

ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ


Π. Αγγελάτος, Δ. Ζήνδρος



Στόχος της ώρας

- Εμβάθυνση σε προηγούμενες έννοιες
- Σφαιρική παρουσίαση εννοιών
- Έννοιες στη φυσική ασφάλεια
- Κρυπτογράφηση δίσκου (LUKS, TrueCrypt, FileVault)
- Plausible deniability
- Περισσότερα για app sec
- Bitcoin πορτοφόλια
- Bitcoin στην πράξη
- Hidden tor services

Όσο ξεκινάμε...

- Κατεβάστε το TrueCrypt για το σύστημά σας:
 - <http://www.truecrypt.org/>
 - Επιβεβαιώστε την υπογραφή GPG στο εκτελέσιμο
 - `gpg --verify TrueCrypt.dmg.sig TrueCrypt.dmg`
 - Εγκαταστήστε το
- 
- υπογραφή αρχείο

Κύκλος ζωής ασφάλειας

#1 Πρόληψη / Αποφυγή:

- Αποφεύγουμε προβλήματα ασφάλειας **πριν** γίνουν
- π.χ. Input validation, escaping
- Κλειδώνουμε το laptop μας
- Κρυπτογραφούμε κωδικούς πριν τους στείλουμε με e-mail
- HTTPS
- Υπογράφουμε ψηφιακά διευθύνσεις bitcoin
- Χρησιμοποιούμε OTR για ασφαλές chat
- Χρησιμοποιούμε Tor όταν θέλουμε να είμαστε ανώνυμοι
- Κλειδώνουμε τα WiFi μας με WPA2

Κύκλος ζωής ασφάλειας

#2 Εντοπισμός:

- Εντοπίζουμε παραβιάσεις ασφάλειας **όταν** γίνονται
- `gpg --verify` σε εκτελέσιμα και υπογραφές
- HTTPS “Invalid certificate”
- HSTS “Cannot connect to the real google.com”
- Βρίσκουμε πού βρίσκεται το πρόβλημα



Cannot connect to the real encrypted.google.com

Something is currently interfering with your secure connection to encrypted.google.com.

Try to reload this page in a few minutes or after switching to a new network. If you have recently connected to a new Wi-Fi network, finish logging in before reloading.

If you were to visit encrypted.google.com right now, you might share private information with an attacker. To protect your privacy, Chrome will not load the page until it can establish a secure connection to the real encrypted.google.com.

[More](#)[Reload](#)

Κύκλος ζωής ασφάλειας

#3 Χειρισμός:

- Χειριζόμαστε παραβιάσεις ασφάλειας **αφού** γίνουν
- Είμαστε ειλικρινείς με τους χρήστες μας
- Ενημερώνουμε τους συνεργάτες μας
- Αλλάζουμε κωδικούς πρόσβασης
- Ελέγχουμε συστήματα που έχουν παραβιαστεί
- “Post-mortem”
- Βάζουμε τα πράγματά μας σε ένα κουτί

Λίγα ακόμα για Application Security

Security through obscurity

- Πολλά συστήματα στηρίζουν την ασφάλειά τους σε μυστικότητα της υλοποίησης
- **Αυτό είναι λάθος!**
- Δεν πρέπει η ασφάλειά μας να στηρίζεται στο ότι ο εχθρός δεν ξέρει τον κώδικα
- Είναι πολύ εύκολο να διαρρεύσει ο κώδικας
 - π.χ. από έναν πρώην υπάλληλο

Kerckhoffs's principle

- Η ασφάλεια ενός κρυπτογραφικού συστήματος πρέπει να στηρίζεται αποκλειστικά στη μυστικότητα του κλειδιού
- Ο εχθρός γνωρίζει...
 - τον αλγόριθμο
 - το σύστημα
 - τον κώδικα
 - τις ρυθμίσεις μας
- Ο εχθρός δεν γνωρίζει...
 - το κλειδί μας
 - τους κωδικούς μας

Kerckhoffs's principle

- Το κλειδί αλλάζει εύκολα σε περίπτωση παραβίασης
- Ο κώδικας όμως όχι

Ανάπτυξη ασφαλών συστημάτων

- Η ασφάλεια είναι ένα Δύσκολο Πρόβλημα™
- Μέθοδος ανάπτυξης τυπικού λογισμικού:
 - Γράφω τον κώδικα
 - Τρέχω τον κώδικα
 - Επιβεβαιώνω ότι δουλεύει
- Τυπική μέθοδος ανάπτυξης «ασφαλούς» συστήματος:
 - Γράφουμε τον κώδικα
 - ...ελπίζουμε ότι είναι ασφαλής
- Είναι ισοδύναμο με το να δημοσιεύουμε ένα πρόγραμμα σε C++ που απλά κάνει compile χωρίς να το τρέξουμε!
- **Αυτό δεν είναι αρκετό**

Ανάπτυξη ασφαλών συστημάτων

- Η ασφάλεια προκύπτει από:
 - Peer reviews - Βάζουμε συναδέλφους να διαβάσουν τον κώδικά μας
 - Απλότητα - Τα κομμάτια κώδικα που αφορούν ασφάλεια πρέπει να είναι σύντομα και απλά
 - Ιδανικά πρέπει να υπάρχει **μία λειτουργική μονάδα** που χειρίζεται την ασφάλεια, και όχι διασκορπισμένος κώδικας

Ανοιχτός κώδικας

- Είναι πιο εύκολο να γίνει peer review
- Τον βλέπουν περισσότερα μάτια
- Μια εφαρμογή δεν αρκεί να είναι ανοιχτού κώδικα για να είναι ασφαλής!
- Πρέπει συνειδητά να αναζητούμε reviews τόσο σε κλειστού κώδικα όσο και σε ανοιχτού κώδικα εφαρμογές

Don't roll your own crypto

- Αν πρέπει να θυμάστε ένα πράγμα από αυτό το σεμινάριο
- Don't roll your own crypto
- Μην υλοποιείτε τους δικούς σας αλγορίθμους!
- Την τελευταία φορά που κάποιος το έκανε
- ...έφτιαξε το WEP
- Δεν είστε ούτε είμαστε ικανοί να σχεδιάσουμε κρυπτογραφικά συστήματα!
- Οι άνθρωποι που σχεδιάζουν κρυπτογραφία αφιερώνουν τη ζωή τους σε αυτό
- Υπάρχουν πάρα πολλά πράγματα που μπορούν να πάνε στραβά

Don't roll your own crypto

- Μην **υλοποιείτε** αλγόριθμους που υπάρχουν ήδη!
 - Χρησιμοποιείτε έτοιμες υλοποιήσεις
 - Μπορείτε να υλοποιήστε για εκπαιδευτικούς σκοπούς
 - Υποσχεθείτε μας ότι δεν θα τα χρησιμοποιήσετε σε production
- Αν είναι εφικτό, μην **καλείτε** καν απευθείας κρυπτογραφικές βιβλιοθήκες!
 - Εκτός από hash functions
 - Αν γράφετε τη λέξη “AES” στον κώδικά σας, μάλλον κάνετε λάθος!
 - Χρησιμοποιήστε έτοιμα συστήματα, π.χ. HTTPS μέσω Apache

Security in depth

- Φροντίζουμε οι συνέπειες παραβίασης ασφάλειας να μην είναι μοιραίες
- Έχουμε πολλά επίπεδα προστασίας
- Password hashing
 - Τι γίνεται αν κλαπεί ένας κωδικός;
 - Θα είναι hashed - δεν είναι καταστροφικές οι συνέπειες
- Principle of least privilege
 - Τι γίνεται αν κάποιος αποκτήσει πρόσβαση σε λογαριασμό μας;
 - Δεν θέλουμε να έχει πρόσβαση παντού

Password hashing

- Στις web εφαρμογές μας, δεν αποθηκεύουμε ποτέ password σε καθαρό κείμενο!
- Χρησιμοποιούμε κάποιο hash function
 - Όχι MD5 - δεν είναι collision resistant
 - SHA-256 ή SHA-512
 - bcrypt
 - PBKDF2
- Προσθέτουμε τυχαίο salt στους κωδικούς χρηστών

```
function hash_password( $password ) {  
    $salt = openssl_random_pseudo_bytes( 32 );  
  
    return [  
        "hash" => hash( 'sha256', $password . $salt ),  
        "salt" => $salt  
    ];  
}
```

Φυσική ασφάλεια

- Προστασία από φυσικές απειλές
 - Κλοπή εγγράφων
 - Πρόσβαση σε hardware
 - Αδιάκριτα βλέμματα
 - Tailgating
 - Ψάξιμο σε σκουπίδια



Μορφές φυσικών επιθέσεων

- **Denial of service**

- Καταστροφή εξοπλισμού
- Αποκοπή από το δίκτυο

- **Εμπιστευτικότητα**

- Κλοπή κωδικών ή δεδομένων

- **Ακεραιότητα**

- Εγκατάσταση/αλλαγή λογισμικού
- Αντικατάσταση/αλλαγή hardware
- Χωρίς να το καταλάβει το θύμα

Κλοπή κωδικών πρόσβασης

- Κοιτάζοντας πάνω από τον ώμο μας
- Φωτογραφία από το παράθυρο
- Post-it με κωδικούς πρόσβασης
- Keyloggers

WARNING
Read the risk of serious injury must
follow the correct Guide provided with
product and at www.hp.com/go



Bank pswd:
lucky 77

yahoo: mary 791a
pswd: eric 3132004

HP Pavilion Entertainment PC

Key loggers

- Τρόπος κλοπής του τι γράφεται στο πληκτρολόγιο:
 - Κωδικοί πρόσβασης
 - Πιστωτικές κάρτες
- Hardware keylogging
 - Αλλαγή πληκτρολογίου
 - Παρεμβολή στο καλώδιο πληκτρολογίου
 - Αποθηκεύουν τους κωδικούς στο hardware μέχρι να ανακτηθούν
 - Ή τους στέλνουν μέσω WiFi
- Software keylogging
 - Ιός - malware
 - Αποθηκεύει τους κωδικούς σε αρχείο
 - Τους στέλνει μέσω Internet στο θύτη



Παρακολούθηση / Παρεμβολή

- Σε φυσικό επίπεδο, μπορούν να παρακολουθούνται:
 - Σταθερό τηλέφωνο
 - Κινητό τηλέφωνο
 - Καλώδια δικτύου
 - WiFi
- Ενδεχομένως να υπάρχουν και παρεμβολές τύπου man-in-the-middle
- Μην εμπιστεύεστε το δίκτυο!

Garbage surfing

- Υποκλοπή εγγράφων από τα σκουπίδια
- Αριθμοί λογαριασμών
- Ονόματα
- Ημερομηνίες γέννησης
- Αριθμοί πιστωτικών καρτών
- Υπόλοιπο τραπεζικού λογαριασμού
- Λίστα συναλλαγών
- Αριθμός ταυτότητας
- ΑΦΜ
- Καταστρέψτε τα έγγραφά σας πριν τα πετάξετε!

Μία ιστορία

- Ο Πέτρος ταξιδεύει από την Αθήνα για το Λονδίνο
- Στα σύνορα, του ζητούν να δουν το laptop του
 - «Για λόγους ασφαλείας»
- Του ζητούν να γράψει τον κωδικό πρόσβασης
 - Σε περίπτωση που αρνηθεί, του απαγορεύεται η είσοδος στη χώρα
- Το laptop «επιθεωρείται» σε ένα δωμάτιο για 10 λεπτά

Τι μπορεί να συνέβη;

- Του εγκαταστάθηκε κάποιος keylogger?
- Έγινε αντίγραφο του δίσκου του;

Διάσχιση συνόρων

- Κίνα, Ρωσία, ΗΠΑ, Αγγλία, Βόρεια Κορέα, κ.ά.
- Μπορεί να μας κατασχεθεί το laptop για «επιθεώρηση»
 - ...ή το κινητό τηλέφωνο
- Μπορεί να μας ζητηθεί νόμιμα ο κωδικός μας
- Μπορεί να γίνει αντίγραφο του δίσκου μας
- Ο εξοπλισμός μας μπορεί να κατασχεθεί μόνιμα

