Freedom of Speech

Ασφάλεια επικοινωνιών σε ασύρματα δίκτυα
Wireless Hotspots
VPNs

Freedom of Speech

Ποιός ;
&
Γιατί ;

Ασφάλεια ασύρματων δικτύων

Ιστορικά

Φάσμα

Τύποι κρυπτογράφησης

Ανοιχτά δίκτυα

VPN

Ιστορικά

Ασύρματα δίκτυα → προτόκολλο 802.11 (1997)

Αρχές '90: WaveLAN

1999: 802.11a (5/3.7GHz)

1999: Wi-Fi Alliance → **Wi-Fi** (**802.11b** 2.4GHz)

2003: **802.11g** (2.4GHz)

2009: **802.11n** (2.4/5 Ghz)

Φάσμα

ISM Bands

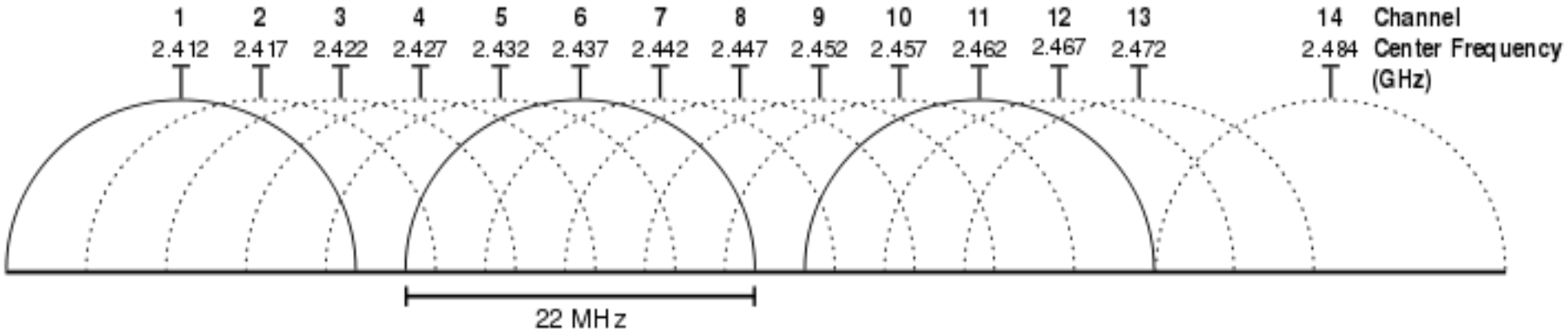
- Industrial, Scientific, Medical
- Ανοχή σε παραμβολές – χρήση χωρίς άδεια
- Ελεύθερες για χρήση σε όλο το κόσμο*
- Πιο διαδεδομένες για data:
  - 2.400 – 2500 MHz
  - 5.725 – 5.875 MHz

*κάθε χώρα θέτει τους δικούς της περιορισμούς

Φάσμα

2.4GHz: Ελεύθερη ζώνη εκπομπής με 11/13(ή 14) επικαλυπτόμενα κανάλια

- Μικρή απορρόφηση από εμπόδια
- Μεγάλη χρήση – Μεγάλες παρεμβολές
- Χρησιμοποιείται ακόμα από: φούρνους μικροκυμάτων, bluetooth, baby radios, ασύρματα τηλέφωνα



Φάσμα

5GHz: Ελεύθερη σε κάποια μέρη του κόσμου με (συνήθως) 23 μη-επικαλυπτόμενα κανάλια

- Κάποιο κομμάτι του φάσματος απαιτεί άδεια
- Όχι κατάλληλο για εσωτερικούς χώρους
- Μεγαλύτερες ταχύτητες σε σχέση με τα 2.4GHz

Το πρόβλημα

- Για να συνδεθεί κανείς σε ένα εταιρικό (καλωδιακό) δίκτυο χρειάζεται να μπει φυσικά στον χώρο και να συνδεθεί σε μία πρίζα. Για να προστατευτεί το δίκτυο μπορούν να εφαρμοστούν ισχυροί ελέγχοι φυσικής προστασίας/εισόδου.

