



Σεμινάρια Linux Essentials



Βασικές & πρακτικές
γνώσεις πάνω στο
Λ/Σ GNU/Linux



Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή I

Όλα ξεκίνησαν στο MIT της Μασαχουσέτης των ΗΠΑ, το **1983** όπου ο **Richard Stallman** ξεκίνησε το **Έργο GNU**.

Στις δεκαετίες του 1950, του 1960, και του 1970, οι χρήστες των υπολογιστών μπορούσαν να χρησιμοποιήσουν και να διανέμουν ελεύθερα τα προγράμματα ενώ το λογισμικό μοιράζονταν ευρέως από τα άτομα που χρησιμοποιούσαν τους υπολογιστές αλλά και από τους κατασκευαστές.

Στα τέλη όμως της δεκαετίας του 1960, η εικόνα άλλαξε και σταδιακά εμφανίστηκε μια βιομηχανία λογισμικού, η οποία δημιουργούσε τα ιδιοταγή-κλειστά λογισμικά (όπως τα γνωρίζουμε σήμερα), ανεβάζοντας το κόστος του λογισμικού δραματικά.



Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή II

Στην προσπάθεια να διασφαλίσει την ελευθερία του λογισμικού για όλους, ο Richard Stallman και η ομάδα του, ξεκίνησε να αναπτύσσει ένα σύνολο προγραμμάτων που θα είχαν όλες αυτές τις βασικές ελευθερίες στο **Έργο GNU**.

Σύντομα αρκετοί άνθρωποι συμμερίστηκαν τις απόψεις του και έτσι το **1985** ιδρύθηκε το Ίδρυμα Ελεύθερου Λογισμικού (**FSF**).

Η ομάδα του FSF σταδιακά ανέπτυξε εφαρμογές και προγράμματα για τις διάφορες χρήσεις ενός υπολογιστή, για παράδειγμα έναν κειμενογράφο με τον οποίο κάποιος θα μπορούσε να συντάξει ελεύθερα κείμενα κτλ.

Ο μεγαλύτερος στόχος όμως ήταν να δημιουργηθεί ένα ελεύθερο Λειτουργικό Σύστημα, που είναι ουσιαστικά το κυριότερο πρόγραμμα που τρέχει ένας υπολογιστής.



Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή III

1983: Έναρξη του έργου **GNU**
από τον Richard Stallman



1985: Ίδρυμα Ελεύθερου
Λογισμικού (**FSF**)

1989: Γενική Άδεια Δημόσιας
Χρήσης **GNU GPL**





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή IV

1991: Ο Φιλανδός Linus Torvalds αρχίζει να αναπτύσσει έναν πυρήνα (Linux) με σκοπό την ανάπτυξη ενός προσομοιωτή τερματικού, για πρόσβαση στα συστήματα UNIX του Πανεπιστημίου του Ελσίνκι!

1992: Εμφάνιση των πρώτων διανομών ***GNU/Linux***





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή V

Ο συνδυαστικός όρος “**Ελεύθερο Λογισμικό / Λογισμικό Ανοικτού Κώδικα**” (ΕΛ/ΛΑΚ) επικράτησε τελευταία, και περιγράφει κάθε λογισμικό που διασφαλίζει τις 4 ελευθερίες του Ελεύθερου Λογισμικού και, συγχρόνως, ακολουθεί το μοντέλο ανάπτυξης Ανοικτού Κώδικα.

Στα Αγγλικά επικράτησε ο όρος “**Free/Libre Open Source Software**” (FLOSS) για να ξεπεραστεί η αμφισημία του Αγγλικού όρου “free” (που μπορεί να εννοηθεί ως “ελεύθερο” αλλά και ως “δωρεάν”).



Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Εισαγωγή VI

Ο όρος «**Ελεύθερο**» εννοεί «**ΕΛΕΥΘΕΡΙΑ ΧΡΗΣΗΣ λογισμικού**».

ΔΕΝ αναφέρεται στην τιμή του λογισμικού
(αν και πολλά προγράμματα ΕΛ/ΛΑΚ παρέχονται δωρεάν)

- (0) **Ελευθερία εκτέλεσης** του λογισμικού, για οποιονδήποτε σκοπό.
- (1) **Ελευθερία μελέτης** του πηγαίου κώδικα (δηλ. του μηχανισμού λειτουργίας) του λογισμικού και **Ελευθερία τροποποίησής** του.
- (2) **Ελευθερία αναδιανομής** σε όσους φίλους, γείτονες, μαθητές ή και σε οποιουσδήποτε άλλους!
- (3) **Ελευθερία διανομής τροποποιήσεων / βελτιώσεων** στο ευρύ κοινό, για να επωφελείται ΟΛΗ η κοινωνία.