Προστασία από φυσικές επιθέσεις

Denial of service

- Backups δεδομένων
- Σε περίπτωση καταστροφής, τα δεδομένα είναι ασφαλή
- Εναλλακτικές μέθοδοι πρόσβασης στο δίκτυο



Προστασία από φυσικές επιθέσεις

Integrity

- Κλείδωμα εξοπλισμού
- Χρήση δυνατών κλειδαριών

Κλειδαριές

- Οι περισσότερες μπορούν να παραβιαστούν εύκολα
 - <https://toool.nl/Toool>

Προστασία από φυσικές επιθέσεις

Confidentiality

- Κρυπτογράφηση δίσκου
- Σε περίπτωση κλοπής εξοπλισμού, τα δεδομένα είναι ασφαλή
- Δυνατοί κωδικοί πρόσβασης
- Ορθή πολιτική χρήσης κωδικών πρόσβασης

Κρυπτογράφηση δίσκου

- Πλήρης ή μερική
- **Πλήρης:** Κρυπτογραφεί όλο το σύστημα αρχείων
- **Μερική:** Κρυπτογραφεί επιλεγμένα αρχεία
- Χρησιμοποιείται συμμετρική κρυπτογραφία (AES)
- Ως κλειδί χρησιμοποιούνται:
 - Κωδικός πρόσβασης
 - Κάποιο αρχείο
 - Και τα δύο

TrueCrypt

- Επιτρέπει μερική/πλήρη κρυπτογράφηση δίσκου
- Χρησιμοποιεί AES
- Είναι ανοιχτού κώδικα
- Υποστηρίζει Linux, Mac, Windows

TrueCrypt demo

Αποκάλυψη κλειδιού

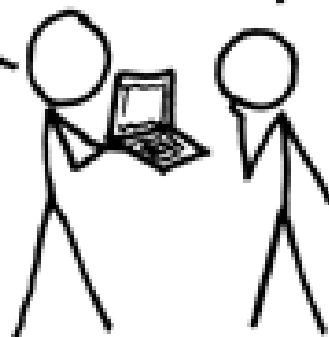
- Κάποιος που βλέπει το δίσκο μπορεί να καταλάβει ότι είναι κρυπτογραφημένος
- Αν υπάρχει υποψία ότι έχουμε παράνομα δεδομένα, μπορεί να μας ζητηθεί ο κωδικός πρόσβασης από κάποια αρχή (αστυνομία, δικαστήριο...)
- Δεν μπορούμε πάντα να αρνηθούμε!

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Quiz

- Πως μπορεί να καταλάβει κάποιος ότι ένας δίσκος είναι κρυπτογραφημένος;

Hidden Volumes

- Μπορούμε να κρύψουμε δύο volumes σε ένα κρυπτογραφημένο δίσκο
- «Ξεκλειδώνει» ένα από τα 2 ανάλογα με τον κωδικό που χρησιμοποιούμε
- Δεν μπορεί να αποδειχθεί ότι υπάρχει 2^ο volume

Hidden Volumes

- Χρησιμοποιούμε το πρώτο volume για να αποθηκεύουμε αθώα ή ελαφρώς ύποπτα δεδομένα
- Πρέπει να είναι αληθοφανή
- Χρησιμοποιούμε το δεύτερο volume για να αποθηκεύουμε εμπιστευτικά δεδομένα

Hidden volume demo

Full Disk Encryption (FDE)

- Όλος ο δίσκος κρυπτογραφείται
 - Λειτουργικό σύστημα
 - Προγράμματα
 - Δεδομένα του χρήστη
- Ακρυπτογράφητος bootloader