- Σε ένα ασύρματο δίκτυο δεν χρειάζεται να μπει κανείς στο κτίριο για να συνδεθεί. Πρέπει να βρεθεί τρόπος να διαπιστώνεται διαφορετικά ποιος μπορεί να χρησιμοποιήσει το δίκτυο.

Άλλοι τύποι προβλημάτων

- Κατά λάθος σύνδεση σε δίκτυο τρίτου
- Κακόβουλη σύνδεση σε δίκτυο τρίτου
- Επιθέσεις Man-in-the-middle
- Ad-Hoc δίκτυα (+ Windows = ♥)
- DoS σε Access Point

Η μη-λύση

~~MAC address filtering~~

Η λύση

Κρυπτογράφηση των ασύρματων συνδέσεων/ επικοινωνιών.

Τύποι κρυπτογράφησης

WEP (Wired Equivalent Privacy)

- Κομμάτι του αρχικού 802.11 πρωτοκόλλου (1999)
- Θεωρείται καταργημένο από το 2005
- Αλγόριθμος: **RC4** → **πολύ** αδύναμο
  I. IV + key → keystream
  II.keystream ⊕ plaintext (XOR)
- WEP-40: 10 hex chars→10 x 2^4 = 40bit + 24bit IV = 64bit key length
- WEP-104: 26 hex chars→10 x 16=104bit + 24bit IV = 128bit key length
- (Σπάνια) WEP-232: 56 hex chars...
- **ΜΗΝ ΤΟ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ!!!**

Τύποι κρυπτογράφησης

WEP (Wired Equivalent Privacy)

- 2 τρόποι αυθεντικοποίησης:
  - **Open System**: δεν υπάρχει αυθεντικοποίηση κατά το association. Όποιος ξέρει το κλειδί κρυπτογραφεί πακέτα και στέλνει προς το Access Point.
  - **Shared Key**: Ο client στέλνει αίτημα αυθεντικοποίησης, το AP απαντάει με ένα clear-text challenge, ο client το κωδικοποιεί με το WEP key και το στέλνει πίσω και αν είναι το σωστό, το AP τον πιστοποιεί.
- Ο ασφαλέστερος είναι το Open System (!!)
  - 24bit IV → πιθανότητα > 50% το ίδιο IV μετά από ~5000 πακέτα
  - Encrypt 2 plaintext με το ίδιο IV + key → εξαγωγή πληροφορίας για το XOR των 2 plaintext. Όταν ξέρεις το ένα plaintext όμως (ARP request) μαθαίνεις και το άλλο...

Τύποι κρυπτογράφησης

WPA (Wi-Fi Protected Access)

- WPA (1999)
  - Διάδοχος του WEP
  - Υποστηρίζει υποσύνολο του IEEE 802.11i
  - Αλγόριθμος: RC4 (ώστε να τρέχει σε hardware που έτρεχε WEP)
  - Εφαρμόζει **TKIP** (Temporal Key Integrity Protocol)
    I. Mixing του κλειδιού και του IV (≠ WEP)
    II.Μετρητής ακολουθίας πακέτων (Sequence counter)
    III.64-bit Message Integrity check (vs CRC32 στο WEP)
  - TKIP → Κρυπτογράφηση κάθε πακέτου με νέο 128bit κλειδί
- Ασφαλέστερο από το WEP αλλά έχει αδύναμο αλγόριθμο.

Τύποι κρυπτογράφησης

WPA (Wi-Fi Protected Access)

- WPA2 (2004)
  - IEEE 802.11i-2004
  - Διάδοχος του WPA
  - Υποχρεωτικό από το 2006 και μετά για Wi-Fi certification
  - Αλγόριθμος: **AES** (CCMP) ή **TKIP**
  - Μήκος κλειδιού: 256bit
  - Inter Client Isolation
  - 2 τύποι λειτουργίας
    - WPA-PSK: Pre-Shared Key (Personal Mode)
    - WPA-Enterprise ή WPA-802.1X (+Radius Authentication Server)

- Το πιο ασφαλές αυτή τη στιγμή.

Τύποι κρυπτογράφησης

WPS (Wi-Fi Protected Setup)

- Μέθοδοι εύκολης προσθήκης συσκευής σε ασύρματο δικτυο
- 4 παραλλαγές λειτουργίας
  i. Δημιουργία ενός 4-ψήφιου PIN στην συσκευή και είσοδος του PIN στο Access Point (υποχρεωτικό)
  ii. Πάτημα ειδικού κουμπιού στο Access Point και στην συσκευή (μη-υποχρεωτικό)
  iii. NFC → RFID - πλησίασμα της συσκευής κοντά στο AP
  iv. USB Flash → είσοδος στο AP, κατέβασμα στοιχείων, πέρασμα στοιχείων στον client (έχει καταργηθεί)
- Βρέθηκε πως μπορεί να γίνει brute-force το PIN με το πολύ 11.000 προσπάθειες → **Απενεργοποιήστε το!**

Προεπιλεγμένοι κωδικοί

Το Access Point/Router στο σπίτι μου λέει πως έχει προεπιλέξει WPA2 και έχει και έτοιμο ένα κωδικό. Άρα είμαι ασφαλής...σωστά;

ΛΑΘΟΣ → Πάντα αλλαγή του προεπ. κωδικού

Οι κωδικοί παράγονται από κάποιο αλγόριθμο που συνήθως περιέχει την MAC Address ή/και το όνομα του SSID → Διαρροή αλγορίθμου → Διαρροή του κωδικού

- OTE Conn-X
- Speedtouch / Thompson
- κ.α.

Εργαλεία

Kismet → 802.11 layer2 wireless network detector, sniffer, and intrusion detection system

Aircrack-ng → WEP and WPA-PSK keys cracking program

Ο εύκολος τρόπος να παίξει κανείς μαζί τους:

- Aircrack-ng VM
- Backtrack VM

Ανοιχτά Δίκτυα

Δίκτυα χωρίς κρυπτογράφηση

- Συνήθως προσωπικά δίκτυα ή hotspots
- Μεγάλη υποστήριξη από κομμάτι του κλάδου της ασφάλειας δικτύων/υπολογιστών
- Μεταφέρουν την ασφάλεια από την περίμετρο του δικτύου στα ίδια τα μηχανήματα/ Εφαρμογή πολιτικών ασφαλείας στα μηχανήματα και όχι (μόνο) στο δίκτυο
- Ευελιξία
- Ευκολότερη χρήση / Διαμοιρασμός με τρίτους

Ανοιχτά Δίκτυα

Αν υπάρχει η δυνατότητα να έχετε 2 wireless δίκτυα (SSID)

- Κρατήστε 1 με encryption/authentication και 1 χωρίς για “επισκέπτες”

Αν μπορείτε να έχετε μόνο 1 wireless δίκτυο, αφήστε το ελεύθερο και κάντε τους γείτονές σας χαρούμενους ☺

- Μην γκρινιάζετε για το bandwidth, βρείτε λύσεις!

Ελληνικοί νόμοι αναφέρουν πως **δεν** αρκεί να βρεθεί η IP αλλά πρέπει να βρεθεί και το μηχάνημα που διέπραξε ένα αδίκημα. **Δεν μπορείτε να κατηγορηθείτε αν δεν έχετε διαπράξει κάποιο αδίκημα επειδή κάποιος χρησιμοποίησε το δίκτυο σας.**

“Hot”spots

Σύνδεση σε δίκτυο → **Όποιος** άλλος είναι συνδεδεμένος μπορεί να δει τα unencrypted connections

Unencrypted connections → γίνονται διαθέσιμα τα usernames/passwords/cookies (session hijacking) σε οποιονδήποτε είναι στο ίδιο δίκτυο

