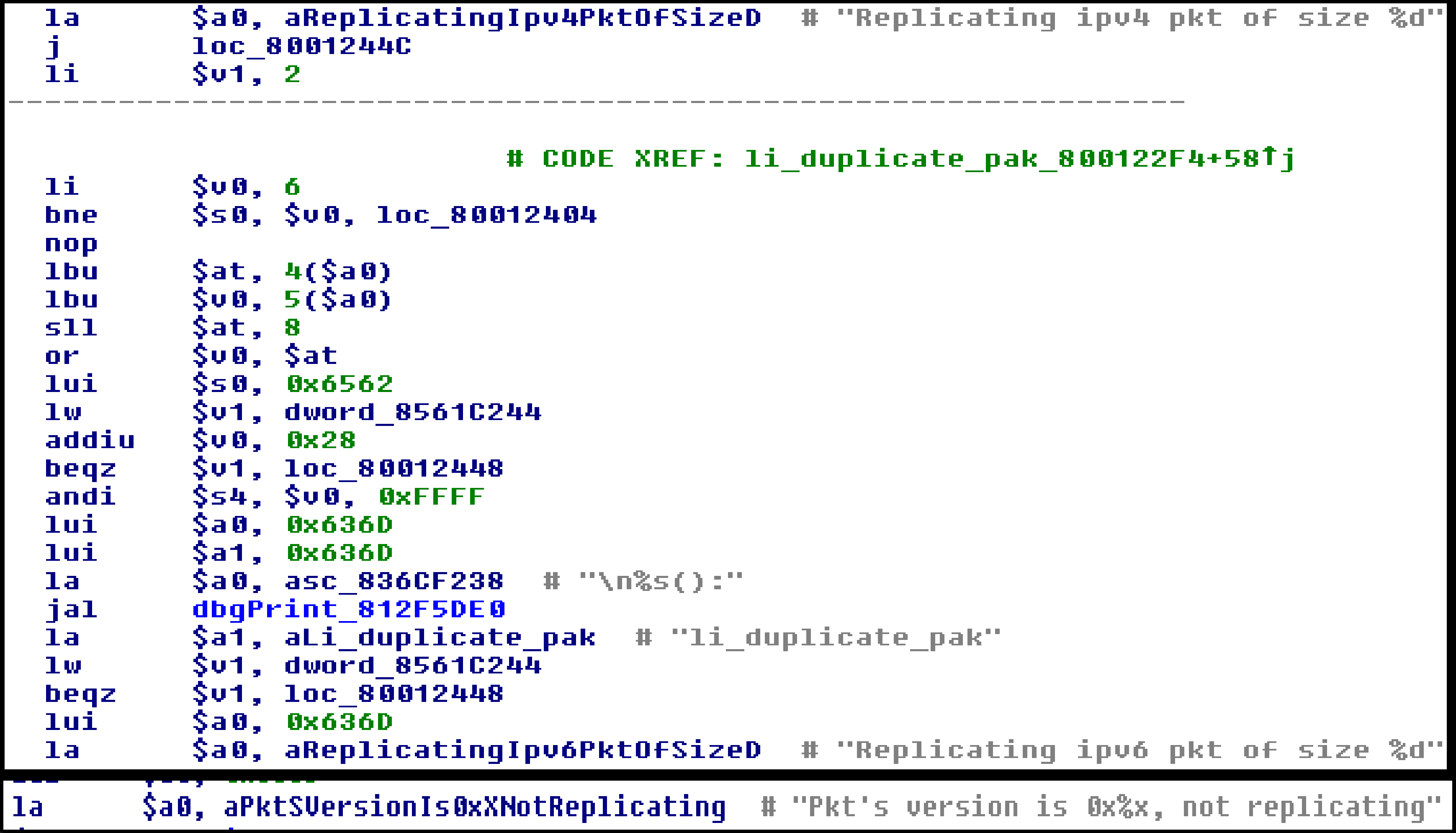
Traffic Not Intercepted: Numbers Do Matter

- Some lawful interception architectures use IPFlow instead of Cisco's tap MIB
- Flow tracking is based on sampling
  - Mostly random packet sampling, that is
- Sending an email while downloading large amounts of porn^Wdocumentaries drastically reduces the chance of the SMTP traffic being sampled
  - Chance being the keyword here!

The Compromised Observer Problem

- Obvious examples for desynchronizing ("confusing"[5]) the interpretation of the intercepted and the communicated information include:
  - IPv4 and IPv6 Fragmentation
    - IPv6 is more interesting for its lack of reliable payload classification. Also, the LEA must support IPv6 as well ;)
  - Invalid or ambiguous TCP SEQ/ACK values
  - IP, TCP and UDP Checksums
  - URI encoding and its interpretation
- A less obvious example is frequency and amplitude modulation of DTMF, as presented in [5]
- It's all just LangSec [6]
  - Does anyone notice the similarities to anti-virus and slightly corrupted compressed archives?

GTFO



```
  la      $a0, aReplicatingIpv4PktOfSizeD  # "Replicating ipv4 pkt of size %d"
  j       loc_8001244C
  li      $v1, 2
 ----------------------------------------------------------------


                           # CODE XREF: li_duplicate_pak_800122F4+58↑j
  li      $v0, 6
  bne     $s0, $v0, loc_80012404
  nop
  lbu     $at, 4($a0)
  lbu     $v0, 5($a0)
  sll     $at, 8
  or      $v0, $at
  lui     $s0, 0x6562
  lw      $v1, dword_8561C244
  addiu   $v0, 0x28
  beqz    $v1, loc_80012448
  andi    $s4, $v0, 0xFFFF
  lui     $a0, 0x636D
  lui     $a1, 0x636D
  la      $a0, asc_836CF238  # "\n%s():"
  jal     dbgPrint_812F5DE0
  la      $a1, aLi_duplicate_pak  # "li_duplicate_pak"
  lw      $v1, dword_8561C244
  beqz    $v1, loc_80012448
  lui     $a0, 0x636D
  la      $a0, aReplicatingIpv6PktOfSizeD  # "Replicating ipv6 pkt of size %d"
```

```
la      $a0, aPktSVersionIs0xXNotReplicating  # "Pkt's version is 0x%x, not replicating"
```