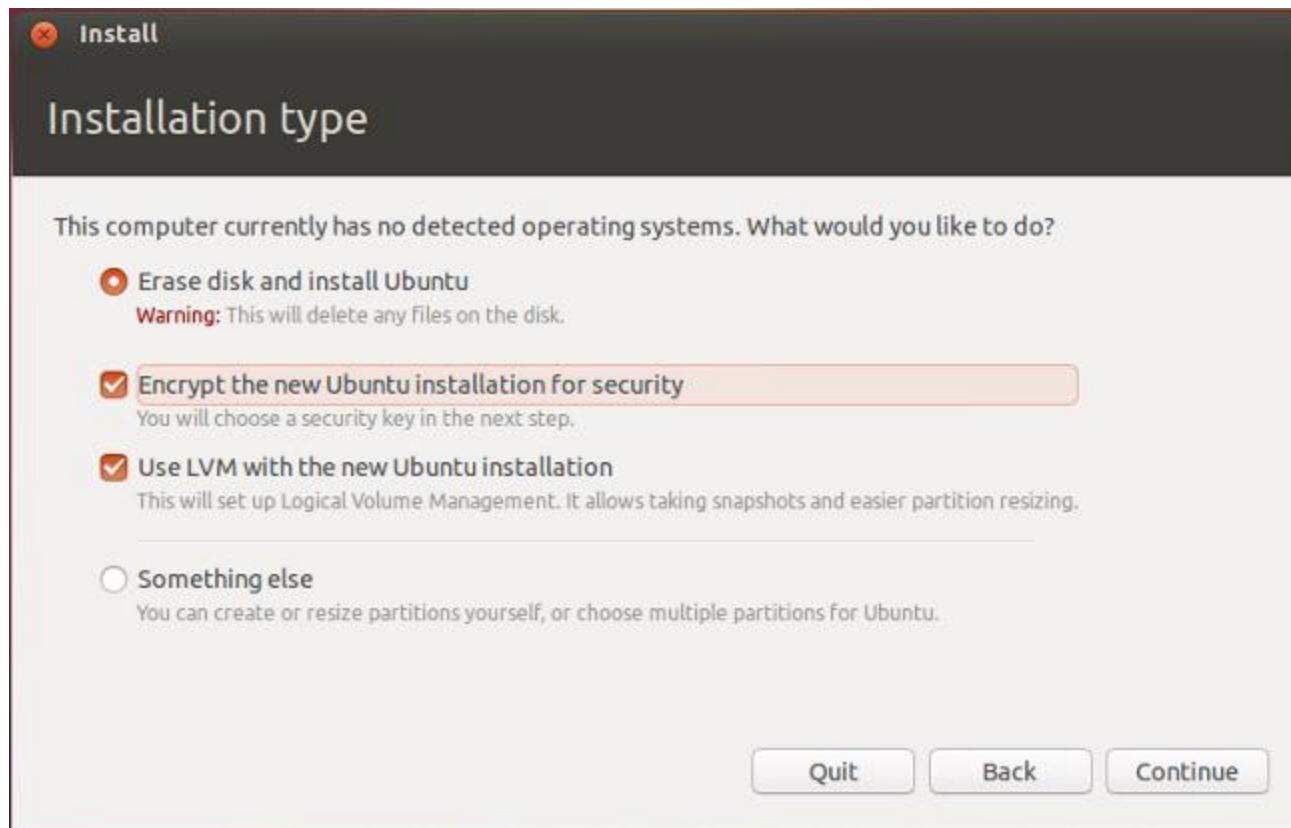
Full Disk Encryption (FDE)

- Mac
 - FileVault



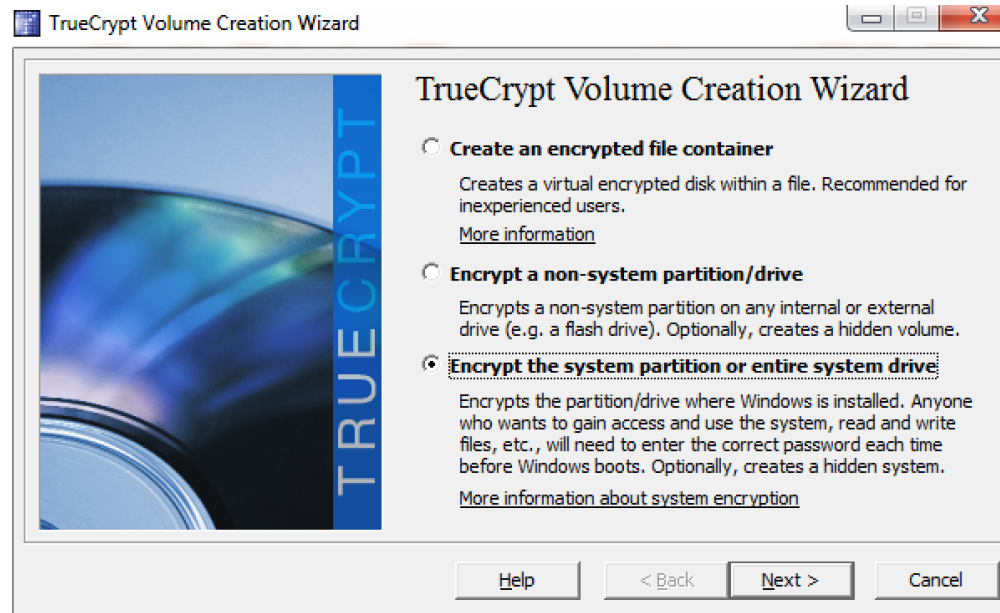
Full Disk Encryption (FDE)

