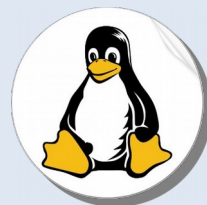




GreekLUG



Ελεύθερο Λογισμικό &



Λογισμικό Ανοικτού Κώδικα



Μάθημα 9ο



Ασφάλεια & Αντίγραφα



Ύλη Μαθημάτων VIII

Μαθ. 9 : Ασφάλεια & Αντίγραφα

- Ασφάλεια/Κρυπτογράφηση (cryptkeeper, keepassx, rgr),
- Δίσκοι (gparted, smartmontools),
- sensors,
- Αντίγραφα ασφαλείας / CloneZilla





Ασφάλεια σε Λ/Σ GNU/Linux

Ανάγκη για ασφάλεια



- › Διαθέσιμος ο κώδικας του Λ/Σ & Εφαρμογών
==
Γνωρίζουμε τι τρέχουμε

Προβλήματα

- › Επικοινωνία
- › Ανταλλαγή πληροφοριών
πχ δεδομένα web, ηλεκτρονική αλληλογραφία

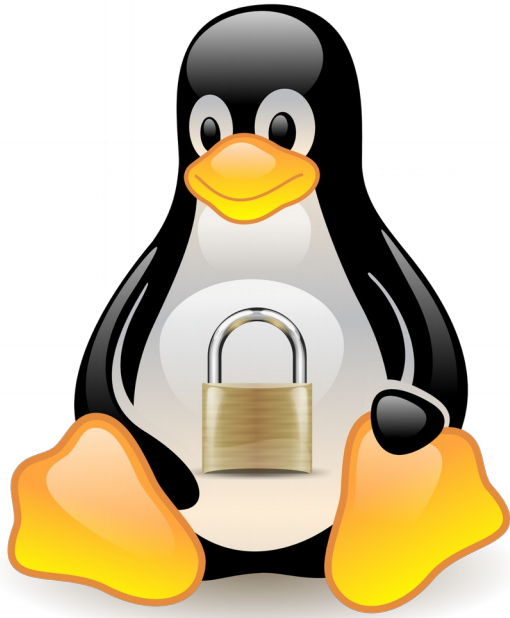
Λύσεις

- › Firewall
- › Μερική ή ολική κρυπτογράφηση



Επίπεδα κρυπτογράφησης

Ανάγκη για ασφάλεια



- › Κωδικοί και δεδομένα
- › Αρχεία και φάκελοι

ΣΥΣΤΗΜΑ ΑΡΧΕΙΩΝ

- › Τμήμα του συστήματος
- › Όλο το σύστημα

ΣΥΣΚΕΥΕΣ		ΑΡΧΕΙΑ	
Loop-AES	dm-crypt +/- LUKS	eCryptfs	EncFs

https://wiki.archlinux.org/index.php/Disk_encryption



Διαχειριστής κωδικών KeePass/KeePassX



- › Το KeePass είναι ένα λογισμικό διαχείρισης κωδικών

Αποθηκεύει ονόματα χρήστη, κωδικούς πρόσβασης, τομείς, σημειώσεις και πολλά άλλα στοιχεία, σε μια ασφαλή κρυπτογραφημένη βάση δεδομένων, που προστατεύεται από ένα μόνο κύριο κωδικό πρόσβασης ή/και αρχείο κλειδιού.

Η κρυπτογραφημένη βάση δεδομένων αποθηκεύεται σε τοπικό επίπεδο.

- › Τελευταία έκδοση: v1.29/v2.30, Απρίλιος/Αύγουστος 2015

- › Υποστήριξη για Λ/Σ: Windows | *Linux, Mac OS, BSD

- › Url: <http://keepass.info/>

KeePassX

- › Υποστήριξη για Λ/Σ Linux
- › Url: <http://www.keepassx.org/>





Διαχειριστής κωδικών KeePass/KeePassX



The screenshot shows the KeePass application window titled "MyDatabase.kdbx - KeePass". The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar, and a tree view on the left showing a database structure with groups like "General", "Windows", "Network", "Internet", "eMail", "Homebanking", and "0 Group" through "8 Group". The main area displays a table of entries:

Title	User Name	Password	URL	Notes
Sample #11	Anonymous	*****	google.com	Some Notes
Sample #28	Anonymous	****		
Sample #29	Anonymous	****		
Sample #35	Anonymous	****		
Sample #47	Anonymous	****		
Sample #50	Anonymous	****		
Sample #73	Anonymous	****		
Sample #77	Anonymous	****		
Sample #80	Anonymous	****		
Sample #81	Anonymous	****		
Sample #87	Anonymous	****		
Sample #97	Anonymous	****		
Sample #111	Anonymous	****		
Sample #114	Anonymous	****		

A context menu is open over the "Sample #11" entry, listing actions such as "Copy User Name", "Copy Password", "URL(s)", "Perform Auto-Type", "Add Entry...", "EditView Entry...", "Duplicate Entry", "Delete Entry", "Selected Entries", "Select All", "Clipboard", and "Rearrange". The status bar at the bottom indicates "1 of 146 selected" and "Ready".