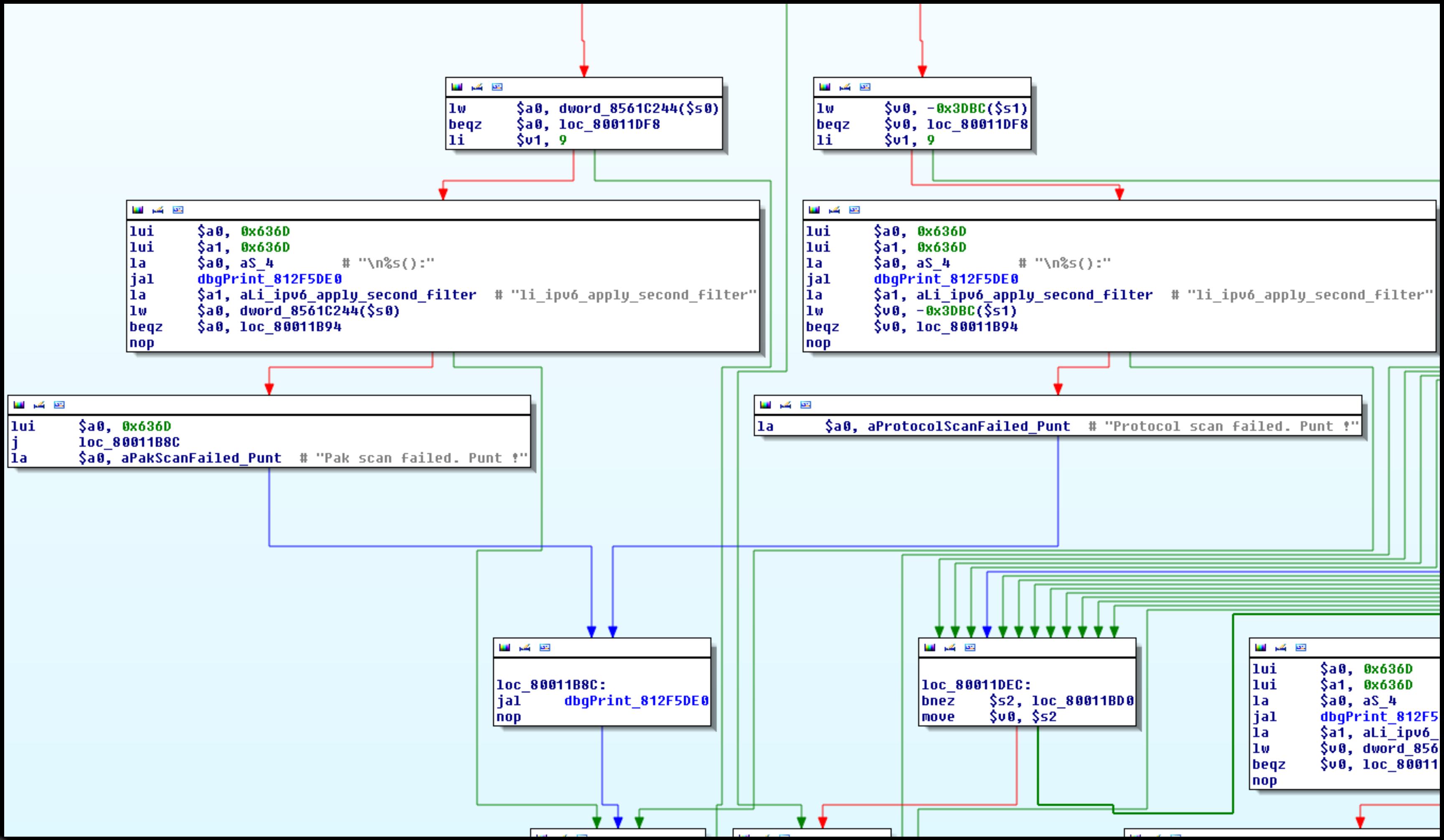
IPv5 is a Laser

- Take a regular IPv4 packet and modify the version field to the value 5
  - Surprisingly, this is forwarded by some routers
  - More surprisingly, some IPv4 stacks just answer
- Why? Several Data-Link Layer (2) protocols hint at the type of their Network Layer (3) payload
  - For example Ethernet 802.3
    - IPv4: 0x0800
    - IPv6: 0x86DD
  - Forwarding IPv4 stacks sometimes use the indication provided by the IEEE 802.3 payload-type field and ignore the IPv4 header value
    - This is not considered a security issue, since the decision to accept or reject the packet is up to the final recipient
- This is apparently easy to misinterpret: IPv5 is an example! **THIS IS NOT A GENERAL CIRCUMVENTION METHOD**

PRISM

Detecting Interceptions

TO HACK AND EXPLORE OLD EUROPE
Phenoelit



```
lw      $a0, dword_8561C244($s0)
beqz    $a0, loc_80011DF8
li      $v1, 9
```

```
lw      $v0, -0x3DBC($s1)
beqz    $v0, loc_80011DF8
li      $v1, 9
```

```
lui     $a0, 0x636D
lui     $a1, 0x636D
la      $a0, aS_4         # "\n%s():"
jal     dbgPrint_812F5DE0
la      $a1, aLi_ipv6_apply_second_filter  # "li_ipv6_apply_second_filter"
lw      $a0, dword_8561C244($s0)
beqz    $a0, loc_80011B94
nop
```

```
lui     $a0, 0x636D
lui     $a1, 0x636D
la      $a0, aS_4         # "\n%s():"
jal     dbgPrint_812F5DE0
la      $a1, aLi_ipv6_apply_second_filter  # "li_ipv6_apply_second_filter"
lw      $v0, -0x3DBC($s1)
beqz    $v0, loc_80011B94
nop
```

```
lui     $a0, 0x636D
j       loc_80011B8C
la      $a0, aPakScanFailed_Punt  # "Pak scan failed. Punt !"
```

```
la      $a0, aProtocolScanFailed_Punt  # "Protocol scan failed. Punt !"
```

```
loc_80011B8C:
jal     dbgPrint_812F5DE0
nop
```

```
loc_80011DEC:
bnez    $s2, loc_80011BD0
move    $v0, $s2
```

```
lui     $a0, 0x636D
lui     $a1, 0x636D
la      $a0, aS_4
jal     dbgPrint_812F5
la      $a1, aLi_ipv6_
lw      $v0, dword_856
beqz    $v0, loc_80011
nop
```