- Linux
 - LUKS/dm-crypt
 - Υποστηρίζεται από τον πυρήνα



Full Disk Encryption (FDE)

- Windows
 - TrueCrypt



Evil Maid Attack

- Ο Διονύσης και ο Πέτρος ταξιδεύουν στις Βρυξέλλες να δουν το αγοράκι που κατουράει



Evil Maid Attack

- Έχουν αφήσει τα laptop τους, που έχουν FDE, στο ξενοδοχείο
- Η καμαριέρα είναι η πρώην γυναίκα του Πέτρου
- Ξεκινάει τα laptop από ένα εξωτερικό USB και αλλάζει τον ακρυπτογράφητο bootloader στον σκληρό δίσκο με έναν κακόβουλο δικό της
- Παίρνει ένα πλήρες αντίγραφο του κρυπτογραφημένου δίσκου
- Αποχωρεί



Evil Maid Attack

- Ο Πέτρος και ο Διονύσης γυρίζουν στο δωμάτιο
- Ανοίγουν τα laptop τους και τρέχουν τον κακόβουλο bootloader
- Πληκτρολογούν τον κωδικό τους
- Ο κακόβουλος bootloader καλεί τον πραγματικό bootloader με το σωστό κωδικό
- Αφού ξεκινήσει το σύστημα ο κακόβουλος bootloader στέλνει τον κωδικό στην Evil Maid
- Ο Πέτρος και ο Διονύσης δεν καταλαβαίνουν ότι συμβαίνει κάτι

Evil Maid Attack

- Η Evil Maid
 - Λαμβάνει τον κωδικό
 - Αποκρυπτογραφεί το κρυπτογραφημένο backup
 - Εγκαθιστά keylogger ή άλλο malware
 - Εγκαθιστά κάποιο rootkit που κρύβει την παρουσία του malware
 - **Ανακαλύπτει ότι ο Πέτρος είναι μυστικός fan του Bieber <3**



Άμυνα στο Evil Maid Attack

- Κλειδώνουμε το BIOS με κωδικό
- Απενεργοποιούμε το boot από εξωτερικές πηγές

-ή-

- Έχουμε τον bootloader μαζί μας

Threat Models

- Ειδικά η φυσική ασφάλεια δεν είναι ποτέ τέλεια
- Πάντα υπάρχουν επιθέσεις αν ο εχθρός έχει αρκετά χρήματα και χρόνο
- Η ουσία είναι να κάνουμε τις επιθέσεις πιο ακριβές και χρονοβόρες

“You can always be a little more paranoid.”

Tom Lowenthal

Quiz

- Υπάρχει περίπτωση να κρυπτογραφηθεί ο δίσκος μας χωρίς να το θέλουμε;

Ransomware

- Ιός που βασίζεται στην κρυπτογραφία
- Κρυπτογραφεί τα αρχεία μας
- Χρησιμοποιεί ασύμμετρη κρυπτογραφία
- Δεν περιέχει το private key
- Μας ζητάει λύτρα για να ξεκλειδώσουν τα αρχεία μας

Your personal files are encrypted!



Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you 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 **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

OTR - Τι βλέπει η Google

Hangout with Petros Aggelatos



Διονύσης Ζήνδρος

?OTR?v2?

dionyziz@gmail.com has requested an Off-the-Record private conversation <<http://otr.cypherpunks.ca/>>. However, you do See <http://otr.cypherpunks.ca/> for more information. 7:05 PM

?OTR:AAIKAAAaWHSaM1qqhqsGgWZH4Zk5cT7n+JtBkNaUEI/83ozBIPBv7icgiWjD30CJTtugotPwPFLoydpk3OulLcce+7JTsf4y66h0ila8wcQh7zRLRvYOD0T/Ugc1irKNWQFym8Pr3ALJE53lpTj0JeR0GsRf7S9TSuqmzbubf48HDHYqy2bYxMbg6MKwP0kORq4pqXPLYjBnGiDR2MY16sldpYC5NxqMoVxSCxq+XviL/IB67NA==.



Petros Aggelatos

?OTR:AAICAAAaXAdRmwqYvKdd3f8WSIAAdDyrmOUMW+0CAm5UPmN8MPqD8j3O72CHANisn6gn+Neyyxm/TVwPI7oMEI7SJ8C2dTCYmHpabLWaxFloXPYzzNzk9de1Svvc7SdTW+FC0qWF79Qdl3ba6NtAC5TOP0QXnXIbbKaT1ZbWds6YJ2hu4/rXOIyafmGGWN7qkq6waMFlgk0GCd5+8i6sKor5J8+jZ/MGCBiulWHoNWP sYYOLR/qKVuRTAYAAAAAg8nNKcS1nTiJTHNnXEV5BoF/sSR8+MjoO8lBAE4gOU=.

?OTR:AAIRAAAAEBX3OXW7JT8pCISYUwRRh/4AAAHSoHl+LqMpylR7mp6VjeH+5BfCwhLbYfeQYdjrAJwEee0M0u701rJr2I1ES62WanrQ4gLXZvkVwmdyViBzGjpUFXEIhCR4aDNKsbfBKc1l+c/QxnmM28Vh9UuvXn6/uC+KwzSudZFWUqg1RleLr514GZLVjVGr5jbmlOJFjnp4o7J8FKpKQ7CR6i/aGKYtqJPsgpcUIDXTmDf4FrG2fuXlrqdxmG9ShKWYJdwb44Ak0CYz2wMRfbRqnB9nlbct7zxBrjDkIYieHpEBgFvZkyTTQtg5ydsHVTkm9kCXwrAvVPsD7GrZELJL9dCrmSd9SwYbAbgwSROYtbYHCJKSA4RrPHq8jaZh2jR6q37MtrLoEDr2/Unofpps80d/1/ZjSb0v3VILsTJs+lyhGciO+TebJzb37DPp0xH0BIGzvErd2zFgkCYfBwcCKzgSV2HMr7s5VbkK7hbqKaamEdTShTW/zUicf+JFdOFOK0A6buidSBDVTml8Pc2if0AywGPFggdgo5mJqGMOd4zxkKLjBf70vo9yuc0rNPcyJFfkyOgdeh3GlyrlayPF6UxKeqWe1Qr8tNbRwgQGtWy7YiTiqG9O4w.

Bitcoin στην πράξη

Διευθύνσεις Bitcoin

- Κάθε client φτιάχνει ένα πορτοφόλι
- Το πορτοφόλι περιέχει πολλαπλές διευθύνσεις
 - Οι διευθύνσεις είναι δημόσια κλειδιά
 - Μπορούν να δημοσιευθούν με ασφάλεια
 - Ξεκινούν πάντα με '1'
 - Είναι σαν αριθμοί λογαριασμών
 - 174aNr4bHZPbTgsm3xudqVKqjZYNPwKK28

