Progetto Mempo
Hardened Privacy for paranoic people

whoami

Consulente informatico IT

- Membro CLUSIT,olografix,soldierx..ecc
- Titolare LEJOT Opensource tecnology
- I like unix <;-)
- Currently security IT specialist on lejot.info

SOLDIERX.COMv2.0
SOLDIERX
NOBODY CAN STOP INFORMATION INSEMINATION
- UNITED WE STAND -

Clusit
Associazione Italiana
per la Sicurezza Informatica

End Summer Camp settembre 2015 VE italy

Mempo project aims to provide most secure and yet comfortable out-of-the-box Desktop and Server computer, for professionals, business, journalists, and every-day users avoiding PRISM-like spying.

ESC 2015

- 73% dei dirigenti sono convinti della solidità delle pratiche di sicurezza
- 41% non sa quanti incidenti negli ultimi 24 mesi o non sa che tipo di incidenti sono avvenuti
- Sicurezza IT:supervisione quotidiana dei sistemi IT e della loro sicurezza
- La sicurezza del sodice è un processo da inseire nella strategia security it

Security Taxonomy

- Mobile Device Security
- Encryption
- Security Management
- Internal Security
- Identity & Access Mgmt
- Perimeter Security
- Storage Security
- Physical Security

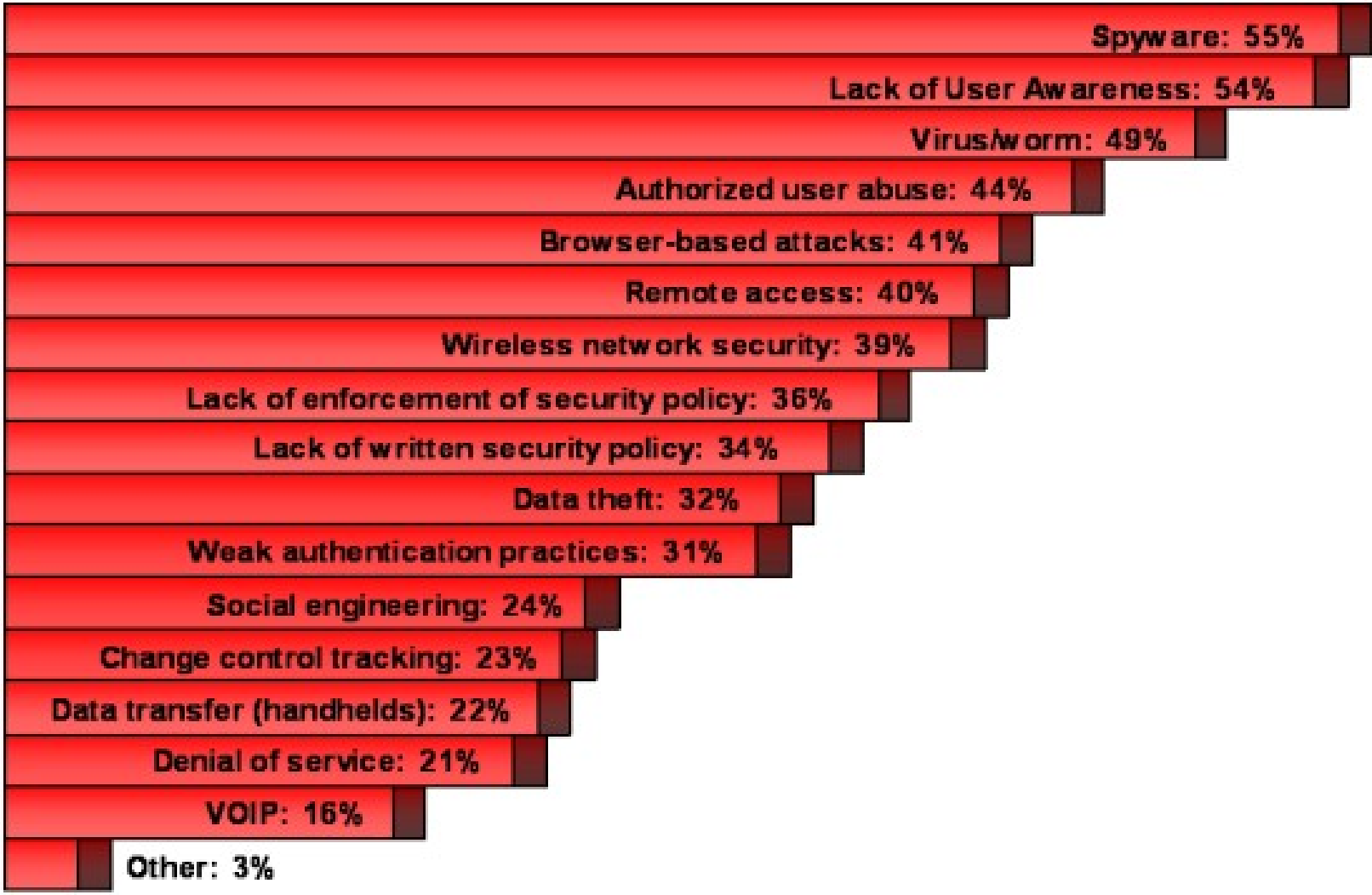
ESC 2015