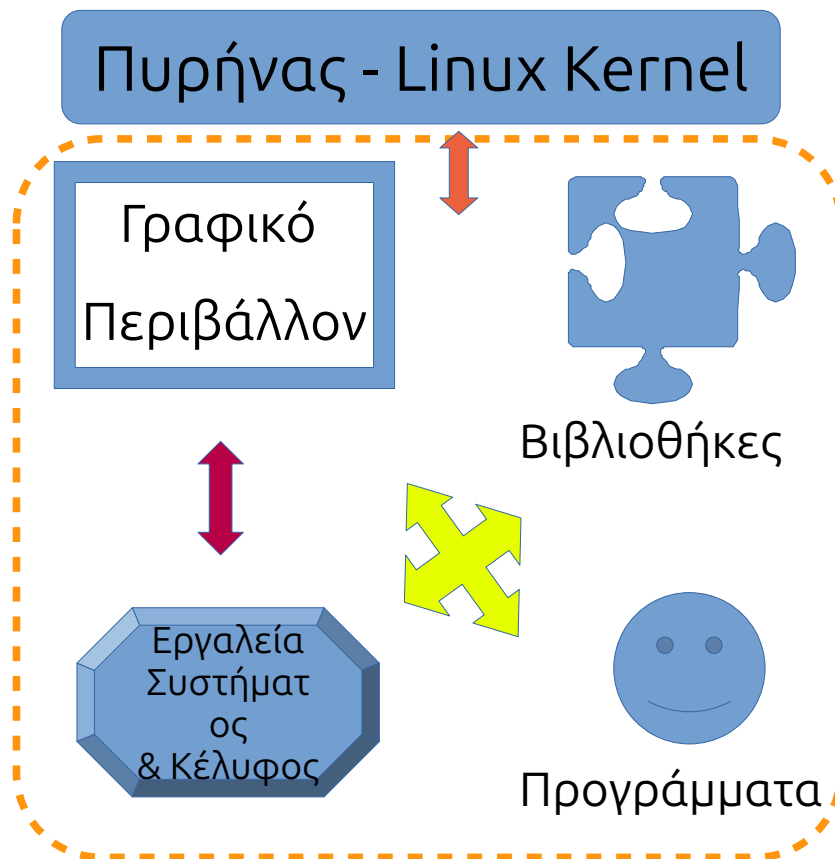
Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Διανομές Linux I





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Διανομές Linux II

Διανομή = ...





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Διανομές Linux III

Debian GNU/Linux (desktop ή server)

Ubuntu desktop (LTS & ενδιάμεσες εκδόσεις)

Ubuntu Server

Linux Mint

*LTS = Long Term Support (5 χρόνια)

**Νέες LTS εκδόσεις Ubuntu κάθε 2 χρόνια

***Νέες ενδιάμεσες εκδόσεις Ubuntu κάθε 6 μήνες

Debian based διανομές: **dpkg** package manager
(πακέτα .deb)





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Διανομές Linux IV

- **Red Hat Enterprise Linux - RHEL** (server)

CentOS (desktop χρήση)

- Rocky Linux & Alma Linux (συμβατά με RHEL - χρήση σε servers)

- **Fedora** (desktop χρήση)
νέα πακέτα, χρήση ως testing για RHEL

- **SUSE Linux Enterprise Server**
openSUSE (desktop, rolling release & σταθερή)

- Arch Linux (rolling release)
- Kali Linux (για εύρεση ευπαθειών λογισμικού)

→ RPM package manager
(πακέτα .rpm)