All	All	Enter address or label to search	Min amount
Date	Type	Address	Amount
✓ 2/20/14 22:01	Sent to	Stavros Messinis	-0.1185834
✓ 2/20/14 18:04	Sent to	Lydia Tsagkou	-0.02335581
✓ 2/15/14 14:24	Sent to	Themis Papameleti	-0.02210606
✓ 2/13/14 12:46	Sent to	Alex Emexezidis	-0.01265188
✓ 2/2/14 18:20	Received with	dionyziz	0.1862
✓ 1/31/14 15:02	Received with	dionyziz	0.1823
✓ 1/22/14 22:30	Sent to	gtklocker	-0.01657862
✓ 1/13/14 08:16	Received with	dionyziz	1.30922042
✓ 1/4/14 01:52	Received with	dionyziz	0.67
✓ 11/19/13 10:28	Sent to	Petros @coinbase	-4.10218609
✓ 11/19/13 09:28	Sent to	Petros @coinbase	-0.01
✓ 11/19/13 05:01	Received with	dionyziz	0.8261
✓ 10/28/13 19:29	Sent to	James (Twitter)	-2.56
✓ 10/28/13 06:01	Received with	dionyziz	0.2807
✓ 10/13/13 01:56	Received with	dionyziz	5.56538609
✓ 10/13/13 01:52	Sent to	dionyziz (Android)	-0.10
✓ 10/13/13 01:45	Received with	dionyziz	0.10
✓ 10/3/13 01:25	Sent to	(16eyGvQYSYsHPHMcuvX32objEsPQRfXv9)	-0.10
✓ 10/3/13 01:25	Sent to	(16eyGvQYSYsHPHMcuvX32objEsPQRfXv9)	-5.56538609
✓ 9/30/13 22:42	Received with	dionyziz	2.63158
✓ 9/30/13 03:41	Received with	dionyziz	2.00
✓ 9/2/13 15:48	Received with	dionyziz	0.25759289

Confirmed (5129 confirmations)
Sent to gtklocker (12CtJLCCpVjFh34NIZSyP2Pum2sptDkws)

Export



Balance 0 BTC (€0.00)

Exchange	Currency	Last
BTC-E	EUR	414.14581

Wallets

Your wallet description



0 BTC (€0.00)

New Wallet

Send

Request

Transactions

Preferences

Your address 1FLdnXgM9woJtKmFfTWhpTowf3PDgzQj7N



Label

Amount

BTC = €



New

Your receiving addresses

Label ▲	Address
	1FLdnXgM9woJtKmFfTWhpTowf3PDgzQj7N

Online

Synchronising with network...

Android Wallet demo



Your Bitcoin Address:

1GjS kw4q HTBS
hMxb xU33 fFCE
SDTo yvfY Kw



mBTC**61.88**

Received

Both

Sent

- **Feb 9** → Ody Varvounis - 9.95
- **Feb 1** → vkoukis - 1.73
- **12/19/2013** → 15oarnxoKSpb... - 2.06
- **12/4/2013** → 1CwU4DEkFW7o... - 23.10
- **11/28/2013** → 16xKFc7LaA9... - 11.10



REQUEST COINS

SEND COINS



You need to [back up your wallet!](#)



Αγορά με Bitcoin Demo

Tor Demo

Μάθαμε

- Εμβάθυνση σε προηγούμενες έννοιες
- Σφαιρική παρουσίαση εννοιών
- Έννοιες στη φυσική ασφάλεια
- Κρυπτογράφηση δίσκου (LUKS, TrueCrypt, FileVault)
- Plausible deniability
- Περισσότερα για app sec
- Hidden tor services
- Bitcoin πορτοφόλια
- Bitcoin στην πράξη

Ευχαριστούμε που μας παρακολουθήσατε!

- Θα συνεχίσουμε ενεργά:
 - Facebook group
 - Google group / mailing list
 - security-class-gr@googlegroups.com
- Παραμένουμε διαθέσιμοι:
 - petrosagg@gmail.com
 - dionyziz@gmail.com
- Κώδικας: MIT license
- Υπόλοιπο υλικό: Creative Commons 3.0 Attribution
- <https://github.com/gtklocker/security-class>

Ασκήσεις

- Παρακαλούμε λύστε τις ασκήσεις!
- 1^η άσκηση: Δημιουργία και χρήση gpg κλειδιών
- 2^η άσκηση: Χρήση HTTPS στη σελίδα σας
- 3^η άσκηση: Διόρθωση ασφάλειας web εφαρμογής
- 4^η άσκηση: Απόκτηση bitcoin
- 5^η άσκηση: Στήσιμο hidden service
- Θα ανέβουν όλες σύντομα
- Τα podcasts θα ανέβουν τις επόμενες εβδομάδες