- La sicurezza informatica è un processo, non un prodotto, non vi è nulla che con il semplice acquisto garantisca la sicurezza della nostra infrastruttura.La sicurezza della nostra rete dipende da molti fattori, i software firewall è solo uno di essi!

ESC 2015

- Audit e sicurezza IT dovrebbero lavorare insieme in un unico ciclo procedurale
- Il mio sistema operativo è sicuro
- Aggiornamento software?
- Installazioni patch critiche di sicurezza entro un mese?
- Scrivo un software e il testing prima del rilascio?

Top Security Threats



ESC 2015

- Injection
- Cross-site scripting(XSS)
- Verifica credenziali
- Security Misconfiguration..quali filtri?..lasciamo il default.....è più facile comprare una scatola che gestire un processo di analisi e sviluppo...si deve accertare che gli input da parte dell'utente al browser dell'applicazione sia controllato attraverso validazione degli input prima di essere inviati alle pagine di output.

ESC 2015

- Rimozione account/dati di test prima dei passaggi in produzione
- Separazione degli ambienti di sviluppo e produzione in termini sistemistici e di personali
- Uso di tecniche di programmazione sicura
- La sicurezza richiede che non siano presenti
- funzionalità non richieste
- Approccio del minimo privilegio
- Sicurezza,qualità e progetti
- Sicurezza sempre valutata da capo e su tutto.