Κρυπτογράφηση: CryptKeeper/GEncfsM
















- Το CryptKeeper είναι μια δωρεάν και ανοικτού κώδικα εφαρμογή διαχείρισης κρυπτογραφημένων φακέλων με το σύστημα **EncFS**
- Αντίστοιχη εφαρμογή ενσωματωμένη στο γραφικό περιβάλλον GNOME, είναι η GEncfsM
- Τελευταία έκδοση: v0.9.5
- Υποστήριξη για Λ/Σ: Linux
- Url: <https://tom.noflag.org.uk/cryptkeeper.html>
Url: <http://libertyzero.com/GEncfsM/>





Κρυπτογράφηση: CryptKeeper/GEncfsM



Όνομα
 4nHfWCnwkobMfjucWW3mTSx9SF0eKwJTUIPeMH,rdDkht1
 dKdegb80sx4PAkj1XNEXq93l
 f0iWPWRCjGh,TYcGFAkoTXh4WmDWOe0O5PkPoIY-ckBV51
 fTktiXgAs8ht093FIIt0A-92
 GQ9nf0EcMSQBxKX0UvKR1b8s
 M6vd5iXuDxMIJmI3iepNXXGP
 MOHH2lmVqRp3EVxxBRtjitCltyBIK3OYpGLa7TmApKrNA0
 O,DVzIFaRrH2nhEmMNYeOSV0
 oWRywe1AogEByvGHHLNnS0IK
 y7Dmq9tYVS26E-lo3EEg68wx
 zicsItuijDuQ464X,0qXJQ0c
 Z,Z1f9AKhYkj71jHhmpnKj08
 3erbKP2oqAIkUk6O-RflxHJQrwa,cBaMcdOeRMsO7WQYF-
 4iMgAW5LiPEPh1MEizuySmTwCx0EuSfuwLzqCFpLH9rSv0
 77,tT9jym9t7tL4YaS1263dm6RVCqMHiKdGhNKGdzCop-
 81ypo1c,17DfA6KS,r3fyd4h07TqUezSGbhghUcc7U3Jn1
 bgS3mY,CNCp3hb9FNk8zk5TNUbRIVR,,OZmPqLFqjxDab0
 bHMGojHdgOlem4HMGz6Ay-lw



Κρυπτογράφηση: PGP

Κρυπτογράφηση δημοσίου κλειδιού

Κάθε χρήστης έχει τα δικά του κλειδιά

- › ένα ιδιωτικό
- › ένα δημόσιο

Σημεία κρυπτογράφησης

- › Κείμενο
- › Υπογραφή

Κείμενο

Μαθήματα πληροφορικής 2015!

Κείμενο με κρυπτογράφηση

-----BEGIN PGP MESSAGE-----

Version: GnuPG v2

jA0EAWMC70UAaa1T7+3yUFqTEuEzTX6rVjf6V9Dqbc7pU
MOIPq+ca8YoVGxHlgnUiiLA1hdfpX3FA1A24bH9IXqn0TS
GloU2IRTV3WIKIchw

-----END PGP MESSAGE-----





Αντίγραφα Ασφαλείας I

Διαπλατφορμικά/δικτυακά αντίγραφα ασφαλείας

- › Bacula

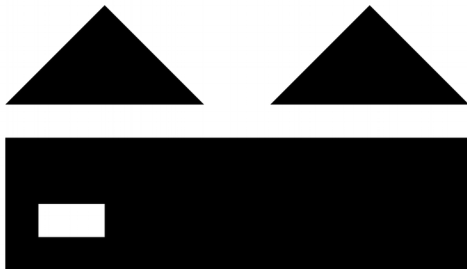
Πλήρη αντίγραφα ασφαλείας

- › Clonezilla

Τοπικά αντίγραφα ασφαλείας

Συγχρονισμός αρχείων

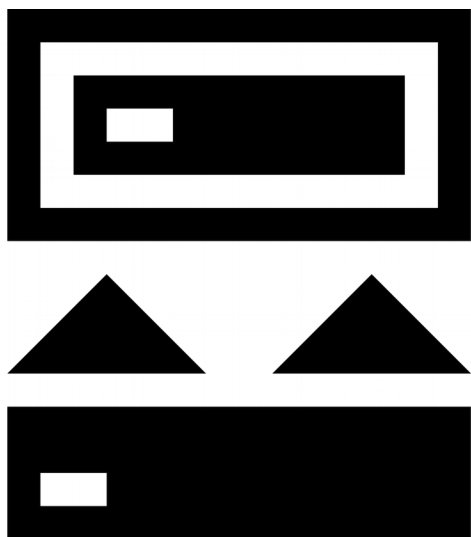
- › rsync/grsync
- › Déjà Dup
- › backintime
- › luckyBackup





Αντίγραφα Ασφαλείας II

Προτεινόμενοι κανόνες



- Το αντίγραφο θα πρέπει να είναι σε άλλη “τοποθεσία” (διαφορετικό δίσκο ή υπολογιστή ή διακομιστή κτλ...)
- Δεν επαρκεί απλά η λήψη του, αλλά θα πρέπει να δοκιμαστεί ώστε να γνωρίζουμε ότι δουλεύει σωστά και ότι σε περίπτωση προβλήματος θα μπορέσουμε να ανακτήσουμε τα δεδομένα μας
- Συνδυασμός αντιγράφων, πχ λήψη αντιγράφου εικόνας με το Clonezilla ανά 6 μήνες & εβδομαδιαία λήψη μέσω rsync

Προσοχή! την ώρα λήψης τοπικών αντιγράφων δεν θα πρέπει να χρησιμοποιείτε τα αρχεία που θέλετε να λάβετε αντίγραφο καθώς αν αντιγράψετε ένα αρχείο την ώρα που αυτό αλλάζει / τροποποιείται από τρίτο πρόγραμμα, το αντίγραφο ασφαλείας πιθανώς δεν θα είναι λειτουργικό