CounterStrike LI
Hot fork my dongle ...
Hypocrisy - Wikipedi...
08:15

Detecting Interceptions

- To "punt a packet" is Cisco slang for passing a packet for forwarding decision to the main CPU
  - This is generally considered a bad thing, since routers tend to run on >50% CPU load all the time
  - In management, this is called "escalation", having similar effects
- Interception targets can intentionally cause punting
  - This should be legal, even in Germany (IANAL)
  - Pushes the CPU load to 100% (like Java)
    - Triggers a watchdog process, reloading (= rebooting) the router
- Therefore, consider the following procedure:
  - Traceroute (A) to your communication partner
  - Send ~10000 packets to your communication partner that get punted only if a tap is in place
  - Traceroute (B) to your communication partner
  - If route A != route B: you or your communication partner are monitored (or your routing equipment sucks)

Taking over LI

- Although Sun Solaris and Windows 2000 may sound juicy, going after the Mediation Device is asking for trouble (i.e. it is highly illegal)
  - Besides, what's the challenge?
- The MD is very likely to be monitored closely by the compliance folks of the SP
  - Tech people don't care about LI
  - Compliance people care about not getting into trouble with the authorities – that's their job
    - Root shells on the MD get them into trouble
- I'm not even mentioning attacks on the LEAs
  - If you need to be told not to do it, all is lost anyway

Taking over IAPs

- CVE-2008-0960 hurts
  - memcmp(MyHMAC, PackHMAC, PackHMAC_len);
  - According to Tom Cross [1], almost none of the LI-enabled IOS images were affected
    - Very interesting by itself
    - The SNMP secret is almost guaranteed to be the same on all routers
      - Take over some other router to get the config
- SNMPv3 gives detailed feedback on authentication failures
  - Bonus feature: SNMPv3 authentication failures are not signaled to the network operators by SNMP traps ;)
    - It's standardized that way! [1]
- In case of ACLs, remember that we are talking about UDP
  - Applied BCP prevent spoofed packets – from other networks
- Apparently people have talked publicly about Cisco IOS exploitation before (and mentioned LI)
  - I'm not sure about that one though

TERRORISTS WIN

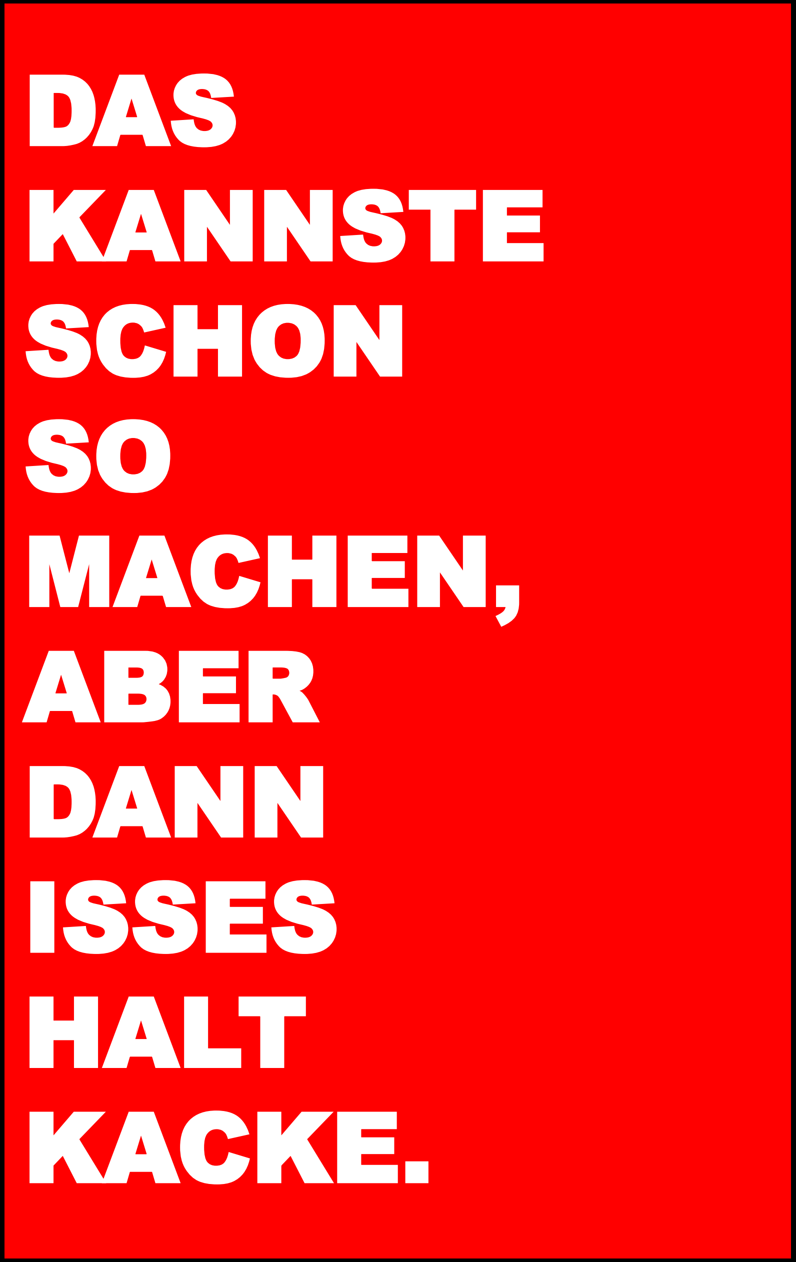
All they need to do is waiting for more interception code.

ENDER WINS – WITH FATALITY

But who does he win for? Does he care?

Conclusions

- **Routers shall not parse packet payloads!!1!**
  - RTFM, start with the f**king ISO OSI model this time!
    - You are not allowed to parse anything other than the destination address of IPv4 packets
- Evading lawful interception seems to be about as challenging as evading anti-virus
  - Did Nation State Actors possibly discover this quite some time ago?
- Weakening our critical infrastructures for everyone and their lobbyists is a disproportional measure
  - Infrastructure stability is never risked to fight crime
  - Why should the Internet be different?



DAS
KANNSTE
SCHON
SO
MACHEN,
ABER
DANN
ISSES
HALT
KACKE.

Credits: kannstemachen.de via momo

In gratitude dedicated to Mummel, Meredith, Jessica, Bine, nowin and the epic Smurfs
Kudos to Tom Cross and John N. Stewart

References

1. "Exploiting Lawful Intercept to Wiretap the Internet", Tom Cross, 2010
   - https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-wp.pdf
1. "Intelligence support systems: technologies for lawful intercepts", Paul Hoffmann, Kornel Terplan, 2006, ISBN 0-8493-2855-1
   - Mr. Hoffmann is the CEO of DATAKOM/GTEN, according to http://www.wikileaks.org/spyfiles/files/0/11_200702-ISS-DXB-GTEN1.pdf
2. "TREATY ON EUROPEAN UNION", Official Journal C 191, 29 July 1992
   - http://eur-lex.europa.eu/en/treaties/dat/11992M/htm/11992M.html
3. "The Computer as a Communication Device", J.C.R. Licklider, Robert W. Taylor, 1968, Science and Technology
   - http://www.cc.utexas.edu/ogs/alumni/events/taylor/licklider-taylor.pdf
4. "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic"
   - ETSI ES 201 671
5. "The Eavesdropper's Dilemma", Eric Cronin, Micah Sherr, and Matt Blaze, Technical Report MS-CIS-05-24
   - http://www.crypto.com/papers/internet-tap.pdf
6. **"Exploiting the Forest with Trees"**, Len Sassaman, Meredith L. Patterson, BlackHat USA, August 2010
   - http://www.youtube.com/watch?v=2qXmPTQ7HFM
7. http://www.cisco.com/en/US/customer/docs/routers/7600/ios/12.2SR/configuration/lawful_intercept/76LIch2.html#wp1058460
8. http://www.cisco.com/en/US/customer/docs/routers/10000/10008/configuration/guides/lawful_intercept/10LIconf.html
9. http://www.cisco.com/en/US/customer/docs/ios/12_2sr/release/notes/122SRcavs1.html
10. http://www.cisco.com/en/US/customer/docs/switches/lan/catalyst6500/ios/12.2ZY/release/notes/ol_13011.html
11. http://www.cisco.com/en/US/customer/docs/routers/10000/10008/configuration/guides/lawful_intercept/10LIconf.html
12. http://www.cisco.com/en/US/customer/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/lawful_intercept_configuration.html