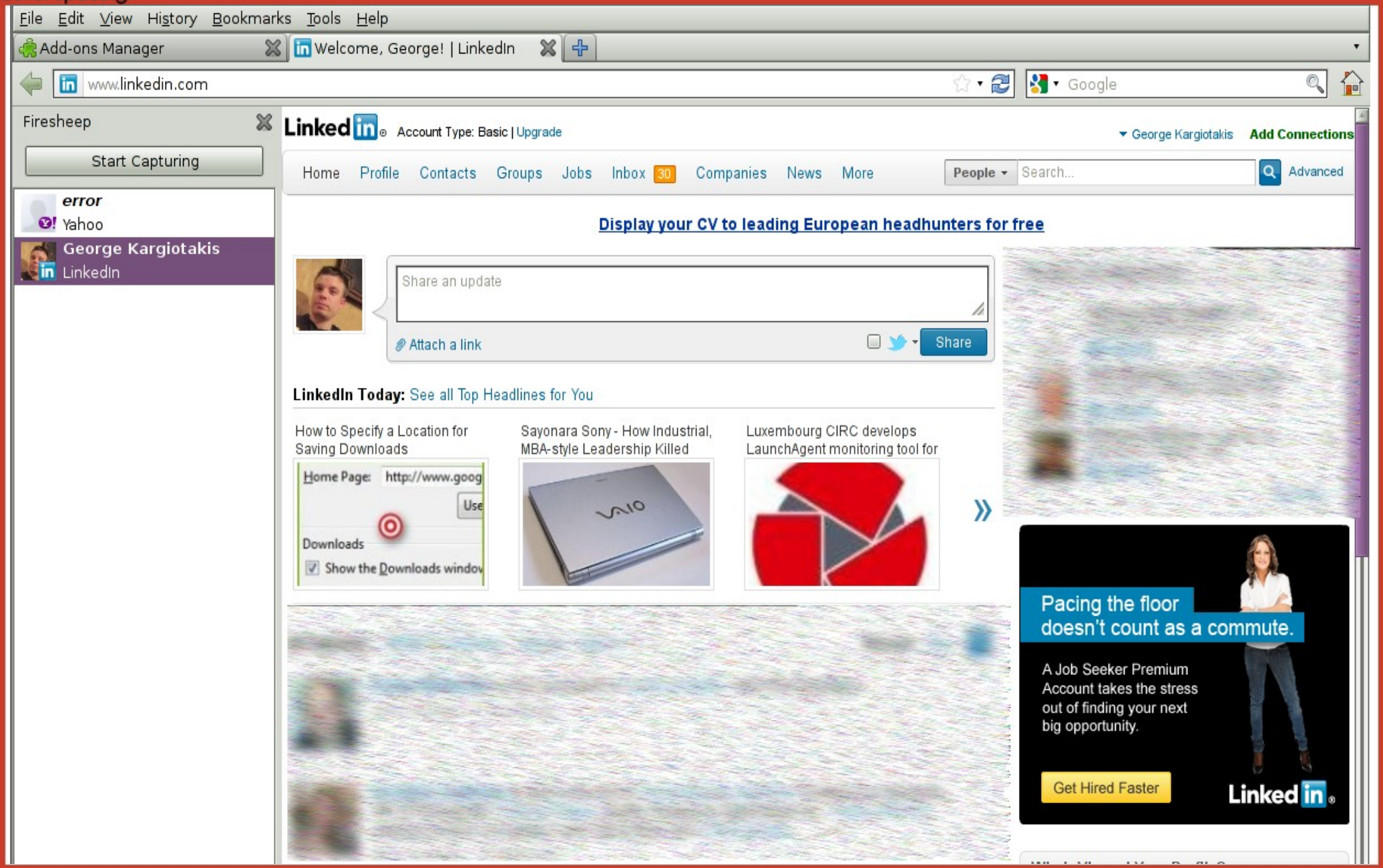
Άρα πάντα να γίνεται χρήση SSL/TLS σε HTTP/Email/IM/κτλ → Freedom of Speech #0

“Hot”spots

FireSheep

- Πρώτη έκδοση 24/10/2010
- Firefox Extension για Mac OS X / Windows / Linux
- HTTP Session Hijacking – Sidejacking
  - Κλέβει τα cookies άλλων χρηστών πάνω στο δίκτυο
  - Δίνει την δυνατότητα να χρησιμοποιήσει κάποιος τα cookies αυτά για είσοδο στα sites
- Τεράστια απήχηση
  - Πολύ εύκολο στην χρήση → Εκατομμύρια χρήστες έκλεβαν accounts σε hotspots την επόμενη μέρα
  - Ανάγκασε Facebook/Twitter/κτλ να υποστηρίξουν HTTPS ή ακόμα και να το κάνουν προεπιλογή
- DroidSheep - Αντίστοιχο εργαλείο sniffing για Android (έχει αποσυρθεί – ιδιαίτερη **προσοχή** αν πάει κάποιος να κατεβάσει έτοιμο apk από τυχαίο site)