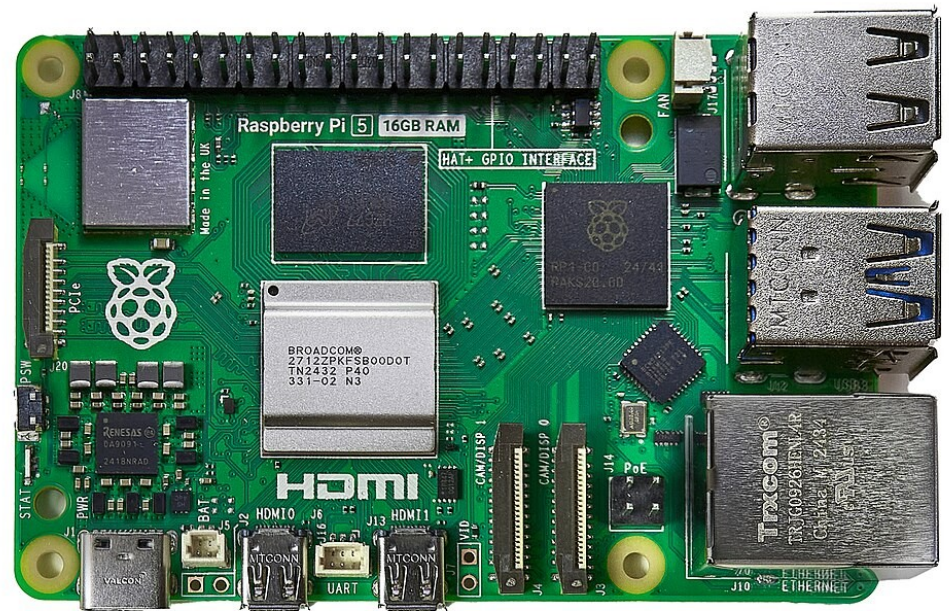
*Rolling release: Δεν υπάρχουν εκδόσεις, αλλά συνεχόμενες καθημερινές ενημερώσεις



Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Ενσωματωμένα Συστήματα

Ενσωματωμένα συστήματα

- συνδυασμός υλικού και λογισμικού για συγκεκριμένη χρήση.
- Βασίζονται σε πυρήνα Linux
 - Android συσκευές (κινητά, αυτοκίνητα, τηλεοράσεις)
 - Πλακέτα Raspberry Pi (Raspberry Pi OS)





Θέμα 1: Το Linux & το Ανοιχτό Λογισμικό – Linux & Cloud

- Πλειοψηφία των δημόσιων server παγκοσμίως τρέχει Linux (AWS, GCP κτλ)
- **Cloud** = Αγορά πόρων από ένα server για εξυπηρέτηση αναγκών
- Εικονικές μηχανές που φιλοξενούν ένα image (Linux διανομή)

Παράδειγμα: **Infrastructure as a service (IaaS)**





Θέμα 2: Κύριες Εφαρμογές Ανοιχτού Κώδικα – διαχείριση πακέτων λογισμικού

Διανομές	Πληροφορίες για ένα πακέτο	Εγκατάσταση πακέτου	Αφαίρεση πακέτου	Πακέτα προς αναβάθμιση	Αναβάθμιση πακέτων
Debian based	<code># apt show</code>	<code># apt install</code>	<code># apt remove</code>	<code># apt update</code>	<code># apt dist-upgrade</code>
RHEL-Fedora-Alma-Rocky	<code># dnf info</code>	<code># dnf install</code>	<code># dnf remove</code>	<code># dnf check-update</code>	<code># dnf upgrade</code>
SUSE/openSUSE	<code># zypper info</code>	<code># zypper install</code>	<code># zypper remove</code>	<code># zypper update</code>	<code># zypper dist-upgrade</code>

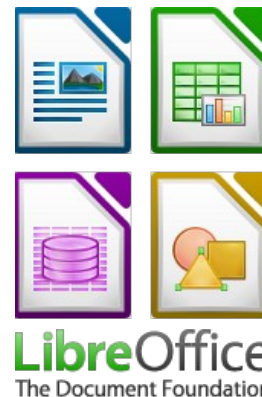


Θέμα 2: Κύριες Εφαρμογές Ανοιχτού Κώδικα – Εφαρμογές γραφείου

OpenOffice → **LibreOffice**



- Συμβατά με Microsoft Office
- Open Document Formart (ODF) Ανοιχτή μορφή αρχείων – τα έγγραφα μπορούν να μεταφερθούν μεταξύ Λ/Σ
- Επεξεργαστής κειμένου (Writer)
- Υπολογιστικά φύλλα (Calc)
- Παρουσιάσεις (Impress)
- Διανυσματικά σχέδια (Draw)
- Μαθηματικοί τύπου (Math)
- Βάση δεδομένων (Base)





Θέμα 2: Κύριες Εφαρμογές Ανοιχτού Κώδικα – Περιηγητές, Πολυμέσα & προγράμματα server

Περιηγητές διαδικτύου:

Chromium, Mozilla Firefox

Γραφικά:

- **Blender** (δημιουργία τρισδιάστατων αντικειμένων/σχεδίων)
- **GIMP** (επεξεργασία εικόνας) – υποστήριξη JPEG, PNG, GIF, TIFF
- **Inkscape** (διανυσματικός επεξεργαστής γραφικών) – αρχεία SVG
- **Audacity** (επεξεργασία ήχου) – υποστήριξη MP3, WAV, OGG, FLAC κ.λπ.
- **VLC** (αναπαραγωγή πολυμέσων)

Προγράμματα Server:

- **Apache, NGINX** (ανοικτού λογισμικού προγράμματα HTTP server)
- **MariaDB, MySQL, PostgreSQL** (ανοικτού λογισμικού βάσεις δεδομένων)

Σχέση **client – server** (πχ περιηγητής web με server που φιλοξενεί μια ιστοσελίδα)



Θέμα 2: Κύριες Εφαρμογές Ανοιχτού Κώδικα – Κοινή χρήση δεδομένων & διαχείριση δικτύου

Κοινή χρήση δεδομένων σε τοπικά δίκτυα:

- **NFS** (Network File System) – πρωτόκολλο για κοινή χρήση αρχείων σε συστήματα Linux, μεταξύ client PC και server.
- **Samba** – πρωτόκολλο για κοινή χρήση αρχείων συμβατό για όλα τα Λ/Σ.
- **OwnCloud / Nextcloud** – ολοκληρωμένη λύση cloud, για κοινή χρήση αρχείων, συγχρονισμού, ημερολόγια, επαφές κτλ, μέσω web.

Διαχείριση δικτύου:

DHCP (Dynamic Host Configuration Protocol) – αυτόματη παροχή IP σε αιτούσα συσκευή, από τον server του παρόχου Internet (ISP).

DNS (Domain Name System) – μετάφραση του domain name (πχ greeklug.gr) στη διεύθυνση IP

Και τα 2 παρέχονται από τον πάροχο Internet, μέσω του router.



Θέμα 2: Κύριες Εφαρμογές Ανοιχτού Κώδικα – Γλώσσες προγραμματισμού

Μεταγλωττισμένες (compiled) γλώσσες: ο **πηγαίος κώδικας** μετατρέπεται σε διαδικό (binary) αρχείο το οποίο εκτελείται από τον Η/Υ. **Γρήγορη εκτέλεση, αλλά αργή ανάπτυξη.**

Interpreted (Scripted) γλώσσες: ένας **διερμηνέας (interpreter)** διαβάζει τον πηγαίο κώδικα και εκτελεί τις οδηγίες του. **Γρήγορη ανάπτυξη, αλλά πιο αργή εκτέλεση.**

JavaScript - interpreted γλώσσα για δημιουργία εφαρμογών στο web & κινητές συσκευές.

C - compiled γλώσσα για ανάπτυξη Λ/Σ, ενσωματωμένα συστήματα, κτλ.

C++ - επέκταση της C, χρήση σε ανάπτυξη παιχνιδιών, browsers, εφαρμογές κτλ.

Java – compiled & interpreted, χρήση σε ανάπτυξη εφαρμογών android και backend.

Python – πολύ δημοφιλής interpreted γλώσσα για πολλές χρήσεις.

PHP - scripting γλώσσα σε server για τη δημιουργία περιεχομένου στο web.

Rust – compiled γλώσσα για ανάπτυξη Λ/Σ, Cloud & υποδομές κτλ.



Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Ορισμός ελεύθερου λογισμικού

4 κριτήρια που πρέπει να πληροί ένα λογισμικό για να θεωρείται **ελεύθερο**:

- 1) Η ελευθερία να **εκτελείτε το πρόγραμμα** όπως επιθυμείτε, **για οποιονδήποτε σκοπό** (freedom 0).
- 2) Η ελευθερία να **μελετάτε πώς λειτουργεί το πρόγραμμα** και να το **αλλάζετε όπως επιθυμείτε** (freedom 1).
- 3) Η ελευθερία να **αναδιανέμετε αντίγραφα** ώστε να μπορείτε να βοηθήσετε άλλους (freedom 2).
- 4) Η ελευθερία να **αναδιανέμετε αντίγραφα των τροποποιημένων εκδόσεών** σας σε άλλους (freedom 3).



Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Ανοιχτό vs ελεύθερο λογισμικό

Για πολλούς, ελεύθερο λογισμικό = ανοιχτό λογισμικό
FOSS (Free & Open Source Software)

Ελεύθερο – σχετίζεται με τον Richard Stallman και το έργο GNU. Προάγει το δικαίωμα στην ελευθερία και τη συνεργασία.

Ανοιχτό – ορίζεται από το OSI (Open Source Initiative). Πιο πρακτική/τεχνολογική προσέγγιση, νοιάζεται περισσότερο για την ποιότητα του κώδικα μέσα από την διαφάνεια.





Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Άδειες FSF

Άδεια λογισμικού: Σαφής ορισμός **όρων/δικαιωμάτων χρήσης** ενός ψηφιακού προϊόντος, όταν μεταβιβάζεται από μια εταιρία/άτομο σε τρίτους.

Άδειες Copyleft

- GNU General Public License (**GPL**) – δημιουργία από το FSF. Οποιοδήποτε παράγωγο έργο πρέπει επίσης να διανεμηθεί υπό την ίδια ακριβώς άδεια GPL.
- GNU Lesser General Public License (**LGPL**) – προσαρμογή της GPL, όπου επιτρέπεται η σύνδεση κλειστού προγράμματος με ανοιχτό λογισμικό, χωρίς να απαιτείται να δοθεί ο πηγαίος κώδικας του κλειστού προγράμματος (πχ σύνδεση προγράμματος με ανοικτές βιβλιοθήκες)
- GNU Affero General Public License (**AGPL**) – η ελεύθερη διάθεση του κώδικα εφαρμογών/υπηρεσιών που τρέχουν μέσω διαδικτύου (cloud).
- GNU Free Documentation License (**FDL**) – προορίζεται για κείμενα (πχ Wikipedia). Δίνει το δικαίωμα σε όλους να αντιγράψουν, να αναδιανείμουν και να τροποποιήσουν ένα κείμενο, με την προϋπόθεση ότι οι νέες εκδόσεις θα είναι επίσης ελεύθερες.



Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Permissive Άδειες

Οι **permissive** (επιτρεπτικές) άδειες επιβάλλουν **ελάχιστους περιορισμούς** στους χρήστες του κώδικα.

Berkeley Software Distribution (BSD)

Κύρια διαφορά με τις GPL, είναι ότι ο τροποποιημένος κώδικας ενός project με άδεια BSD, μπορεί να κυκλοφορήσει ως **ιδιοταγής/κλειστός**.

2-Clause BSD (FreeBSD)

Απαιτεί από τον χρήστη δύο βασικές προϋποθέσεις αν αναδιανείμει τον κώδικα:

- **Διατήρηση** της Σημείωσης Πνευματικών Δικαιωμάτων
- Συμπερίληψη των δικαιωμάτων σε περίπτωση που το λογισμικό διανεμηθεί σε **Δυαδική Μορφή**



Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Άδειες Creative Commons I

Open source σε μη τεχνικούς τομείς - **πνευματικά έργα**. Πχ επιστημονικό έργο/κείμενο που να μπορεί να διαμοιραστεί και να υποβληθεί σε επεξεργασία. Ανάγκη για δημιουργία νέων αδειών (εκτός των GPL, Permissive κτλ) ώστε να εξυπηρετούν τους σκοπούς των πνευματικών έργων.

Πρωτοβουλία Creative Commons (CC):

Παγκόσμιος μη κερδοσκοπικός οργανισμός που επιτρέπει την ανταλλαγή και την επαναχρησιμοποίηση της δημιουργικότητας και της γνώσης, μέσω της παροχής δωρεάν νομικών εργαλείων.

Ο **δημιουργός ενός έργου**, δεν παραχωρεί τα δικαιώματα στον εκδότη, αλλά **αποφασίζει αυτός** πώς θα χρησιμοποιηθεί το έργο από τρίτους, επιλέγοντας μέσα από ένα σύνολο χαρακτηριστικών/ιδιοτήτων.





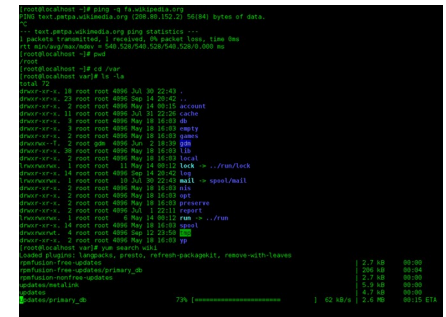
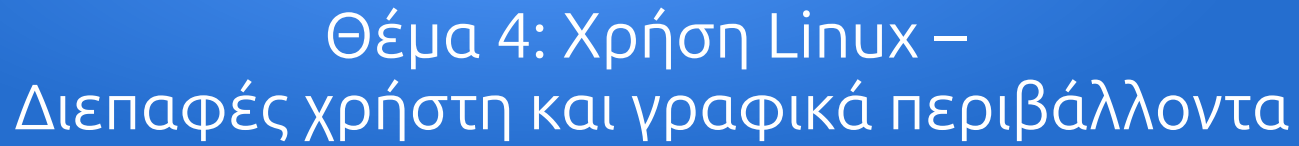
Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Άδειες Creative Commons II