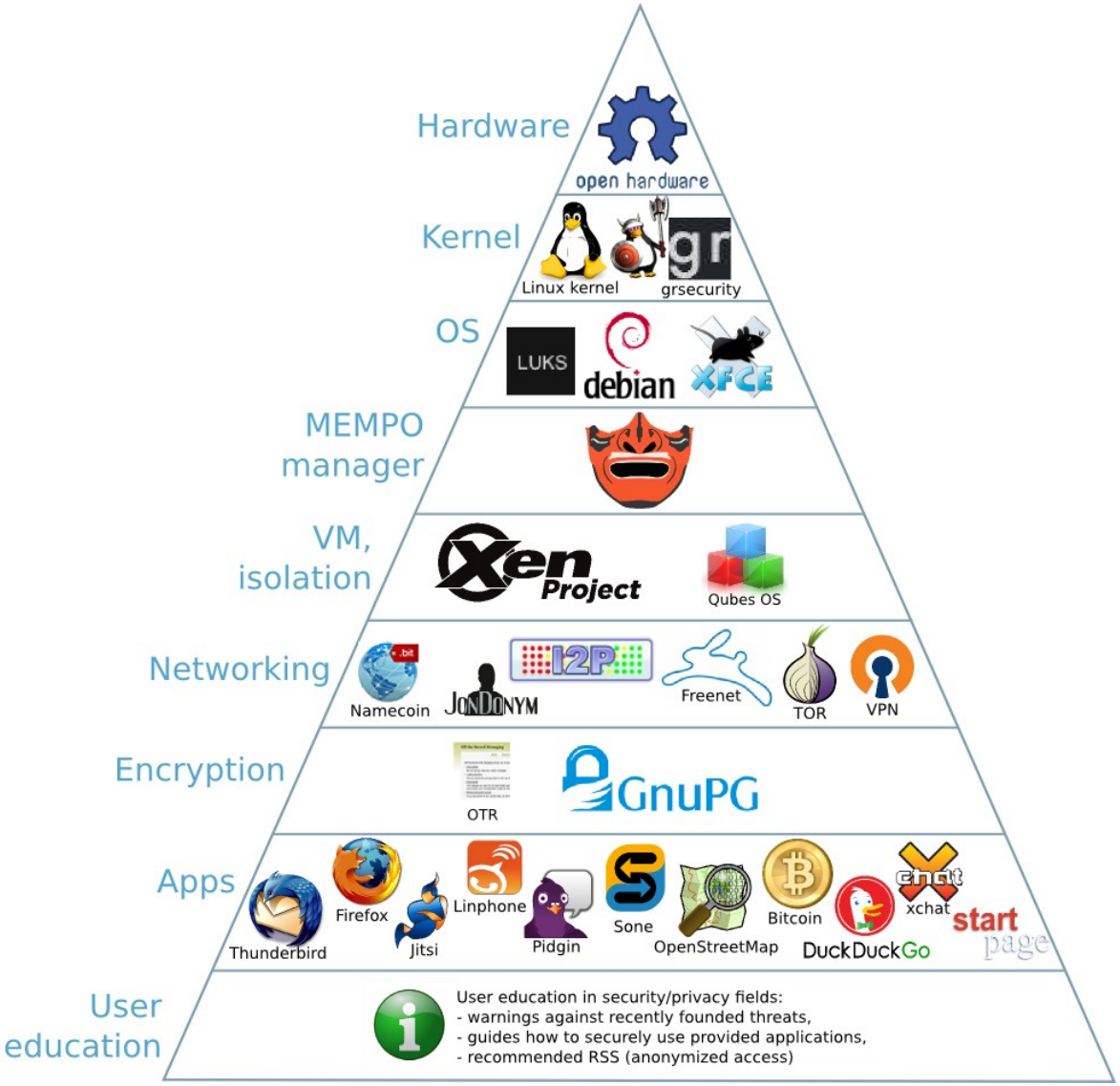
ESC 2015

- ➲Pochissimi sono i veri Progetti di Sicurezza IT crittografia,Autenticazione,...
- ➲Spesso si vede la“Messa in Sicurezza” di un Sistema IT tramite “Cerotti”si sente spesso..se il sistema fosse stato progettato e implementato bene fin dall'inizio non avrebbe bisogno di cerotti che hanno funzionalità temporanea
- ➲Revisionare il codice è il modo più efficace di verificare se un'applicazione è sicura. I test possono solo verificare che un'altra applicazione non è sicura.

ESC 2015

- https://wiki.debian.org/Mempo
- https://github.com/mempo/
- http://deb.pl.mempo.org/
  http://deb.pl.mempo.org/index-all.html
- http://deb.pl.mempo.org/#news_archive
- http://deb.pl.mempo.org/#postinstall

ESC 2015


Hardware
open hardware
Kernel
Linux kernel
grsecurity
OS
LUKS
debian
XFCE
MEMPO manager
VM, isolation
Xen Project
Qubes OS
Networking
Namecoin
JONDONYM
I2P
Freenet
TOR
VPN
Encryption
OTR
GnuPG
Apps
Thunderbird
Firefox
Jitsi
Linphone
Pidgin
Sone
OpenStreetMap
Bitcoin
DuckDuckGo
xchat
start page
User education
User education in security/privacy fields:
- warnings against recently founded threats,
- guides how to securely use provided applications,
- recommended RSS (anonymized access)

ESC 2015 italian grappa

- 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.

ESC 2015 italian grappa

- Only grsecurity provides protection against zero-day and other advanced threats that buys administrators valuable time while vulnerability fixes make their way out to distributions and production testing. This is made possible by our focus on eliminating entire bug classes and exploit vectors, rather than the status-quo elimination of individual vulnerabilities.

ESC 2015 MEMPO

- Variant serv-Extra protection. For Server (or compatible desktop). All grsecurity is used, including kmem/IOports.

- Variant desk-Good protection. For Desktop. All grsecurity is used, except kmem/IOports.

  Therefore video cards should work (on open-source drivers, binary blobs might not work).

ESC 2015 italian grappa

- Only grsecurity provides protection against zero-day and other advanced threats that buys administrators valuable time while vulnerability fixes make their way out to distributions and production testing. This is made possible by our focus on eliminating entire bug classes and exploit vectors, rather than the status-quo elimination of individual vulnerabilities.

ESC 2015 italian grappa

ESC 2-6 settembre VE italy italian grappa,arp-sp..

- Tnx per la vostra attenzione by ryuw
- fabiocarlettiryuw@gmail.com