“Hot”spots


File Edit View History Bookmarks Tools Help
Add-ons Manager
Welcome, George! | LinkedIn
www.linkedin.com
Google
Firesheep
Start Capturing
error
Yahoo
George Kargiotakis
LinkedIn
Account Type: Basic | Upgrade
George Kargiotakis
Add Connections
Home Profile Contacts Groups Jobs Inbox 30 Companies News More
People
Search...
Advanced
Display your CV to leading European headhunters for free
Share an update
Attach a link
Share
LinkedIn Today: See all Top Headlines for You
How to Specify a Location for Saving Downloads
Sayonara Sony - How Industrial, MBA-style Leadership Killed
Luxembourg CIRC develops LaunchAgent monitoring tool for
Home Page: http://www.goog
Downloads
Show the Downloads windov
Pacing the floor doesn't count as a commute.
A Job Seeker Premium Account takes the stress out of finding your next big opportunity.
Get Hired Faster
LinkedIn

“Hot”spots

Είναι επικίνδυνο να χρησιμοποιεί κανείς HotSpot για την ευαίσθητη επικοινωνία του.

Μην χρησιμοποείτε ελεύθερα HotSpots που δεν γνωρίζετε και εμπιστεύεστε όχι μόνο τον διαχειριστή τους αλλά και τους χρήστες του!

Αν νοιάζεστε για την ασφάλεια των δεδομένων σας μην χρησιμοποιείτε **ποτέ** ελεύθερα HotSpot

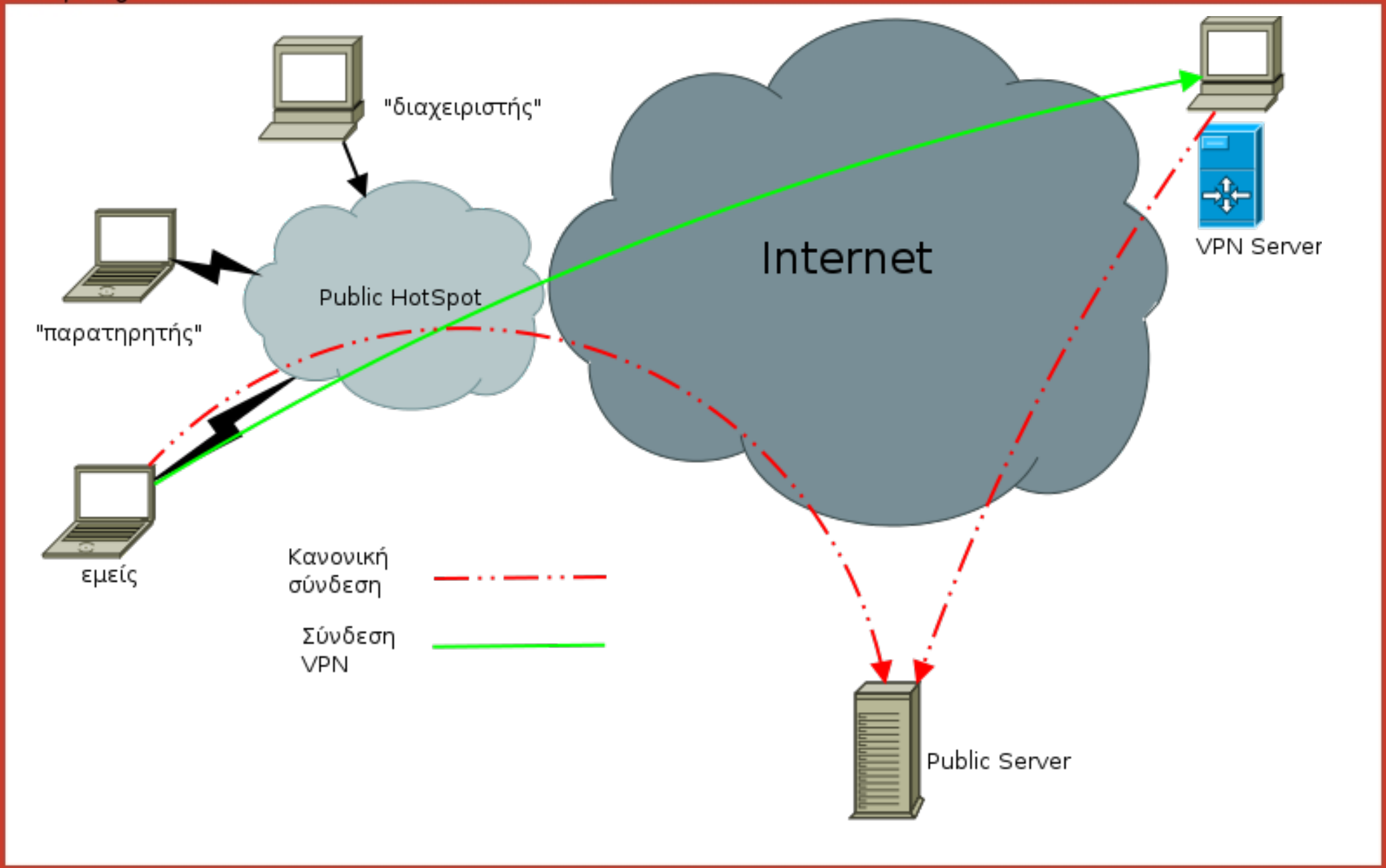
- Αεροδρομίων/Σταθμών/Καφέ
- Μην έχετε ανοιχτό το Wi-Fi συνέχεια στο κινητό!

VPN

VPN → Virtual Private Networking

- Ασφαλή δίκτυα που προσφέρουν
  - Αυθεντικοποίηση
  - Κρυπτογράφηση
- Δημιουργούν ένα “tunnel” από άκρο σε άκρο
- Συνδέουν απομακρυσμένους χρήστες στο δίκτυο κάποιας κεντρικής τοποθεσίας.
- Συνδέουν απομακρυσμένες τοποθεσίες μεταξύ τους σε ένα κοινό δίκτυο.

VPN


"διαχειριστής"
"παρατηρητής"
Public HotSpot
Internet
VPN Server
εμείς
Κανονική σύνδεση
Σύνδεση VPN
Public Server

VPN

Δημοφιλή VPN

- IPsec
- OpenVPN (Windows/Linux/OS X)
  - SSL/TLS VPN
  - Αυθεντικοποίηση με Certificates ή Static Key
- MPPE (Microsoft Point-to-Point Encryption)
- SSTP (Secure Socket Tunelling Protocol)
- SSH VPN

VPN

OpenVPN

- Δημιουργία certificates μέσω του easy-rsa ή static key
- Δημιουργία Server/Client Config
- Ρυθμίσεις Firewall
- Διαμοιρασμός σύνδεσης (connection sharing)

Γενικές οδηγίες

Οδηγίες για Server σε Windows

Οδηγίες για Server σε Linux (Ubuntu)

VPN

Ρυθμίσεις OpenVPN

Server Config	Client Config
dev tun port 1194 ca ca.crt cert server.crt key server.key dh dh1024.pem server 10.1.0.0 255.255.255.0 comp-lzo verb 3 push “redirect-gateway def1”	client dev tun remote my.VPNHOST.gr 1194 ca ca.crt key kargig.key cert kargig.crt comp-lzo verb 3

Ρυθμίσεις Server για NAT:

- sysctl -w net.ipv4.ip_forward=1
- iptables -t nat -A POSTROUTING -o eth0 -s 10.1.0.0/24 -j SNAT --to-source PUBLIC.IP.GOES.HERE

VPN

SSH VPN

- Server (sshd_config)
  - PermitRootLogin yes
  - PermitTunnel yes
- Client
  - (sudo) ssh -w 0:0 REMOTE.IP.GOES.HERE
  - Προσθήκη IPs (client + Server) στο tun interface
  - Προσθήκη routes (+ NAT)

Λεπτομερείς οδηγίες

VPN

Microsoft VPN

- Click click click
- Κλικ Κλικ Κλικ
- Δεν καταλαβαίνω τι λέει αλλά κάνω κλικ κλικ κλικ
- Κουράστηκα αλλά συνεχίζω να κάνω κλικ κλικ κλικ στα τυφλά

→ **Πόνος**

Όποιος τολμάει ας διαβάσει οδηγίες

ή αυτές τις οδηγίες

ή αυτό το “κείμενάκι” 32 σελίδων

VPN

SSH Socks/Port Forwarding

- Τρόπος 1
  - ssh -D 8999 username@REMOTE.IP
  - Browser: SOCKS Proxy → localhost:8999
  - Τα DNS requests φεύγουν μέσω της κύριας σύνδεσης (!!)
- Τρόπος 2
  - Τρέχουμε Privoxy στον server
  - ssh -L8118:localhost:8118 username@REMOTE.IP
  - Browser: HTTP Proxy → localhost:8118

VPN

Αγορά VPN account

- Gaming / Casino / Privacy / κ.α.
- Διαφορετικές τιμές αναλόγως την ταχύτητα / όγκο δεδομένων / χώρα / ταυτόχρονες συνδέσεις
- Προσοχή στα “Anonymity VPNs” (!!)
- Τιμές από 5-30$/μήνα

Γενικές Συμβουλές

- Κλείστε τα shared folders όταν φεύγετε από το δικό σας δίκτυο.
  - Ποτέ μα ποτέ ανοιχτά folders σε όλο το κόσμο! Πάντα με αυθεντικοποίηση!
- Εγκαταστείστε firewall που να επιτρέπει μόνο συγκεκριμένους υπολογιστές να συνδέονται στους δικτυακούς πόρους του υπολογιστή σας.
- Απενεργοποιήστε τα Ad-Hoc δίκτυα (Windows)
- Απενεργοποιήστε την αυτόματη σύνδεση σε δίκτυα
- Κλείστε την Wi-Fi κάρτα αν δεν σκοπεύετε να είστε συνδεδεμένοι με κάποιο δίκτυο (σώζετε και μπαταρία → go green!)

DNS Tunnel

Τι κάνει κάποιος όταν βρίσκεται σε επί-πληρωμή HotSpot και...δεν έχει να πληρώσει ?

- DNS Tunnel → encapsulate IP μέσα από DNS queries
- Απαιτούμενα
  - 1 domain (πχ mytn.gr) → όσο μικρότερο τόσο καλύτερα
  - DNS Server σε κάποιο μηχάνημα/VM που θα τρέχει και το dns-tunnel server (iodined)
  - Ο client στο μηχάνημα μας (iodine)
  - Ρυθμίσεις Firewall,Routing,NAT,κτλ
- Συνδυάζεται με τα υπόλοιπα VPNs (double tunneling)
- Περισσότερα: iodine

Freedom of Speech

Βιβλία

Τεχνικά:

- *Real 802.11 Security: Wi-Fi Protected Access and 802.11i* (Jon Edney, William A. Arbaugh)
- *BackTrack 5 Wireless Penetration Testing Beginner's Guide* (Vivek Ramachandran)
- OpenVPN 2 Cookbook (Jan Just Keijser)

Freedom of Speech

Ευχαριστίες

- **Όσοι έστειλαν ιδέες**
- **Όσοι επικοινώνησαν μαζί μου για να βοήθησουν :)**

- **EFF**

Freedom of Speech

Sites to visit

- **hackerspace.gr**
- **dln.gr**

Freedom of Speech

Διαγωνισμός

1. Σηκώστε ένα OpenVPN server
2. Δημιουργήστε certificates
3. Δημιουργήστε server config που να δίνει default gw
4. Δημιουργήστε client config αρχεία
5. Στείλτε (μόνο) τα (απαραίτητα) αρχεία στο kargig [at] void [dot] gr
   - Προφανώς κρυπτογραφημένα με GPG ☺
6. Αν δουλέψει, κάντε revoke το certificate ώστε να μην μπορεί να ξαναμπεί ο client

Ο πρώτος που θα κάνει όλα τα βήματα κερδίζει ένα T-Shirt του EFF

Freedom of Speech

Ερωτήσεις / Συζήτηση