Ιδιότητες / Άδειες	Επεξήγηση
CC BY (Attribution)	Επιτρέπει σε οποιονδήποτε να επεξεργαστεί και να διανείμει το έργο αρκεί να κατονομάσει τον δημιουργό.
CC BY-SA (Attribution-ShareAlike)	Όπως η CC BY + το τροποποιημένο έργο μπορεί να διανεμηθεί μόνο με την ίδια άδεια.
CC BY-ND (Attribution-NoDerivatives)	Όπως η CC BY + το έργο μπορεί να μεταβιβαστεί μόνο ατροποποίητο.
CC BY-NC (Attribution-NonCommercial)	Όπως η CC BY + το έργο μπορεί να αναδιανεμηθεί μόνο υπό μη εμπορικούς όρους.
CC BY-NC-SA (Attribution-NonCommercial-ShareAlike)	Όπως η CC BY-NC + το έργο μπορεί να μοιραστεί μόνο υπό τους ίδιους όρους.
CC BY-NC-ND (Attribution-NonCommercial-NoDerivatives)	Η διανομή επιτρέπεται με αναφορά στον δημιουργό, αλλά μόνο αμετάβλητη και υπό μη εμπορικούς όρους.



Θέμα 3: Ανοιχτό Λογισμικό & Άδειες – Επιχειρηματικά Μοντέλα στο Open Source

- * **Crowdfunding** – συλλογή δωρεών με αντάλλαγμα ειδικά χαρακτηριστικά του προϊόντος.
- * **Διπλή άδεια** – παροχή προγράμματος με 2 άδειες, μια ελεύθερη και μια που παρέχει περισσότερα χαρακτηριστικά σε όσους τα πληρώσουν.
- * **Παροχή επαγγελματικών υπηρεσιών** – υποστήριξη, consulting κτλ
- * Πώληση **πιστοποιητικών χρήσης του προγράμματος** προς τεκμηρίωση της γνώσης σε πελάτες.
- * **SaaS** (Software as a Service) πώληση πόρων για χρήση του προγράμματος.
- * Πώληση **επεκτάσεων** προγράμματος κατά παραγγελία.





Θέμα 4: Χρήση Linux – Βιομηχανικές χρήσεις του Linux

- * - **IaaS** (Infrastructure as a Service): Οι χρήστες νοικιάζουν πόρους ενός server (συνήθως ένα λειτουργικό σύστημα που τρέχει σε ένα VM, μέσω ενός hypervisor). Υπάρχουν 3 κύριοι hypervisors: Xen, KVM και VirtualBox. Η διαχείριση του Λ/Σ εναπόκειται στον χρήστη.
- * - Το **OpenStack** είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα για την κατασκευή και διαχείριση πλατφορμών cloud computing προκειμένου. Πλήρες IaaS cloud περιβάλλον on-premise (πχ CERN).
- * - **PaaS** (managed server) - Platform as a Service: Οι χρήστες έχουν πρόσβαση σε μια πλατφόρμα, προκειμένου να αναπτύξουν και να εκτελέσουν την εφαρμογή τους, χωρίς το βάρος της διαχείρισης του server. Παράδειγμα είναι τα Heroku, Red Hat Openshift, κτλ.
- * - **SaaS** (Software as a Service): Πληρωμή συνδρομής για τη χρήση ενός λογισμικού.



Θέμα 4: Χρήση Linux – Ζητήματα Απορρήτου στο Διαδίκτυο

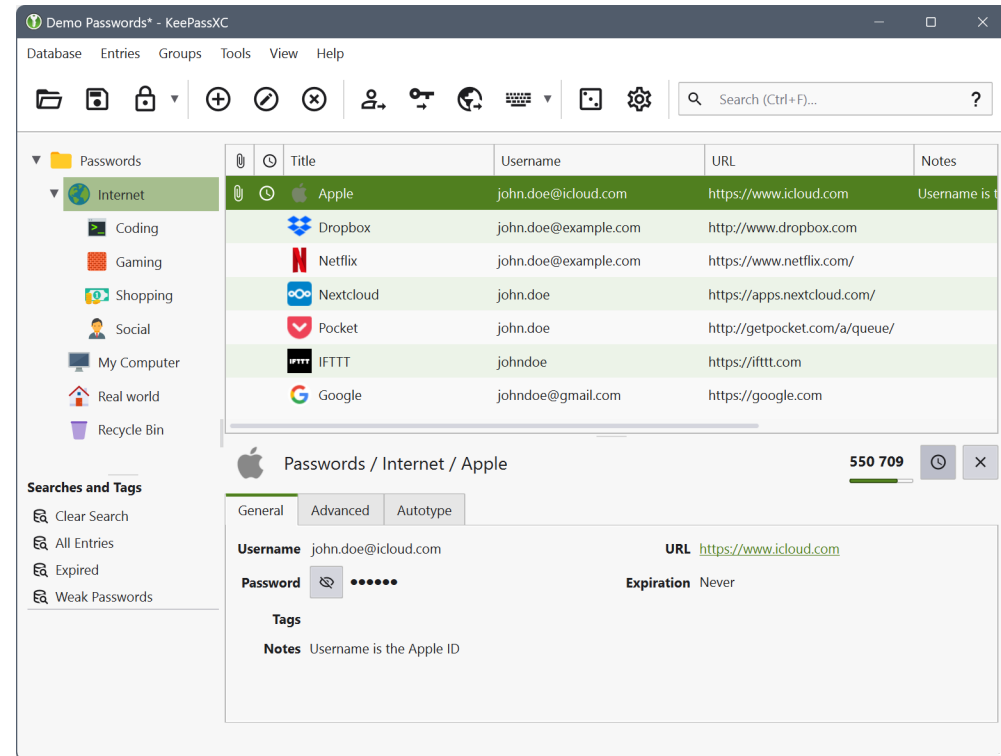
Σχεδόν όλες οι ενέργειες που γίνονται μέσω ενός browser παρακολουθούνται και αναλύονται από διάφορα μέρη.

- * **Cookie Tracking:** Τα cookies είναι μικρά αρχεία που μπορεί να αποθηκεύσει ένας ιστότοπος στον υπολογιστή μας προκειμένου να αποθηκεύσει και να ανακτήσει κάποιο είδος πληροφορίας που μπορεί να είναι χρήσιμη για την πλοήγησή μας.
- * **Do Not Track (DNT):** Είναι ακρωνύμιο για το "Do Not Track" και μπορεί να ενεργοποιηθεί σε οποιονδήποτε σύγχρονο browser. Αλλά, στην πραγματικότητα, οι ίδιοι οι ιστότοποι είναι αυτοί που θα αποφασίσουν αν θα σεβαστούν την επιλογή μας ή όχι.
- * **"Private" Windows:** Ανώνυμα παράθυρα, αποφεύγουν το cookie tracking και δεν αφήνουν ίχνη στον υπολογιστή που χρησιμοποιούμε.



Θέμα 4: Χρήση Linux – Διαχείριση κωδικών πρόσβασης

- * Χρήση **μη προβλέψιμων & σύνθετων** κωδικών
- * Χρήση **διαφορετικών κωδικών** για κάθε λογαριασμό/υπηρεσία
- * Χρήση πολλαπλής ταυτοποίησης (**MFA**)
- * Χρήση διαχειριστών κωδικών (**password managers**), όπως keepassxc, bitwarden
- * Δημιουργία τυχαίων κωδικών, αποθήκευση σε κρυπτογραφημένη βάση, δυνατότητα εύρεσης λογαριασμών που έχουν διαρρεύσει τα στοιχεία τους.

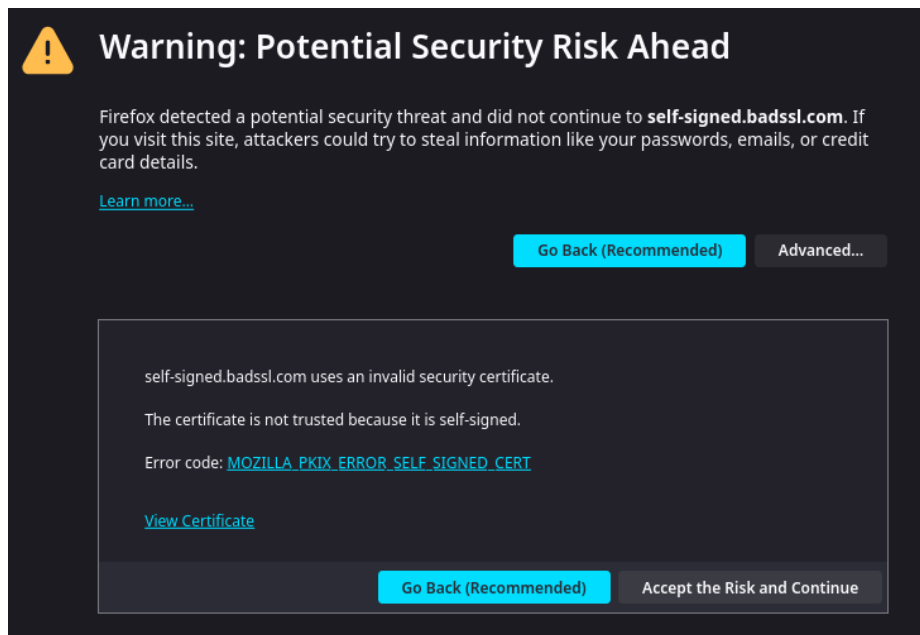




Θέμα 4: Χρήση Linux – Κρυπτογράφηση TLS

Τρίτα μέρη μπορούν να έχουν πρόσβαση κατά τη μεταφορά δεδομένων στο διαδίκτυο. Είναι επιβεβλημένη η κρυπτογράφηση των πληροφοριών και των συνδέσεων, προτού φύγουν από μια συσκευή.

TLS (Transport Layer Security) – πρωτόκολλο που προσφέρει ασφάλεια συνδέσεων. Χρησιμοποιείται στο πρωτόκολλο HTTPS (HTTP μέσω TLS), ώστε να καταστεί δυνατή η αποστολή ευαίσθητων δεδομένων (πχ στοιχεία πιστωτικών καρτών).





Θέμα 4: Χρήση Linux – Κρυπτογράφηση με GnuPG

GnuPG (GNU Privacy Guard) είναι open source υλοποίηση του προτύπου OpenPGP. Χρησιμοποιείται για την υπογραφή, κρυπτογράφηση και αποκρυπτογράφηση κειμένων, μηνυμάτων ηλεκτρονικού ταχυδρομείου, αρχείων, καταλόγων & δίσκων.

Λειτουργεί με **κρυπτογραφία δημόσιου κλειδιού**. Δημιουργεί ένα ζευγάρι κλειδιών (δημόσιο και ιδιωτικό), όπου παρέχουμε το δημόσιο κλειδί μας σε τρίτους και κρατάμε σε ασφαλή τοποθεσία το ιδιωτικό.

Χρησιμοποιούμε το ιδιωτικό κλειδί μας για υπογραφή μηνυμάτων email (ψηφιακή υπογραφή) και ο παραλήπτης επαληθεύει την υπογραφή με το δημόσιο κλειδί μας.

Για **διατερματική κρυπτογράφηση** κατά την αποστολή email, χρησιμοποιούμε το δημόσιο κλειδί του παραλήπτη, για να “κλειδώσουμε” το μήνυμα. Έτσι κανείς, πέρα από τον αποστολέα και τον παραλήπτη, δεν μπορεί να διαβάσει το μήνυμα.



Θέμα 4: Χρήση Linux – Κρυπτογράφηση δίσκου

Stacked encryption: Τα αρχεία και οι κατάλογοι κρυπτογραφούνται πριν αποθηκευτούν στο σύστημα αρχείων και αποκρυπτογραφούνται μετά την ανάγνωσή τους. Τρίτα άτομα δεν μπορούν να δουν τα περιεχόμενα (βλέπουν απλά τυχαία δεδομένα), αλλά μπορούν να δουν ότι πρόκειται για αρχεία. Το **EncFS** δεν απαιτεί root δικαιώματα για την υλοποίηση και μπορεί να λειτουργήσει σε υπάρχον σύστημα αρχείων χωρίς τροποποιήσεις.

Block device encryption: Τα αρχεία κρυπτογραφούνται πριν εγγραφούν στον δίσκο. Ότι εγγράφεται σε μια block συσκευή κρυπτογραφείται. Τρίτα άτομα δεν μπορούν καν να δουν το σύστημα αρχείων, ούτε αν υπάρχουν αρχεία, κατάλογοι κ.λπ., επειδή τα metadata, η δομή του καταλόγου και τα permissions είναι επίσης κρυπτογραφημένα.

- Το **dm-crypt** είναι ένα πρότυπο για block device κρυπτογράφηση, που χρησιμοποιείται με το **LUKS** (Linux Unified Key Setup).

- Το **VeraCrypt** είναι πρόγραμμα cross-platform (Win, Linux, macOS), που επιτρέπει την κρυπτογράφηση αρχείων.



Το αρχείο της παρουσίασης από την Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ
(GreeklUG) διέπεται από την άδεια

Creative Commons Αναφορά Δημιουργού - Μη Εμπορική Χρήση -
Παρόμοια Διανομή 4.0 Διεθνές (CC BY-NC-SA 4.0)

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.el>



Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ | GreeklUG
<https://www.greeklug.gr/>