Ασφάλεια & Ηλεκτρονικό Επιχειρείν

Γιάννης Ηλιάδης
jiliad@aegean.gr

Σύνοψη Παρουσίασης

- Εισαγωγή στο Ηλεκτρονικό Επιχειρείν
- Ηλεκτρονικό Επιχειρείν και Ασφάλεια Πληροφοριών
- Εισαγωγή στην Ασφάλεια Πληροφοριών
- Αντιμετωπίζοντας τις Απειλές από το Ηλεκτρονικό Επιχειρείν
- Συνοπτική αναφορά στα Συστήματα Ηλεκτρονικών Πληρωμών και Πληρωμών με Κινητά Τηλέφωνα
- Μελέτη Περίπτωσης: Προβλήματα Ασφαλείας στα ATM

Εισαγωγή στο Ηλεκτρονικό Επιχειρείν

Ηλεκτρονικό Επιχειρείν: Επιχειρηματική και Τεχνολογική Καινοτομία

Το Ηλεκτρονικό Επιχειρείν εισάγει νέες μεθόδους στα ακόλουθα:

- Τηλεπικοινωνίες
- Επιχειρηματικές Δοσοληψίες
- Δομή Αγοράς
- Εκπαίδευση
- Εργασία

Πλεονεκτήματα Ηλεκτρονικού Επιχειρείν

- Εύκολη και γρήγορη πρόσβαση στην πληροφορία για το ευρύ κοινό
- Μείωση του κόστους
- Διεύρυνση αγοράς
- Αύξηση ανταγωνισμού
- Μείωση τιμών

Μειονεκτήματα Ηλεκτρονικού Επιχειρείν

- Ο Κυβερνοχώρος είναι άναρχος
- Το Ηλεκτρονικό Επιχειρείν μειώνει το επιχειρηματικό κόστος και για τους επίδοξους απατεώνες
- Αναιρεί την εγγενή εμπιστοσύνη που υπάρχει στις παραδοσιακές μεθόδους του επιχειρείν
  - Συμβόλαια,
  - Τιμολόγια, παραστατικά
  - Επαφή πρόσωπο με πρόσωπο,
  - Υπάρχον νομικό επιχειρηματικό πλαίσιο
- «Ψηφιακό χάσμα» (πολιτισμικό και φυλετικό χάσμα στην πρόσβαση και χρήση του Διαδικτύου)

Το Ηλεκτρονικό Επιχειρείν στην Ελλάδα

- 38% των εταιρειών που συμμετείχαν στην έρευνα χρησιμοποιούν πρακτικές Ηλεκτρονικού Επιχειρείν
  - Το 12.5% εξ' αυτών έχουν ενσωματώσει το Ηλεκτρονικό Επιχειρείν στην καθημερινή επιχειρηματική τους δραστηριότητα
  - Το υπόλοιπο 25.5% χρησιμοποιεί το Ηλεκτρονικό Επιχειρείν ευκαιριακά

- Το 47% των εταιρειών σχεδιάζουν να υιοθετήσουν πρακτικές Ηλεκτρονικού Επιχειρείν, ενώ το 33% εξ' αυτών σχεδιάζουν να υιοθετήσουν πρακτικές Ηλεκτρονικού Επιχειρείν μέσα στο επόμενο έτος.

Μελέτη από το ELTRUN, ΑΣΣΟΕ, Ελλάδα (2001);
Στατιστικό δείγμα: 240 Ελληνικές εταιρείες

Ηλεκτρονικό Επιχειρείν & Εμπιστοσύνη

Τι είναι Εμπιστοσύνη;

- Η εμπιστοσύνη μας επιτρέπει να βασιζόμαστε στην πληροφόρηση ή τις ενέργειες ενός τρίτου
- Η εμπιστοσύνη είναι εγγενής και υποκειμενική ιδιότητα. Διαδίδεται, αλλά δεν μεταβιβάζεται.

Ηλεκτρονικό Επιχειρείν & Εμπιστοσύνη (2)

- Εμπιστοσύνη στο παραδοσιακό επιχειρηματικό περιβάλλον
  - Συμβόλαια, παραστατικά, προσωπική επαφή, υπάρχον νομικό πλαίσιο για την επιχειρηματικότητα
- Εμπιστοσύνη στο Ηλεκτρονικό Επιχειρείν
  - Δεν υπάρχει σαφές νομικό πλαίσιο, τουλάχιστον όχι για τις δοσοληψίες B2C; Υπό κατασκευή
  - Δοσοληψίες από απόσταση μεταξύ αγνώστων
    - Έλλειψη έμπιστης πληροφόρησης για την ταυτότητα του άλλου μέρους
    - Έλλειψη έμπιστης πληροφόρησης για την επαλήθευση της ταυτότητας του άλλου μέρους

Εγγενής Ανάγκη για Εμπιστοσύνη

- Η ανάγκη για μεγιστοποίηση της εμπιστοσύνης είναι εγγενής, γιατί οι σχέσεις εμπιστοσύνης αποτελούν πρόσφορο έδαφος για την επιχειρηματικότητα, αλλά
  - Περισσότερη εμπιστοσύνη = Περισσότερη επικινδυνότητα
- Πρέπει να αναλύσουμε και να διαχειριστούμε την επικινδυνότητα (απαλοιφή, αποδοχή μεταβίβαση)
- Η Διαχείριση Επικινδυνότητας είναι μία διαδεδομένα έννοια στους σύγχρονους επιχειρηματικούς οργανισμούς

Ηλεκτρονικό Επιχειρείν και Ασφάλεια Πληροφοριών

Διοικητικές Αποφάσεις και Ανάλυση Επικινδυνότητας

- Δεν υπάρχει 100% Ασφάλεια
- Υπάρχει η ανάγκη για μία λύση που ισορροπεί το κόστος και τις απαιτήσεις ασφαλείας
- Η Ασφάλεια Πληροφοριών δεν είναι αποτρεπτικός παράγοντας για το Ηλεκτρονικό Επιχειρείν, αντίθετα εξασφαλίζει περισσότερο την βιωσιμότητά του

Κόστος Ασφάλειας Πληροφοριών

- Κόστος υλοποίησης
- Κόστος ενσωμάτωσης διαδικασιών, υπηρεσιών και μηχανισμών στα υπάρχοντα συστήματα
- Κόστος ανάπτυξης νέων διαδικασιών, υπηρεσιών και μηχανισμών
- Λειτουργικά κόστη
  - Υλικό
  - Λογισμικό
  - Κόστος Προσωπικού
  - Διαχείριση Αλλαγών
  - Νέες Επιχειρηματικές Διεργασίες

Από που προέρχονται οι Απαιτήσεις Ασφαλείας;

- Ανάλυση Επικινδυνότητας, με βάση:
  - Υπάρχουσες, αποτυπωμένες επιχειρηματικές διεργασίες
  - Συνεντεύξεις με ανώτερα στελέχη
  - Νομικά ζητήματα (π.χ. Νομοθεσία για την προστασία προσωπικών δεδομένων)
  - Εταιρική εικόνα
  - Ενδεχόμενοι επιχειρηματικοί αντίπαλοι (πιθανότητα για επίθεση στα Πληροφοριακά Συστήματα)

Κύκλος ζωής Ασφαλείας

- Ανάλυση επικινδυνότητας
- Πολιτική Ασφαλείας
- Επανασχεδιασμός συστημάτων
- Διαχείριση του υλοποιημένου συστήματος ασφαλείας
- Διαδικασίες Αναφοράς Επεισοδίων
- Σχέδιο Συνέχειας Επιχειρηματικής Δραστηριότητας

Ανάλυση Επικινδυνότητας!

Τι βρίσκεται σε κίνδυνο
- Ποσοτική ανάλυση
- Ποιοτική ανάλυση

Ποιες ευπάθειες είναι εκμεταλλεύσιμες
- Τεχνικές
- Διαδικασίες
- Ανθρώπινος παράγοντας

Διαχείριση Επικινδυνότητας
- Εξάλειψη επικινδυνότητας
- Αποδοχή επικινδυνότητας
- Μεταβίβαση επικινδυνότητας

Η Διαχείριση της Επικινδυνότητας γίνεται μέρος της καθημερινής επιχειρηματικής πρακτικής

Πολιτική Ασφάλειας Πληροφοριών

- Η βάση για όλες τις προσπάθειες για Ασφάλεια Πληροφοριών
- Κατευθύνει τον τρόπο χειρισμού καταστάσεων και τον τρόπο εκμετάλλευσης τεχνολογιών
- Το πλέον εύκολο μέτρο στην εκτέλεση, αλλά το πιο δύσκολο στην υλοποίηση
- Η υλοποίηση της Πολιτικής Ασφαλείας είναι δύσκολη, γιατί:
  - Δεν πρέπει να αντικρούεται με καμμία νομοθεσία
  - Πρέπει να είναι εκμεταλλεύσιμη σε περίπτωση δικαστικής διένεξης
  - Πρέπει να διαχειρίζεται και να παρακολουθείται στενά

Η Ανάγκη για Ασφάλεια στο Ηλεκτρονικό Επιχειρείν

- Το πλήθος των κυβερνοεπιθέσεων αυξήθηκε απότομα από 22.000 το 2000 στις 82.000 το 2002
- Το πρώτο τρίμηνο του 2003, ήταν ήδη 43.000

Πηγή: US Computer Emergency Response Team (US CERT)

Εισαγωγή στην Ασφάλεια Πληροφοριών

Εισαγωγή στην Ασφάλεια Πληροφοριών

- …δεν είναι απλώς τεχνολογία, ή τουλάχιστον όχι μόνο τεχνολογία
- Αφορά στην δημιουργία Πληροφοριακών Συστημάτων με τέτοιον τρόπο που η επικινδυνότητα να είναι διαχειρίσιμη (να μπορεί να εξαλειφθεί, να γίνει αποδεκτή ή να μεταβιβασθεί)

- Βασικές Ιδιότητες της Ασφάλειας Πληροφοριών: CIA
  - Confidentiality (Εμπιστευτικότητα)
  - Integrity (Ακεραιότητα)
  - Availability (Διαθεσιμότητα)

…περισσότερες υπηρεσίες Ασφάλειας Πληροφοριών

- Επαλήθευση Ταυτότητας
- Έλεγχος Πρόσβασης
- Μη αποποίηση ευθύνης
- Ιδιωτικότητα
- Ανωνυμία

Προκλήσεις για την Ασφάλεια Πληροφοριών

Πληροφοριακά Συστήματα

Τότε

- Κεντρικοποιημένα, κλειστά
- Ιδιωτικά, δεν επιτρεπόταν η πρόσβαση από τρίτους
- Ευρύ φάσμα από πρωτόκολλα επικοινωνίας που διέφεραν ανά σύστημα
- Ακριβά
- Περιορισμένη ομάδα ενδιαφέροντος

Τώρα

- Κατανεμημένα, ανοιχτά
- Δεν υπάρχει ιδιοκτησία
- Ανθεκτικότητα,
- Πρόσβαση σε όλους
- Προτυποποιημένα πρωτόκολλα επικοινωνίας
- Χαμηλό κόστος πρόσβασης στο Διαδίκτυο

Μερικές Γενικές Αρχές

- ...ένα σύστημα είναι τόσο ασφαλές, όσο το λιγότερο ασφαλές τμήμα του
- Η επικινδυνότητα δεν προέρχεται μόνο από εξωτερικές πηγές. Συχνά προέρχεται από εσωτερικές (π.χ. απογοητευμένοι υπάλληλοι)
- Η μυστικοπάθεια όσον αφορά στο πως έχουν υλοποιηθεί οι μηχανισμοί Ασφαλείας δεν ωφελεί. (“… the only good locks are open, public and accessible ones”, W. Diffie)

Bottom-up προσέγγιση στην Ασφάλεια Πληροφοριών

- Οι Διαχειριστές Συστημάτων προσπαθούν να βελτιώσουν την ασφάλεια των συστημάτων τους
- Τα εμπλεκόμενα πρόσωπα είναι τεχνικά άρτια καταρτισμένα
- Δεν εφαρμόζεται στην πράξη, διότι δεν εξασφαλίζει:
  - Υποστήριξη από την Διοίκηση του οργανισμού
  - Υποστήριξη από το προσωπικό του οργανισμού

Top-down προσέγγιση στην Ασφάλεια Πληροφοριών

Σημείο εκκίνησης η Διοίκηση του οργανισμού

- Εκδίδει πολιτικές και δόκιμες πρακτικές
- Προδιαγράφει τα αναμενόμενα αποτελέσματα
- Καθορίζει ποιος είναι υπεύθυνος και για ποιες δράσεις

Πλεονεκτήματα:

- Ισχυρή υποστήριξη από την Διοίκηση
- Εξασφαλισμένο προσωπικό Πληροφορικής
- Εξασφαλισμένη χρηματοδότηση
- Χρονοδιάγραμμα εκτέλεσης
- Υποστήριξη από το προσωπικό

Ομάδα Έργου Ασφάλειας Πληροφοριών

- Chief Security Officer
- Chief Information Officer
- Risk assessment specialists
- Security administrators
- Security engineers
- System administrators
- End users (!)

Εισαγωγή στην Κρυπτογραφία

- Συμμετρικά Κρυπτοσυστήματα
- Ασύμμετρα Κρυπτοσυστήματα
- Ψηφιακές Υπογραφές

Εισαγωγή στην Κρυπτογραφία: Συμμετρικά Κρυπτοσυστήματα

Alice

Συμμετρικό κλειδί: "pass21"

ENCRYPT

έγγραφο

Κρυπτογραφημένο έγγραφο

Network

Network

Bob

Συμμετρικό κλειδί : "pass21"

DECRYPT

Κρυπτογραφημένο έγγραφο

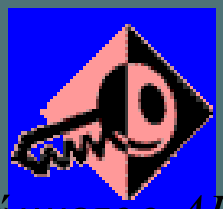
έγγραφο

Εισαγωγή στην Κρυπτογραφία: Συμμετρικά Κρυπτοσυστήματα

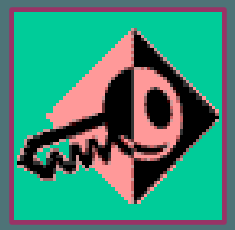
- Η Alice και ο Bob έχουν το ίδιο κλειδί (pass21)
- *Κρυπτογράφηση/αποκρυπτογράφηση*
  - Βήμα 1: Η Alice κρυπτογραφεί το έγγραφο με κλειδί “pass21” και αποστέλλει στον Bob (π,χ, με e-mail) το κρυπτογραφημένο έγγραφο
  - Βήμα 2: Ο Bob λαμβάνει (π.χ. e-mail) το κρυπτογραφημένο έγγραφο και χρησιμοποιεί το κλειδί “pass21” για να το αποκρυπτογραφήσει και να αποκτήσει πρόσβαση στο αρχικό έγγραφο
- Η Alice πρέπει να επικοινωνήσει στον Bob το κλειδί (“pass21”) με έναν ασφαλή τρόπο, δηλαδή κανείς δεν πρέπει να μάθει ποιο είναι αυτό το κλειδί (εμπιστευτικότητα του κλειδιού)

Εισαγωγή στην Κρυπτογραφία: Ασύμμετρα Κρυπτοσυστήματα

Alice



Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί της Alice "pert35"



Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί της Alice "pert35"

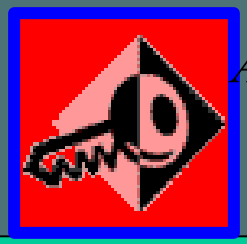
Bob

Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί του Bob's "dfgsd3

Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί του Bob's "3trer4"

Εισαγωγή στην Κρυπτογραφία: Ασύμμετρα Κρυπτοσυστήματα

Alice



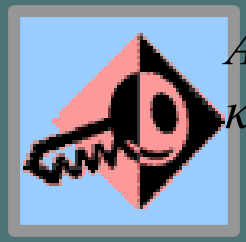
Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί του Bob's "dfgsd34"

ENCRYPT

έγγραφο

Κρυπτογραφημένο έγγραφο

Network



Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί του Bob's"3trer4"

Network

Bob

DECRYPT

Κρυπτογραφημένο έγγραφο

έγγραφο

Εισαγωγή στην Κρυπτογραφία: Ασύμμετρα Κρυπτοσυστήματα

- Η Alice διαθέτει ένα ΔΗΜΟΣΙΟ και ένα ΙΔΙΩΤΙΚΟ κλειδί
- Ο Bob διαθέτει ένα διαφορετικό ΔΗΜΟΣΙΟ και ένα διαφορετικό ΙΔΙΩΤΙΚΟ κλειδί
- *Κρυπτογράφηση/Αποκρυπτογράφηση:*
  - Βήμα 1: Η Alice κρυπτογραφεί το έγγραφο με το ΔΗΜΟΣΙΟ κλειδί του Bob “dfgsd34” και αποστέλλει στον Bob (π.χ. Με e-mail) το κρυπτογραφημένο έγγραφο.
  - Βήμα 2: Ο Bob λαμβάνει (π,χ, e-mail) το κρυπτογραφημένο έγγραφο και χρησιμοποιεί το ΙΔΙΩΤΙΚΟ κλειδί του “3trer4” για να αποκρυπτογραφήσει το έγγραφο και να ανακτήσει το αρχικό έγγραφο.
- Ο Bob πρέπει να στείλει στην Alice το ΔΗΜΟΣΙΟ κλειδί του (“dfgsd34”) με έναν ασφαλή τρόπο, δηλαδή κανείς δεν πρέπει να είναι σε θέση να παραβιάσει την **ακεραιότητα του ΔΗΜΟΣΙΟΥ** κλειδιού του Bob κατά την αποστολή του προς την Alice.

Σύγκριση συμμετρικών & ασύμμετρων κρυπτοσυστημάτων

- Συμμετρικά κρυπτοσυστήματα
  - Χρησιμοποιείται μόνο ένα κλειδί που έχουν από κοινού η A(lice) και ο B(ob),
  - Αυτό το κλειδί πρέπει να παραμείνει **εμπιστευτικό**, δηλαδή δεν πρέπει κανείς να μάθει το περιεχόμενο του κλειδιού εκτός της Alice και του Bob.
- Ασύμμετρα κρυπτοσυστήματα
  - Χρησιμοποιείται ένα ζεύγος κλειδιών (ΔΗΜΟΣΙΟ+ΙΔΙΩΤΙΚΟ) για κάθε μέλος της επικοινωνίας.
  - Το ΔΗΜΟΣΙΟ κλειδί του Bob πρέπει να κοινοποιηθεί στην Alice με τέτοιον τρόπο που να διασφαλίζεται η **ακεραιότητα** του κλειδιού, δηλαδή ότι η Alice θα λάβει όντως το κλειδί του Bob και όχι κάποιο άλλο κλειδί.

Ψηφιακές Υπογραφές

Alice

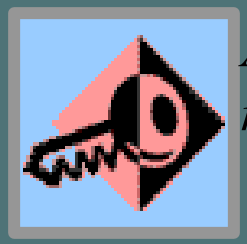
Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί της Alice "pert35"

SIGN

έγγραφο

Υπογεγραμμένο έγγραφο

Network



Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί της Alice "pert35"

Bob

Network

VERIFY SIGNATURE

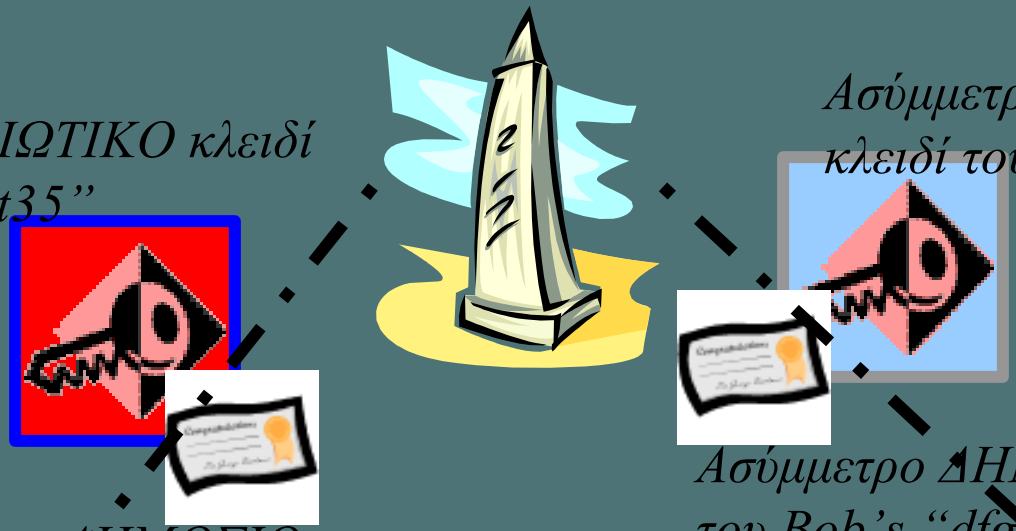
Υπογεγραμμένο έγγραφο

έγγραφο

Πάροχος Υπηρεσίας Πιστοποίησης

Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί της Alice "pert35"

Ασύμμετρο ΙΔΙΩΤΙΚΟ κλειδί του Bob's "3trer4"



Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί της Alice "pert35"

Ασύμμετρο ΔΗΜΟΣΙΟ κλειδί του Bob's "dfgsd34"

Alice

Bob

Αντιμετωπίζοντας τις Απειλές από το Ηλεκτρονικό Επιχειρείν

Απειλές στις Ηλεκτρονικές Συναλλαγές

- Παρακολούθηση των γραμμών επικοινωνίας
- Εικασία του διαμοιραζόμενου συμμετρικού κλειδιού
- Υποκλοπή του διαμοιραζόμενου συμμετρικού κλειδιού
- Μη εξουσιοδοτημένη τροποποίηση πληροφορίας κατά την μεταφορά
- Μεταμφίεση
- Υποκλοπή συνθηματικού
- Μη εξουσιοδοτημένη πρόσβαση

Μη Ασφαλείς Συναλλαγές

insecure communication channel

Αντιμετωπίζοντας τις Απειλές με Κρυπτογραφικούς Μηχανισμούς

- *Παρακολούθηση γραμμών επικοινωνίας*

  Κρυπτογράφηση με τυχαίο διαμοιραζόμενο συμμετρικό κλειδί
- *Εικασία/Υποκλοπή του διαμοιραζόμενου συμμετρικού κλειδιού*

  Κρυπτογράφηση του διαμοιραζόμενου συμμετρικού κλειδιού με το ΔΗΜΟΣΙΟ κλειδί της οντότητας που λαμβάνει την πληροφορία
- *Μη εξουσιοδοτημένη τροποποίηση της πληροφορίας, κατά την μεταφορά*

  Συναρτήσεις σύνοψης και παραγωγή message authentication codes, κρυπτογραφώντας τα αποτελέσματα των συναρτήσεων σύνοψης

Αντιμετωπίζοντας τις Απειλές με Κρυπτογραφικούς Μηχανισμούς (2)

- *Μεταμφίεση*

  Ανταλλαγή ψηφιακών πιστοποιητικών

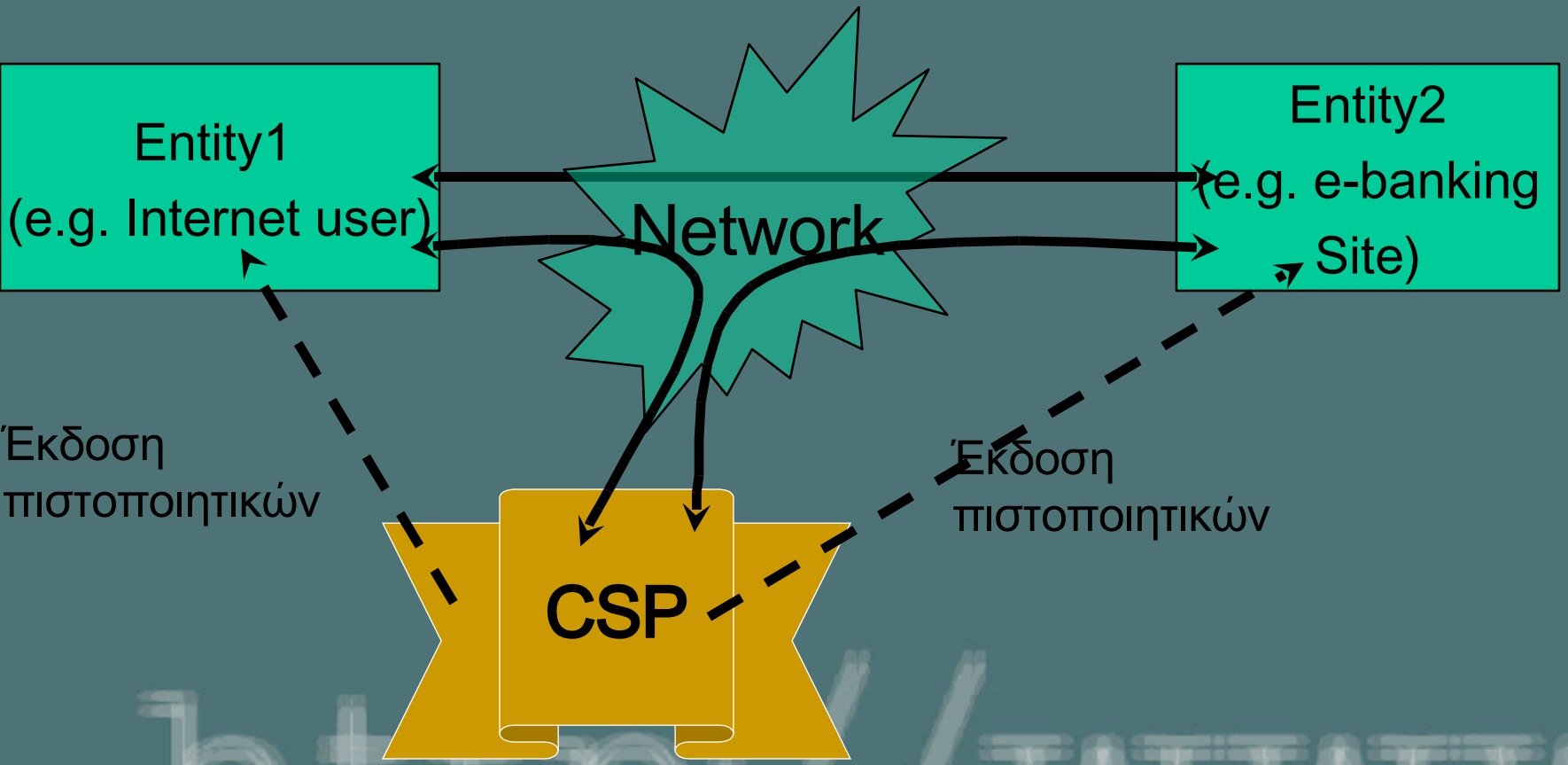
- *Υποκλοπή συνθηματικού*

  Τα συνθηματικά δεν ταξιδεύουν ποτέ στο δίκτυο

- *Μη εξουσιοδοτημένη πρόσβαση*

  Τοπική Λίστα Ελέγχου Πρόσβασης, Επαλήθευση ταυτότητας με την χρήση ψηφιακών πιστοποιητικών

Ασφάλεια στις Ηλεκτρονικές Συναλλαγές με την Χρήση Υποδομής Δημόσιου Κλειδιού



Πάροχος Υπηρεσιών Πιστοποίησης: Ο ακρογωνιαίος λίθος της Υποδομής Δημόσιου Κλειδιού

Έμπιστη Τρίτη Οντότητα (ΕΤΟ): «ένας οργανισμός που δημιουργεί κλίμα εμπιστοσύνης σε μία ηλεκτρονική συναλλαγή, χρησιμοποιώντας επιχειρηματικά και τεχνικά μέτρα»

Οι Πάροχοι Υπηρεσιών Πιστοποίησης είναι Έμπιστες Τρίτες Οντότητες που ελέγχουν τον κύκλο ζωής των ψηφιακών πιστοποιητικών

Υποδομή Δημόσιου Κλειδιού: Τρέχουσα Μόδα...

- Έχει δημιουργήσει ρεύμα τεχνολογικής μόδας...
- Είναι εύκολο στην υλοποίηση
- Πληροί αρκετές απαιτήσεις ασφαλείας, διότι προσφέρει έναν μεγάλο αριθμό υπηρεσιών ασφαλείας που κυμαίνονται από εμπιστευτικότητα ως ηλεκτρονικές συμβολαιογραφικές υπηρεσίες
- Είναι πανάκεια!

Υποδομή Δημόσιου Κλειδιού: Τρέχουσα Μόδα...

...όμως:

- Μία τυπική υλοποίηση και λειτουργία ενός Παρόχου Υπηρεσιών Πιστοποίησης, χωρίς να έχει προηγηθεί ανάλυση απαιτήσεων ασφαλείας και χωρίς να έχει σχεδιασθεί Πολιτική Ασφαλείας και Πολιτική Έκδοσης Πιστοποιητικών αποτελεί **περισσότερο πρόβλημα παρά λύση**. Η Υποδομή Δημόσιου Κλειδιού δεν είναι μία πανάκεια, ούτε μία λύση ασφαλείας που ταιριάζει σε όλα τα προβλήματα ασφαλείας.

Κακόβουλο Λογισμικό

- *το λογισμικό που περιέχει τις απαιτούμενες εντολές για μία επίθεση σε ένα υπολογιστικό σύστημα.*
- *…επίθεση: η παραβίαση (ή η απόπειρα παραβίασης) της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας του συστήματος*

Κατηγορίες Κακόβουλου Λογισμικού

Ιομορφικό Λογισμικό

- Ιοί Τομέα Εκκίνησης
- Παρασιτικοί
- Πολυμερείς
- Διαμένοντες στην Κύρια Μνήμη
- Κρυφοί
- Κρυπτογραφημένοι
- Πολυμορφικοί
- Ρετρο-Ιοί
- Ιοί που διαγράφουν τμήμα του ξενιστή
- Μακρο-Ιοί

Μη Ιομορφικό Λογισμικό

- Κερκόπορτες
- Λογικές Βόμβες
- Δούρειοι Ίπποι
- Αναπαραγωγοί
- Βακτήρια
- Παραπλανητική Πληροφόρηση

Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού

- Επίγνωση σε θέματα Ασφαλείας
- Αντιβιοτικό Λογισμικό
- Αρχεία Ελέγχου του Λειτουργικού Συστήματος
- Αυστηρά μέτρα Ασφαλείας
- Απαγόρευση μεταφόρτωσης εκτελέσιμου κώδικα
- Απομόνωση
- Αναχώματα Ασφαλείας
- Εργαλεία Ανίχνευσης Εισβολών
- Διατυπωμένη διαδικασία ανάνηψης από προσβολή και περιορισμού Κακόβουλου Λογισμικού
- Συνεργασία με τους οργανισμούς που προσφέρουν προϊόντα υλικού και λογισμικού για προστασία από Κακόβουλο Λογισμικό

Αντιμετωπίζοντας Απόπειρες Εισβολής

Συστήματα Ανίχνευσης Εισβολών

- ***Ανίχνευση ανωμαλίας (Anomaly Detection)***

  Ανιχνεύουν μία σειρά από ενέργειες που είναι ασυνήθιστο να συμβούν, τουλάχιστον όχι με την συγκεκριμένη σειρά

- ***Ανίχνευση κακής χρήσης (Misuse Models)***

  Ανιχνεύουν μία σειρά από ενέργειες που είναι γνωστό ότι παραβιάζουν την Πολιτική Ασφαλείας

- ***Με βάση τις προδιαγραφές (Specification based)***

  Ανιχνεύουν μία σειρά από ενέργειες που δεν συμβαδίζουν με τις προδιαγραφές ενεργειών που το Σύστημα Ανίχνευσης Εισβολών γνωρίζει

Ηλεκτρονικό Επιχειρείν και Νομικά Ζητήματα

- Παράνομες ενέργειες σε δίκτυα (Computer Misuse Act, UK)
- Νομικοί περιορισμοί στην εξαγωγή και χρήση κρυπτογραφικής τεχνολογίας (ΗΠΑ)
- Νομοθεσίες ηλεκτρονικών υπογραφών
- Ηλεκτρονικά «χρήματα»
- Επιχειρηματική αναδιοργάνωση και ο ρόλος του IT Security Manager (Αρχή Προστασίας Δεδομένων)
- Συντονισμός των Αρχών Πιστοποίησης και των Έμπιστων Τρίτων Οντοτήτων
- Νομοθεσία σχετικά με την ιδιωτικότητα
- Φορολόγηση του συναλλαγών ηλεκτρονικού εμπορίου

Κοινωνική Μηχανική

… η διαδικασία της χρήσης κοινωνικών μεθόδων για να πεισθούν κάποιοι να αποκαλύψουν συνθηματικά ή άλλη χρήσιμη πληροφορία σε έναν κακόβουλο χρήστη

Ασφάλεια και Ηλεκτρονικό Επιχειρείν: Περίληψη

Ασφάλεια Δικτύων

- Ηλεκτρονικά αναχώματα
- Δρομολογητές που ελέγχουν την κίνηση των TCP/IP πακέτων
- Πληρεξούσιοι επιπέδου εφαρμογής
- Εικονικά Ιδιωτικά Δίκτυα
- Συστήματα Ανίχνευσης Εισβολών

Ασφάλεια και Ηλεκτρονικό Επιχειρείν: Περίληψη (2)

Ασφάλεια Εφαρμογών

- Ασφαλείς Πληρωμές
  - Secure Electronic Transactions (SET), Secure Socket Layer (SSL)
  - Electronic cash
  - Micropayments
- Προστασία του chip στην έξυπνη κάρτα, ηλεκτρονικά πορτοφόλια
- Προστασία περιεχομένου (digital watermarking)

Άλλα

- Βιομετρική τεχνολογία
- Υποδομή Δημόσιου Κλειδιού
- Άλλα ζητήματα ιδιωτικότητας (remailers, rewebbers, PyTHIA)
- Αντιβιοτικό Λογισμικό
- Νομική προστασία (Προστασία προσωπικών δεδομένων, Ψηφιακές Υπογραφές, Computer Misuse Act)
- ***Ενημερότητα για ζητήματα Ασφαλείας!***

Έρευνα για την Ασφάλεια σε ΜΜΕ στην Ελλάδα (1)

- Σε ερώτηση του αν υπήρξε περιστατικό ασφαλείας στην συγκεκριμένη εταιρεία::
  - 62% απαντήσανε όχι
  - 21% απαντήσανε ναι
  - 16% απαντήσανε «Δεν απαντώ»

- Τα τεχνικά αντίμετρα ασφαλείας έχουν υλοποιηθεί από:
  - Υπαλλήλους της εταιρείας (76%)
  - Εξωτερικούς συμβούλους (24%)

- Λιγότερες από 50% από τις εταιρείες που ερωτήθηκαν έχουν αναπτύξει Σχέδια Συνέχειας της Επιχειρηματικής τους δραστηριότητας

Source: E-business forum, Work cycle B, Task Force TF B1, “Information & Communication Systems Security in e-Business”

Έρευνα για την Ασφάλεια σε ΜΜΕ στην Ελλάδα (2)

- 47% των εταιρειών έχουν επικοινωνήσει με την Αρχή Προστασίας Προσωπικών Δεδομένων σχετικά με θέματα που άπτονται της δραστηριότητας της εταιρείας
- 45% των εταιρειών δήλωσαν ότι ο Ιστοχώρος τους περιέχει μία δήλωση (σεβασμού της) ιδιωτικότητας
- Η μεγάλη πλειοψηφία των εταιρειών δήλωσε ότι πιστεύουν ότι οι φόβοι και οι δισταγμοί που πηγάζουν από τα μέτρα προστασίας των προσωπικών δεδομένων έχουν αποθαρρύνει τους καταναλωτές από το να κάνουν ηλεκτρονικές συναλλαγές.

Source: E-business forum, Work cycle B, Task Force TF B1, “Information & Communication Systems Security in e-Business”

A Survey of E-Payment and M-Payment Systems

Secure Electronic Transaction Protocols

- Visa 3-D Secure international.visa.com/fb/paytech/secure/
- Bank Internet Payment System (BIPS, www.fstc.com)
- Fix (www.fixprotocol.org)
- Homebanking Computer Interface (HBCI, www.hbci.de)
- Open Financial Exchange (www.ofx.net/ofx/default.asp)
- Secure Electronic Transaction (SET, 56www.setco.org)
- Universal Cardholder Authentication Field (UCAF, http://www.mastercardintl.com/newtechnology/ecommercesecurity/spa/ucaf.html)
- Jalda (www.jalda.com)
- Magic Axess (www.magicaxess.com)

Secure Electronic Transaction Protocols (2)

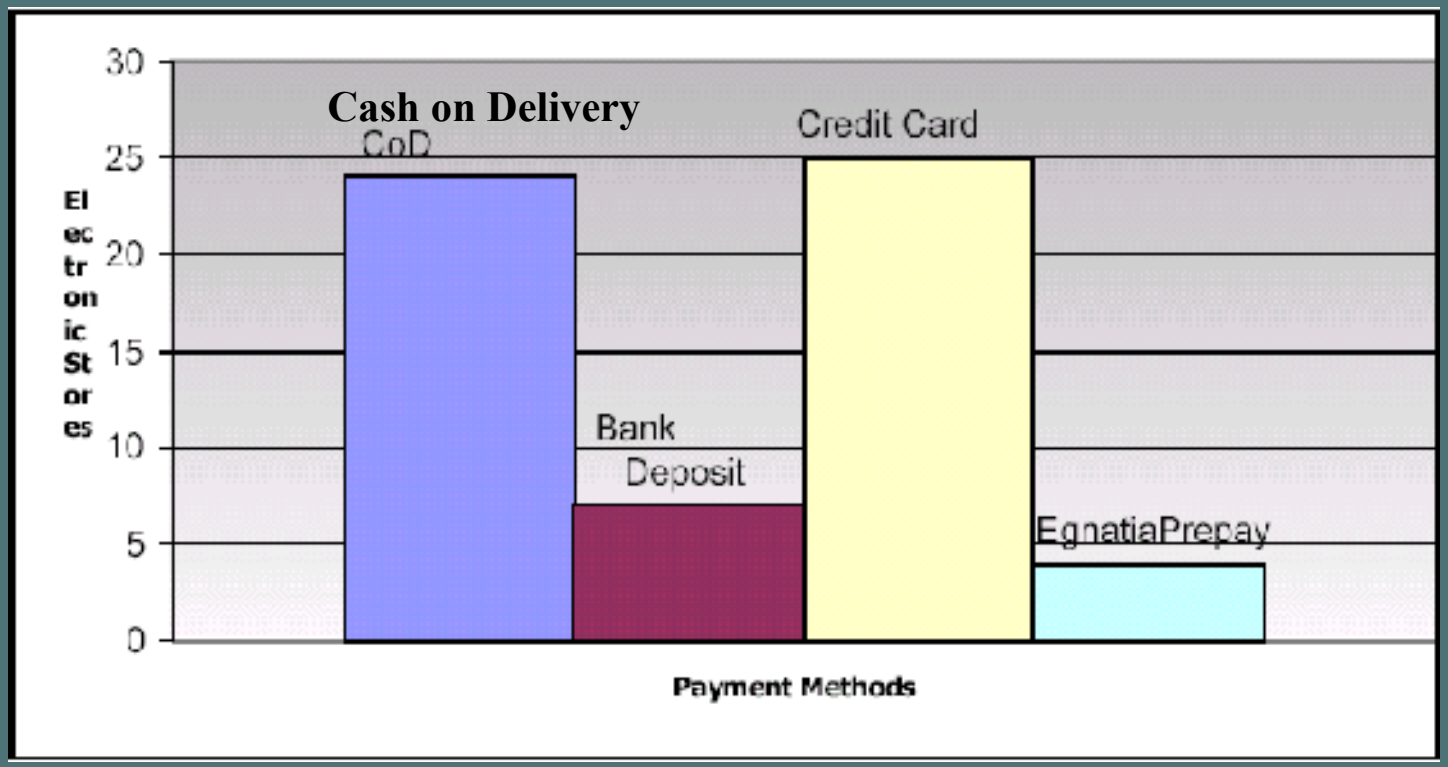
- XMLPay (www.verisign.com/developer/xml/xmlpay.html)
- OBI (Opening Buying on the Internet, www.openbuy.org)
- IOTP (Internet Open Trading Protocol, www.iotp.org/)
- Echeck (www.echeck.org)

Ηλεκτρονικές πληρωμές

«… ο όρος ηλεκτρονικές πληρωμές περιλαμβάνει κάθε πληρωμή σε επιχειρήσεις, τράπεζες ή δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις, η οποία εκτελείται μέσω ενός δικτύου τηλεπικοινωνιών χρησιμοποιώντας σύγχρονη τεχνολογία»

Πηγή : e-Business Forum, Ε΄ Κύκλος Εργασιών, Ομάδα Εργασίας Ε3, Περίληψη των Τελικών Αποτελεσμάτων για τις Ηλεκτρονικές Πληρωμές: Προβλήματα και προοπτικές

E-payments in Greece: a survey



The results in the chart above stem from a study of the Work Group E3, of e-Business forum. The sample data was 30 electronic stores, selling a variety of goods.

E-payment systems

- E-cash payment systems
- Micropayment systems
- Mobile payment systems

E-payment Systems: E-cash payment systems

- Ecash (www.digicash.com)
- CAFÉ (www.semper.org/sirene/projects/cafe/)
- NetCash (www.isi.edu/gost/gost-group/)
- Mondex (www.mondex.com)
- AMADIGI (www.oakington.com/amadigi.htm)
- SmartAxis (www.smartaxis.com)
- Bibit (www.bibit.com)
- CyberCash (www.cybercash.com)

Micropayment Systems

- Millicent (www.millicent.com)
- PayWord (theory.lcs.mit.edu/~cis/pubs/rivest/RivestShamir-mpay.ps)
- MicroMint (theory.lcs.mit.edu/~cis/pubs/rivest/RivestShamir-mpay.ps)
- CEPS (www.ecbs.org)
- CLIP (www.europay.com)
- Visa Cash (international.visa.com/ps/products/vcash/)
- VISA Direct (www.visa.de/presse/presse_15112002.htm)
- Yahoo PayDirect (paydirect.yahoo.com)

MicroPayment Systems (2)

- iPIN (www.ipin.com)
- W-HA (www.w-ha.com)
- WISP (www.trivnet.com)
- Telia PayIT (www.telia.se)
- AvA (www.leskiosques.com/V2/k_webwap/ava/index.htm)
- Cartio MicroPayments (www.cartio.com)
- InternetCash (www.internetcash.com)
- Coulomb IMPS (www.coulomb.co.uk)
- Geldkarte (www.scard.de)
- Proton (www.protonworld.com)

Mobile payment systems

- TELEPAY (www.ertico.com/activiti/projects/telepay/home.htm)
- Sm-PaySoc (www.smpaysoc.org)
- Sonera (www.sonera.fi/english/)
- PayBox (www.paybox.net)
- PayByTel (www.paybytel.net)
- M-pay bill (http://mpay-bill.vodafone.co.uk)
- Mobipay (www.mobipay.com)
- Visa Movíl (www.visa.es)
- Street Cash (www.streetcash.de)

Mobile payment systems (2)

- Safetrader (www.ehpt.com)
- EartPort (www.earthport.com)
- SPA - Secure Payment Application (http://www.mastercardintl.com/spa/)
- EMPS (http://www.nordea.fi/E/Merita/sijoita/uutta/990524.ASP)
- GiSMo (www.gismo.net)
- Fundamo (www.fundamo.com)
- Faircash (www.e-faircash.com)
- eCharge Phone (www.echarge.com)
- Genion m-payment (www.genion.de)

Mobile payment systems (3)

- Easybuy (http://www.gsmagazine.com/timeasybuy.htm)
- NewGenPay (www.newgenpay.com)
- eTopup.com (www.etopup.com)
- MoxMo (www.moxmo.com)
- Beam Trust (www.beamtrust.com)
- i-mode (www.nttdocomo.co.jp/english/p_s/imode/index.html)

Μελέτη Περίπτωσης: Προβλήματα Ασφαλείας στα ATM

Μελέτη Περίπτωσης: Προβλήματα Ασφαλείας στα ATM

Η ενημερότητα σε θέματα Ασφάλειας Πληροφοριών είναι ύψιστης σημασίας. Ακόμα και τα καλύτερα τεχνικά αντίμετρα Ασφαλείας είναι δυνατόν να καμφθούν εξαιτίας του απρόβλεπτου ή μη ενημερωμένου ανθρώπινου παράγοντα

Κοινωνική Μηχανική

- Σε αυτοκόλλητη ταμπέλα που υπήρχε πάνω σε ένα ATM (Maryville, Tennessee, USA, Μάιος 2004) έγραφε: «Εξαιτίας πρόσφατων αποπειρών ηλεκτρονικής απάτης με στόχο πελάτες της Τράπεζας μας, σας ζητάμε να σαρώσετε πρώτα την κάρτα σας στον καρταναγνώστη που βρίσκεται κάτω από την παρούσα ταμπέλα και έπειτα στο ATM, για την δική σας ασφάλεια»,
- Τηλεφωνική επικοινωνία από εκπροσώπους τραπεζικών φορέων, οι οποίοι ζητούν προσωπικά στοιχεία του υποκειμένου για λόγους επαλήθευσης των στοιχείων που τηρούνται στην Τράπεζα,

Μελέτη Περίπτωσης: Προβλήματα Ασφαλείας στα ATM (2)

- Η κάρτα φαίνεται να έχει δεσμευτεί από το ATM (στην πραγματικότητα ένα τμήμα πλαστικού έχει επικολληθεί από κακόβουλο χρήστη μέσα στην σχισμή και αποτρέπει την έξοδο της κάρτας). Καθώς ο πελάτης που χρησιμοποιεί το ATM αποφασίζει να φύγει, ένας περαστικός σταματά και του προσφέρει την βοήθεια του. Ο περαστικός ρωτά τον πελάτη της Τράπεζας το Pin της κάρτας του για να προσπαθήσει να το πληκτρολογήσει ο ίδιος, μήπως βγει η κάρτα. Η κάρτα τελικά δεν εξέρχεται, ο πελάτης φεύγει, και ο κακόβουλος χρήστης φεύγει επίσης, με την κάρτα του νόμιμου πελάτη στα χέρια του.

Μελέτη Περίπτωσης: Προβλήματα Ασφαλείας στα ATM (2)

- Προσοχή σε όσους κοιτάνε πάνω από τον ώμο σας,
- Μικροί σαρωτές καρτών πάνω στην σχισμή κάρτας του ATM (skimming),
- Φυσική βία.

Q&A