

# Full Take Österreich *Die Maschinen wissen alles!*

*License CC0: "No Rights Reserved"*  
*2014-04-12 Barcamp Graz*

Arno "Mr. X" Nuehm  
*aka Anton*

[an.to\\_n-73@riseup.net](mailto:an.to_n-73@riseup.net)

PGP Fingerprint: 0B4C DF2C CB22 5DF4 25EA F212 49D1 ABF2 A2A9 7D7D  
Bitmessage: BM-2cTY8fuXGGXmh3fVgfQMaRCqTpgqp479ux  
I2P-Bote: an-ton\_4612



© Oliver Bienkowski

# Full Take Österreich

- Programmname MYSTIC

- Abgreifen ALLER elektronischen Kommunikation

- Zwischenpeichern für 30 T

- Automatisiertes Auswerten (Speech to text, semantische Erkennung, lernfähige Algorithmen, etc.)



- Bekannt seit Mo, 2014-04-07 (1)
- Bisher kein hartes Dementi! (2)  
*"Es gibt keinen Anknüpfungspunkt zwischen dem Verteidigungsministerium und einer möglichen Überwachung der NSA in Österreich"*  
→ Aber auch noch keine Belege veröffentlicht.
- Erstmals angewendet unter Gen. Keith Alexander 2005 im Irak (3)
- *Gerüchte* über Polen und Frankreich

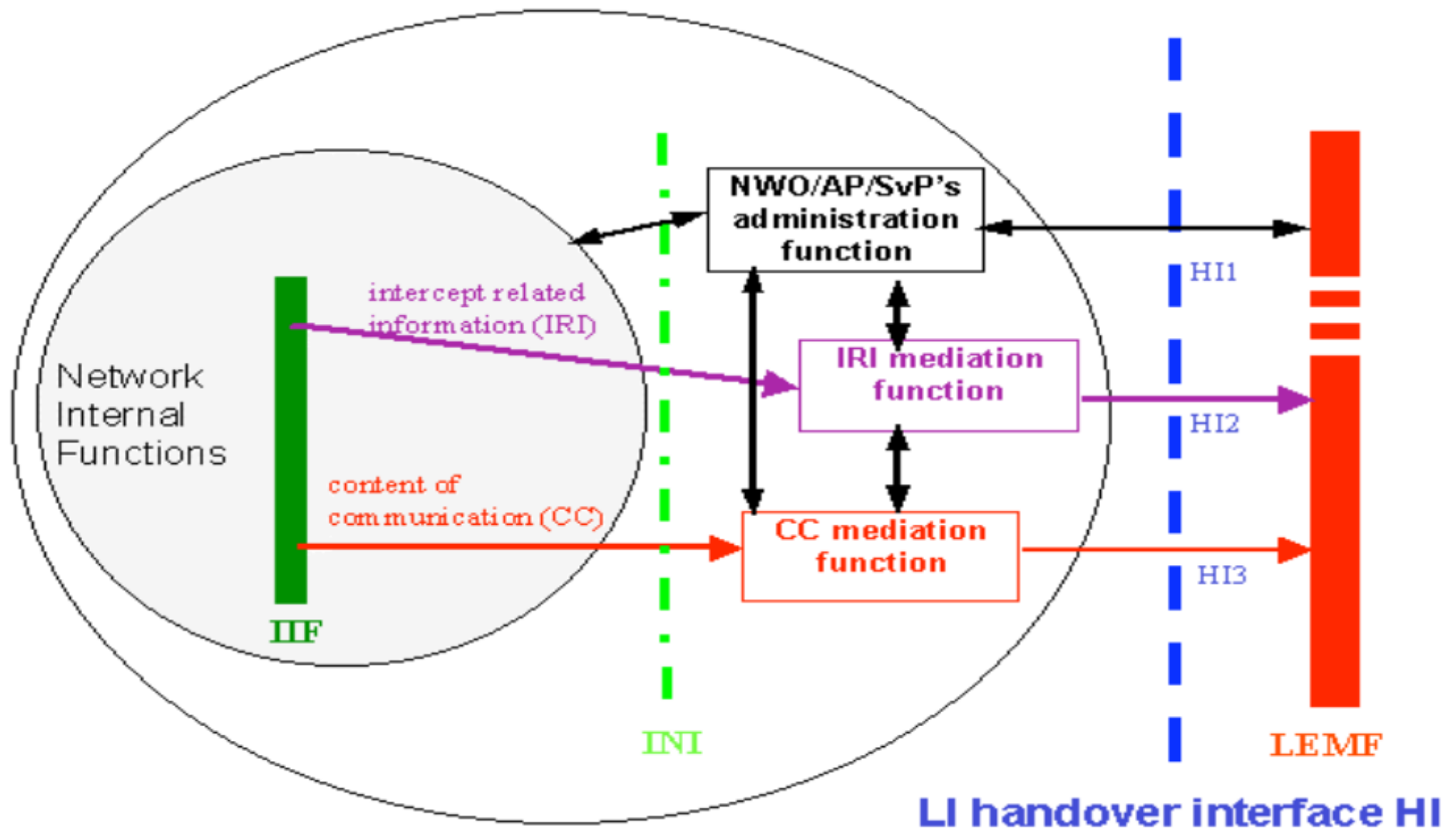
# Mögliche Schnittstellen

- Telefon – Richtfunkstrecken (hier Sendeturm Exelberg) (4)



- Vienna Internet eXchange, Knoten Wien (5)

- Standardisierte Abhör-Schnittstellen in ALLEN Telekom-Schaltschränken (6)(7)



Handover Interface Concept (TS 101 671)  
 (8) F. 22

# Ausnutzung Heartbleed

## Schwerer Fehler im SSL Protokoll (httpS)

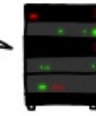
SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "POTATO" (6 LETTERS).



...this pages about "books". User Olivia requests  
secure connection using key "4538538374224".  
User Meg wants these 6 letters: POTATO. User  
Olivia wants pages about "irl games". Unlocking  
secure records with master key 5130985733435  
Note: (from user) reads this message: "H



...this pages about "books". User Olivia requests  
secure connection using key "4538538374224".  
User Meg wants these 6 letters: **POTATO**. User  
Olivia wants pages about "irl games". Unlocking  
secure records with master key 5130985733435  
Note: (from user) reads this message: "H

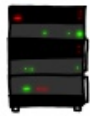


POTATO

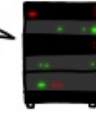
SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "BIRD" (4 LETTERS).



...User Olivia from London wants pages about "the  
bees in car why". Note: Files for IP 375.381.  
883.17 are in /tmp/files-3843. User Meg wants  
these 4 letters: BIRD. There are currently 346  
connections open. User Brendan uploaded the file  
ts-fc-fc-1 (contents: 834ba962e2c6b9ff89b43b6f8



...User Olivia from London wants pages about "the  
bees in car why". Note: Files for IP 375.381.  
883.17 are in /tmp/files-3843. User Meg wants  
these 4 letters: **BIRD**. There are currently 346  
connections open. User Brendan uploaded the file  
ts-fc-fc-1 (contents: 834ba962e2c6b9ff89b43b6f8



BIRD

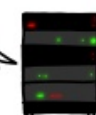
SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).



...a connection. Jake requested pictures of bees.  
User Meg wants these 500 letters: HAT. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



...a connection. Jake requested pictures of bees.  
User Meg wants these 500 letters: **HAT**. Lucas  
requests the "missed connections" page. Eve  
(administrator) wants to set server's master  
key to "14835038534". Isabel wants pages about  
snakes but not too long". User Karen wants to  
change account password to "CoHoBaSt". User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User

- EFF hat Spuren von Nutzung gefunden (11)

- Bericht 2014-04-12, Bloomberg  
NSA wusste kurz nach Entstehung 2012 von Fehler und nutzte diesen aktiv aus: *“(...) and regularly used it to gather critical intelligence, two people familiar with the matter said. (...)”* (12)

Aber: Sofortiges kategorisches Dementi! (13) → ? Was stimmt ?



- Heartbleed Exploit hinterläßt keine Spuren!

- Möglichkeit: Maschinelle Nutzung auf Knopfdruck.

Massenabgriff unwahrscheinlich, aber gezielte Nutzung. "Persons of interest"

**=> Es gibt noch viel mehr unentdeckte "Heartbleeds"! Bei den Profi-Crackern mit hohem Budget.**



## Quellen

1) <http://www.format.at/articles/1414/524/374054/nsa-oesterreich>

2)

<http://derstandard.at/1395364765315/Verteidigungsministerium-Keine-Verwicklung-in-NSA-Ueber>

3) <http://www.latimes.com/nation/la-na-alexander-nsa-20140331,0,3369988,full.story>

4) [http://www.peterpilz.at/2013-11/peter-pilz-tagebuch.htm#t\\_15](http://www.peterpilz.at/2013-11/peter-pilz-tagebuch.htm#t_15)

5) [https://de.wikipedia.org/wiki/Vienna\\_Internet\\_eXchange](https://de.wikipedia.org/wiki/Vienna_Internet_eXchange)

6) <http://www.heise.de/tp/artikel/7/7220/1.html>

7) <http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception>

8)

[https://wikileaks.org/spyfiles/docs/etsi/28\\_etsi-tc-li-overview-on-lawful-interception-and-retained-d](https://wikileaks.org/spyfiles/docs/etsi/28_etsi-tc-li-overview-on-lawful-interception-and-retained-d)

9) <https://xkcd.com/1354/>

10)

<http://www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html>

11)

<https://www.eff.org/deeplinks/2014/04/wild-heart-were-intelligence-agencies-using-heartbleed-now>

12)

<http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-co>

13)

<http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa->