ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΕΙΝ
Διάλεξη #8

3/12/2020

Διδάσκουσα: Δρ. Ελένη Καρφάκη
Τμήμα: Ψηφιακών Συστημάτων
2020 – 2021

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020

Περιβάλλον ασφαλείας στο περιβάλλον του ηλεκτρονικού εμπορίου

Δραστηριότητα

- Παρακολουθείστε στο κανάλι μας στο youtube https://www.youtube.com/playlist?list=PLiI8bQQag6UxK7oXhbQkJhwvfBZopNWKj τα βίντεο που έχουν αναρτηθεί από την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος cyberalert.gr

- Επίσης μελετήστε τις συμβουλές του cyberalert.grσχετικά με την προστασία των συναλλαγών ηλεκτρονικού εμπορίου στο διαδίκτυο https://cyberalert.gr/e-commerce/

Στατιστικά κυβερνοεγκλήματος

Έρευνα Ponemon (2017):

- Μέσο ετήσιο κόστος για θύματα κυβερνοεγκλήματος 11,7 εκατ. $ ανά εταιρεία, 22% περισσότερο από το προηγούμενο έτος
- Υψηλότερο κόστος ανά επίθεση για τις αμερικάνικες εταιρείες: 21 εκατ. $
- Το μέσο κόστος ανά επίθεση διαφοροποιείται ανά κλάδο παραγωγής, υψηλότερο στον χρηματοοικονομικό κλάδο (>18 εκατ. $)
- Αύξηση >27% στον αριθμό των επιτυχημένων κυβερνοεπιθέσεων
- Πιο κοστοβόρα ηλεκτρονικά εγκλήματα από επιθέσεις άρνησης υπηρεσίας, κακόβουλα άτομα και κακόβουλο κώδικα

- Έρευνα Accenture (2017) για τους πιο συνηθισμένους τύπους κακόβουλου λογισμικού:
  - Ιοί, σκουλήκια, Δούρειοι Ίπποι που πλήττουν το 98% των επιχειρήσεων της έρευνας
  - Phishing και κοινωνική μηχανική (69%)
  - Επιθέσεις στο Web (67%)
  - Botnet (63%)
  - Κακόβουλος κώδικας (58%)
  - Επιθέσεις άρνησης υπηρεσίας (53%)

Στατιστικά κυβερνοεγκλήματος 2020 και Covid 19

- Το 46% των επιχειρήσεων αντιμετώπισαν απειλή στον κυβερνοχώρο από το lockdown (Barracuda)
- Η Google ανέφερε 18 εκατομμύρια καθημερινά μηνύματα κακόβουλου λογισμικού και ηλεκτρονικού ψαρέματος (phishing) μέσα σε μια εβδομάδα (Google)
- Το έγκλημα στον κυβερνοχώρο αυξήθηκε κατά 86% στην Ινδία από το lockdown (Reuters)
- Οι επιθέσεις στον κυβερνοχώρο σε οργανισμούς υγειονομικής περίθαλψης διπλασιάστηκαν (Crowdstrike)
- Οι χάκερ επιτίθενται κάθε 39 δευτερόλεπτα ή 2.244 φορές την ημέρα (University of Maryland)
- Το μέσο κόστος μιας παραβίασης δεδομένων είναι 3,9 εκατομμύρια $ (IBM)
- Οι ομάδες απόκρισης Cyber Incident μειώνουν το κόστος παραβίασης δεδομένων κατά 360.000 $ (IBM)
- Χρειάζονται 279 ημέρες για να αντιμετωπιστεί μια παραβίαση (IBM)
- Μόνο το 5% των οργανισμών έχει προστατευμένους φακέλους (Varonis)
- 64% των Αμερικανών δεν ξέρουν πώς να χειριστούν μια παραβίαση δεδομένων (Varonis)

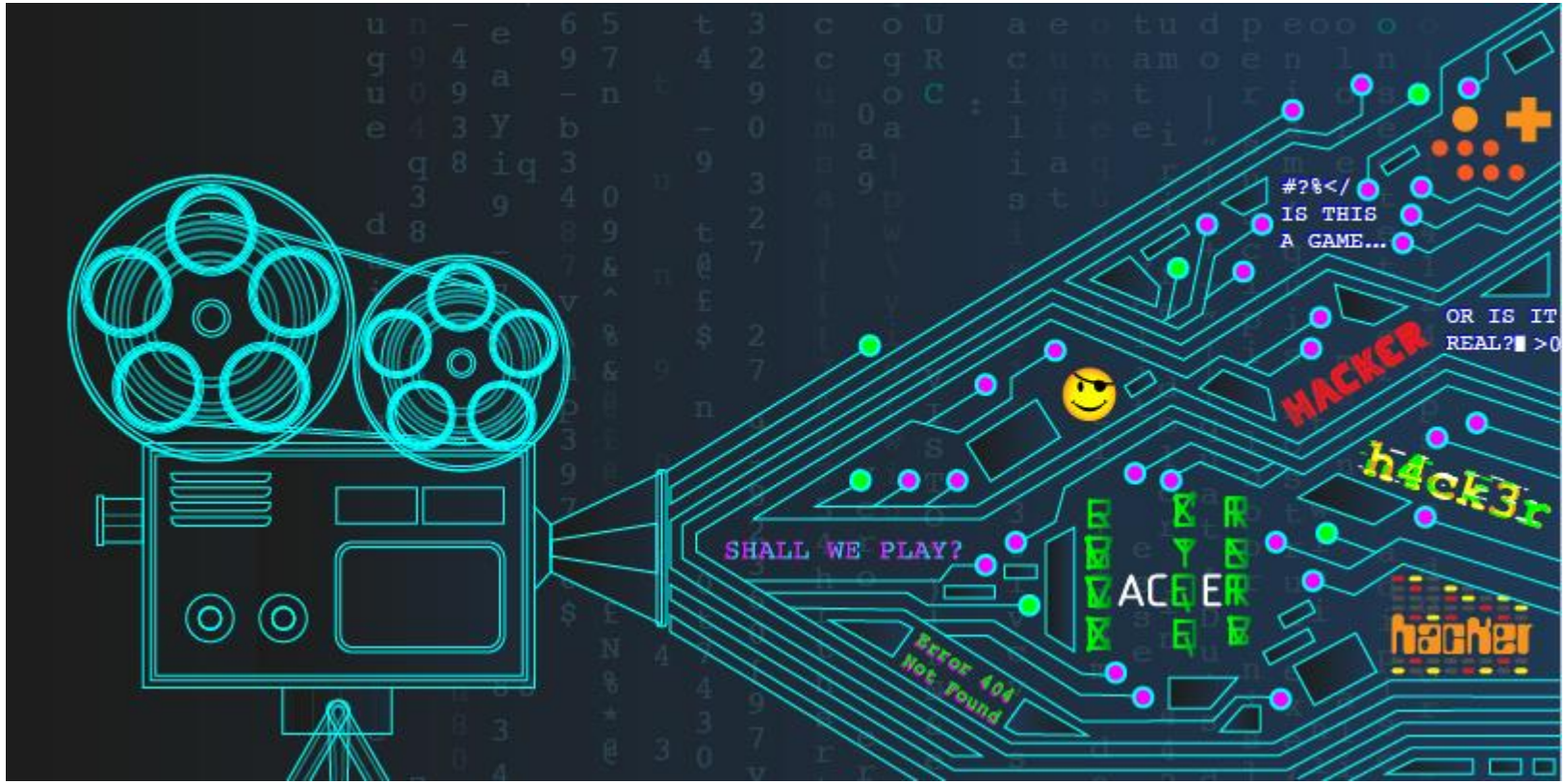
Πηγή: https://c-mric.org/cyber-crime-2020-10-statistics-you-should-know/

Προβλέψεις για το 2021 …

- Το κόστος ζημιών στον κυβερνοχώρο προβλέπεται να φτάσει τα 6 τρισεκατομμύρια δολάρια ετησίως έως το 2021.
- Οι δαπάνες για την ασφάλεια στον κυβερνοχώρο θα υπερβούν το 1 τρισεκατομμύριο δολάρια από το 2017 έως το 2021.
- Ο κόσμος θα έχει 3,5 εκατομμύρια θέσεις εργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο έως το τέλος του 2021.
- Το κόστος βλάβης του Ransomware προβλέπεται να αυξηθεί περισσότερο από 57φορές από το 2015 έως το 2021.
- Το 70% των συναλλαγών κρυπτογράφησης θα είναι για παράνομη δραστηριότητα έως το 2021
- Έως το 2021 περισσότερο από το 70% όλων των συναλλαγών κρυπτογράφησης ετησίως θα αφορούν παράνομη δραστηριότητα, από τις τρέχουσες εκτιμήσεις που κυμαίνονται οπουδήποτε από 20% (από τα 5 κύρια κρυπτονομίσματα) έως σχεδόν 50% (του bitcoin)

Πηγή: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/

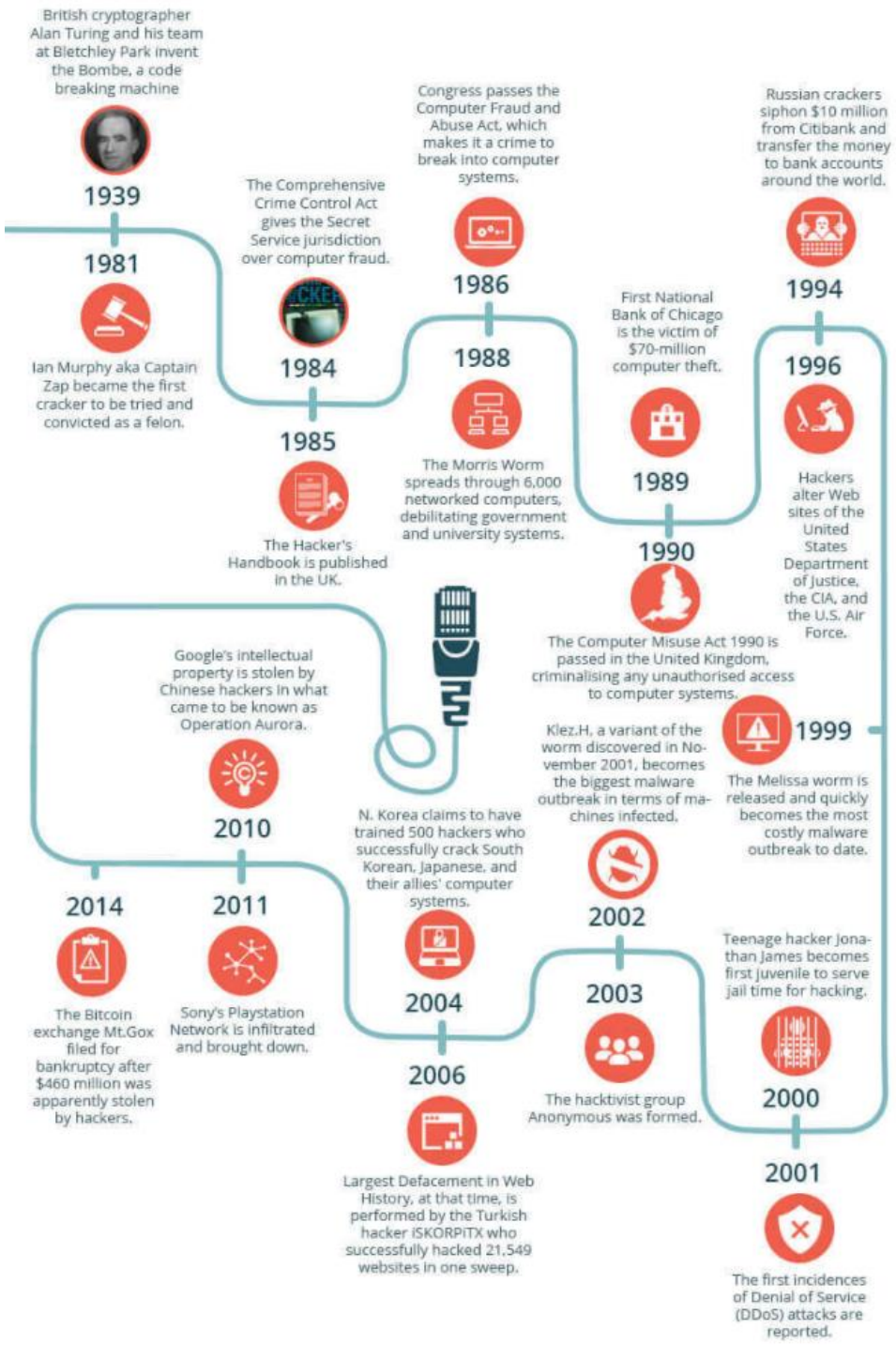
Cine Cyber Security



https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking/

Ιστορία κυβερνοεγκλήματος

- https://eforensicsmag.com/cyber_history/



Βασικές έννοιες

- **Παραοικονομία**: η αξία των κλεμμένων πληροφοριών, οι οποίες αποτελούν ένα είδος νομίσματος.

ΔΕΔΟΜΕΝΑ	ΤΙΜΗ
Αριθμός ατομικής κάρτας ταυτότητας ΗΠΑ μαζί με την ημερομηνία λήξης και τον αριθμό ασφαλείας CVV2 (ο τριψήφιος αριθμός στο πίσω μέρος της κάρτας, αναφέρεται ως CVV)	5-8 δολάρια
Αριθμός ατομικής κάρτας ταυτότητας ΗΠΑ με πλήρη στοιχεία: πλήρες όνομα, διεύθυνση χρέωσης, ημερομηνία λήξης, αριθμός ασφαλείας CVV2, ημερομηνία γέννησης, επώνυμο μητέρας κ.λπ. (αναφέρεται ως Fullz ή Fullzinfo)	20-60 δολάρια
Αποτυπωμένα στοιχεία (dump data) αμερικανικής κάρτας (ο όρος «dump» αναφέρεται σε ανεπεξέργαστα στοιχεία όπως όνομα, αριθμός τραπεζικού λογαριασμού, ημερομηνία λήξης και αριθμός CVV, τα οποία είναι κρυπτογραφημένα στην μαγνητική λωρίδα στο πίσω μέρος της κάρτας)	60-100 δολάρια
Ηλεκτρονικοί λογαριασμοί για πληρωμές στο Internet	20-300 δολάρια
Διαπιστευτήρια σύνδεσης τραπεζικού λογαριασμού	80-700 δολάρια
Διαπιστευτήρια σύνδεσης διαδικτυακού λογαριασμού (Facebook, Twitter, eBay)	10-15 δολάρια
Ιατρικές πληροφορίες/διαπιστευτήρια περίθαλψης	15-20 δολάρια
1.000 διευθύνσεις ηλεκτρονικού ταχυδρομείου	1-10 δολάρια
Σάρωση ενός διαβατηρίου	1-3 δολάρια

Πηγή: **Laudon and Traver (2018)**

Βασικές έννοιες

- **Επίπεδα ασφαλείας στο ηλεκτρονικό εμπόριο**

Διαστάσεις ασφάλειας

ΔΙΑΣΤΑΣΕΙΣ	ΑΠΟ ΤΗΝ ΠΛΕΥΡΑ ΤΟΥ ΠΕΛΑΤΗ	ΑΠΟ ΤΗΝ ΠΛΕΥΡΑ ΤΟΥ ΕΜΠΟΡΟΥ
Ακεραιότητα	Τροποποιήθηκαν οι πληροφορίες κατά τη μεταφορά ή τη λήψη;	Τα δεδομένα στο site τροποποιήθηκαν από κάποιον μη εξουσιοδοτημένο; Μήπως κάποιος μη εξουσιοδοτημένος πελάτης λαμβάνει τα δεδομένα;
Μη αποποίηση	Μπορεί κάποιος που έκανε συναλλαγές μαζί μου να τις αρνηθεί;	Μπορεί ένας πελάτης να αρνηθεί ότι παρήγγειλε προϊόντα;
Αυθεντικοποίηση	Με ποιον συναλλάσσομαι; Πώς μπορώ να ξέρω αν το άτομο ή ο φορέας με τον οποίο συνεργάστηκα είναι αυτός που λέει ότι είναι;	Ποια είναι η πραγματική ταυτότητα του πελάτη;
Εμπιστευτικότητα	Μπορεί κάποιος άλλος από τον προοριζόμενο παραλήπτη να διαβάσει τα μηνύματά μου;	Έχει πρόσβαση άλλος από τον εξουσιοδοτημένο στα μηνύματα ή στα απόρρητα δεδομένα;
Ιδιωτικότητα	Μπορώ να ελέγξω τη χρήση πληροφοριών που αφορούν εμένα και μεταφέρονται σε έναν έμπορο που δραστηριοποιείται στο ηλεκτρονικό εμπόριο;	Πώς μπορούν να χρησιμοποιηθούν τα προσωπικά δεδομένα που συλλέγονται ως μέρος της συναλλαγής ηλεκτρονικού εμπορίου; Οι προσωπικές πληροφορίες για τους πελάτες χρησιμοποιούνται με μη εξουσιοδοτημένο τρόπο;
Διαθεσιμότητα	Μπορώ να έχω πρόσβαση στο site;	Είναι λειτουργικό το site;

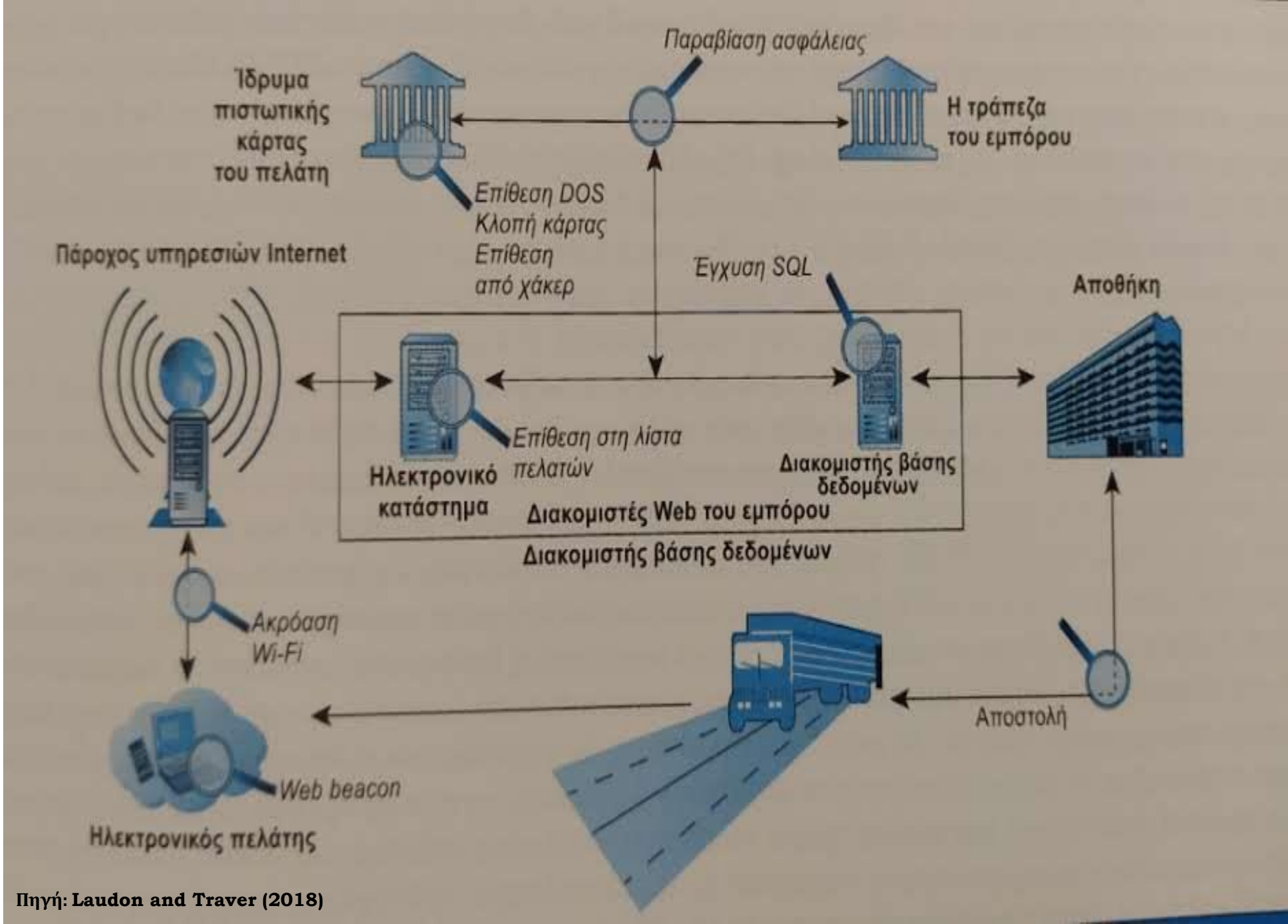
Πηγή: **Laudon and Traver (2018)**

Απειλές ασφαλείας στο ηλεκτρονικό εμπόριο

Απειλές ασφάλειας τυπική συναλλαγή

Πηγή: **Laudon and Traver (2018)**

Απειλές ασφάλειας τρωτά σημεία σε συναλλαγή



Πηγή: **Laudon and Traver (2018)**

Κακόβουλος κώδικας

- **Κακόβουλο λογισμικό**: περιλαμβάνει απειλές όπως ιοί, σκουλήκια, δούρειοι ίπποι και bot
- **Πακέτα προγραμμάτων εκμετάλλευσης τρωτών σημείων**: συλλογές που ενοικιάζονται οι πωλούνται για να εκμεταλλευτούν στόχους ευρείας εφαρμογής Πχ Windows
- **Κακόβουλη διαφήμιση (malvertising)**: διαδικτυακή διαφήμιση που περιέχει κακόβουλο κώδικα
- **Λήψη διέλευσης:** κακόβουλο λογισμικό που συνοδεύει ένα αρχείο το οποίο κατεβάζει ο χρήστης
- **Ιός**: πρόγραμμα υπολογιστή που μπορεί να αντιγράφει ή να δημιουργεί αντίτυπα του εαυτού του και να τα εξαπλώνει σε άλλα αρχεία
- **Σκουλήκι**: κακόβουλο λογισμικό σχεδιασμένο ώστε να εξαπλώνεται από τον ένα υπολογιστή στον άλλο
- **Ransomware:** κακόβουλο λογισμικό που εμποδίζει την πρόσβαση στον υπολογιστή ή τα αρχεία σας και απαιτεί την καταβολή λύτρων

Κακόβουλος κώδικας

- **Δούρειος Ίππος**: φαίνεται ακίνδυνος αλλά κάνει κάτι διαφορετικό από το αναμενόμενο. Είναι το μέσο με το οποίο άλλοι ιοί ή κακόβουλα προγράμματα εισβάλλουν σε συστήματα υπολογιστών
- **Πίσω πόρτα**: χαρακτηριστικό ιών, σκουληκιών και Δούρειων Ίππων που επιτρέπουν στους επιτιθέμενους να προσπελαύνουν εξ αποστάσεως έναν εκτεθειμένο υπολογιστή
- **Bot**: είδος κακόβουλου λογισμικού που μπορεί να εγκατασταθεί κρυφά σε έναν υπολογιστή όταν αυτός συνδέεται στο internet. Από τη στιγμή που θα εγκατασταθεί ανταποκρίνεται σε εξωτερικές εντολές που στέλνει ο επιτιθέμενος
- **Botnet**: δίκτυο μολυσμένων υπολογιστών bot

Διάσημα παραδείγματα κακόβουλου λογισμικού

ΟΝΟΜΑ	ΤΥΠΟΣ	ΠΕΡΙΓΡΑΦΗ
WannaCry	Ransomware / Σκουλήκι	Πρωτοεμφανίστηκε τον Μάιο του 2017. Εκμεταλλεύεται τρωτά σημεία παλαιότερων εκδόσεων λειτουργικών συστημάτων Windows, κρυπτογραφεί δεδομένα και απαιτεί λύτρα για την αποκρυπτογράφηση τους.
Cryptolocker	Ransomware / Δούρειος Ίππος	Υποκλέπτει φωτογραφίες, βίντεο και αρχεία κειμένου του χρήστη, τα κρυπτογραφεί με σχεδόν απρόσβλητη ασύμμετρη κρυπτογράφηση και απαιτεί λύτρα για αυτά.
Citadel	Δούρειος Ίππος /botnet	Παραλλαγή του Δούρειου Ίππου Zeus, εστιάζει στην κλοπή στοιχείων ταυτότητας και σε οικονομικές απάτες. Τα botnet που εξαπλώνουν το Citadel αποτέλεσαν στόχους της σύμπραξης Microsoft/FBI το 2012.
Zeus	Δούρειος Ίππος /botnet	Μερικές φορές αναφέρεται ως ο βασιλιάς του οικονομικού κακόβουλου λογισμικού. Μπορεί να εγκατασταθεί μέσω λήψης με διέλευση και αποφεύγει τον εντοπισμό αναλαμβάνοντας τον έλεγχο του προγράμματος περιήγησης και υποκλέπτοντας δεδομένα τα οποία ανταλλάσσονται με τους διακομιστές των τραπεζών.
Reventon	Ransomware Σκουλήκι / Δούρειος Ίππος	Βασίζεται στους Citadel/Zeus. Κλειδώνει τους υπολογιστές και εμφανίζει προειδοποιήσεις από τοπικές αστυνομικές αρχές για διάπραξη παράνομων δραστηριοτήτων στον υπολογιστή και απαιτεί πληρωμή προστίμου για να τον ξεκλειδώσει.
Ramnit	Δούρειος Ίππος / botnet	Μία από τις εν ενεργεία κυριάρχες οικογένειες κακόβουλου κώδικα. Λειτουργεί από το 2010 αλλά σχεδόν εξαφανίστηκε το 2015 μετά την απομάκρυνση του botnet που το είχε διαδώσει. Ξαναεμφανίστηκε το 2016 για να γίνει ένας από τους ευρύτερα διαδεδομένους Δούρειους ίππους με επιθέσεις στοχευμένες στον οικονομικό τομέα.
Conficker	Σκουλήκι	Πρωτοπαρουσιάστηκε τον Νοέμβριο του 2008. Στοχεύει το λειτουργικό σύστημα της Microsoft. Χρησιμοποιεί προηγμένες τεχνικές κακόβουλου κώδικα. Η μεγαλύτερη προσβολή από σκουλήκι μετά το Slammer το 2003.
Netsky.P	Σκουλήκι/ Δούρειος Ίππος	Πρωτοεμφανίστηκε στις αρχές του 2003 και εξακολουθεί να είναι από τα πιο συνηθισμένα σκουλήκια. Διαδίδεται συλλέγοντας διευθύνσεις e-mail από τους υπολογιστές που μολύνει και στέλνοντας e-mail σε όλους τους αποδέκτες από τον μολυσμένο υπολογιστή. Χρησιμοποιείται συνήθως από bot δίκτυα για να διαδώσει spam και επιθέσεις άρνησης υπηρεσίας.
Storm (Peacomm, NuWar)	Σκουλήκι/ Δούρειος Ίππος	Πρωτοεμφανίστηκε το 2007. Διαδίδεται όπως το σκουλήκι Netsky.P. Μπορεί επίσης να ληφθεί και να εκτελέσει άλλα προγράμματα Δούρειου Ίππου και σκουλήκια.
Nymex	Σκουλήκι	Πρωτοεμφανίστηκε το 2006. Διαδίδεται με ομαδική αλληλογραφία. Ενεργοποιείται κάθε 3η του μηνός και προσπαθεί να καταστρέψει συγκεκριμένα αρχεία.
Zotob	Σκουλήκι	Πρωτοεμφανίστηκε το 2005. Γνωστό σκουλήκι που μόλυνε πολλές αμερικανικές διαφημιστικές εταιρείες.
Mydoom	Σκουλήκι	Πρωτοεμφανίστηκε το 2004. Ένα από τα πιο γρήγορα μεταδιδόμενα σκουλήκια ομαδικής αλληλογραφίας.
Slammer	Σκουλήκι	Παρουσιάστηκε το 2003. Προκάλεσε πολλά προβλήματα.
CodeRed	Σκουλήκι	Εμφανίστηκε το 2001. Κατάφερε να μολύνει πάνω από 20.000 υπολογιστές εντός 10 λεπτών από τη στιγμή που εξαπολύθηκε και διαδόθηκε τελικά σε εκατοντάδες χιλιάδες συστήματα.
Melissa	Ιός μακροεντολών/ Σκουλήκι	Εντοπίστηκε αρχικά το 1999. Ήταν το πιο ταχέως διαδιδόμενο επιβλαβές πρόγραμμα. Μόλυνε το πρότυπο Normal.dot του Microsoft Word και έτσι μόλυνε όλα τα έγγραφα που είχαν δημιουργηθεί πρόσφατα. Επίσης έστειλε με e-mail ένα μολυσμένο αρχείο Word στις πρώτες 50 εγγραφές του βιβλίου διευθύνσεων του Microsoft Outlook κάθε χρήστη.

Πηγή: **Laudon and Traver (2018)**

Ανεπιθύμητα προγράμματα

- **Ανεπιθύμητα προγράμματα**: Προγράμματα που εγκαθίστανται μόνα τους σε υπολογιστή συνήθως χωρίς την συγκατάθεση του χρήστη
- **Adware**: ένα ανεπιθύμητο πρόγραμμα που εμφανίζει αναδυόμενες διαφημίσεις στον υπολογιστή σας
- **Παράσιτο προγράμματος περιήγησης**: ένα πρόγραμμα που μπορεί να παρακολουθεί και να αλλάζει τις ρυθμίσεις του προγράμματος περιήγησης του χρήστη πχ αλλάζοντας την αρχική σελίδα του
- **Spyware**: πρόγραμμα που χρησιμοποιείται για την άντληση πληροφοριών όπως τα πλήκτρα που πατά ο χρήστης, αντίγραφα μηνυμάτων ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων κ.ο.κ.

Phishing

- **Κοινωνική μηχανική**: εκμετάλλευση της ευπιστίας των ανθρώπων για διανομή κακόβουλου λογισμικού
- **Ψάρεμα (Phishing)**: κάθε παραπλανητική προσπάθεια που γίνεται στο internet από κάποιον τρίτο για να αντλήσει απόρρητες πληροφορίες για οικονομικό όφελος
- **E-mail τύπου «επιστολή από τη Νιγηρία»**: scam (πλαστό μήνυμα ηλεκτρονικού ταχυδρομείου) του τύπου θα κερδίσετε χρήματα αν δώσετε τον αριθμό τραπεζικού λογαριασμού
- **Ψάρεμα BEC:** παραλλαγή της Νιγηριανής απάτης, κατά την οποία ο επιτιθέμενος εμφανίζεται ως υψηλόβαθμο στέλεχος μιας επιχείρησης και ζητά από άλλον υπάλληλο να μεταφέρει χρηματικά ποσά σε πλαστούς λογαριασμούς

Πηγή: **Laudon and Traver (2018)**

Hacking

- **Hacker**: το άτομο που αποσκοπεί στο να αποκτήσει χωρίς έγκριση πρόσβαση σε ένα σύστημα υπολογιστή
- **Cracker**: μέσα στην κοινότητα των χάκερ ο όρος αυτός χρησιμοποιείται για να δηλώσει έναν χάκερ με παράνομες προθέσεις
- **Κυβερνοβανδαλισμός:** η εσκεμμένη διατάραξη, η αλλαγή της αρχικής σελίδας ή η καταστροφή του site
- **Hacktivism:** βανδαλισμός στο internet και κλοπή δεδομένων για πολιτικούς σκοπούς
- **White hat:** καλοί χάκερ που βοηθούν διάφορους φορείς να εντοπίσουν και να επιδιορθώσουν τα κενά ασφαλείας
- **Black hat:** χάκερ που εμπλέκονται σε συναφείς δραστηριότητες αλλά χωρίς να πληρώνονται ή να προσλαμβάνονται από τον φορέα-στόχο και έχουν κακές προθέσεις
- **Grey hat:** χάκερ που πιστεύουν ότι κάνουν κακό επειδή σπάνε και αποκαλύπτουν τα κενά του συτήματος

Διαρροές δεδομένων

- **Διαρροή δεδομένων (data breach):** συμβαίνει όταν ένας οργανισμός χάνει τον έλεγχο των πληροφοριών του από αγνώστους

Απάτη/κλοπή πιστωτικών καρτών

- Μία από τις πιο επικίνδυνες μορφές κλοπής στο Internet για την αντιμετώπιση της οποίας οι ηλεκτρονικοί έμποροι έχουν αναπτύξει διάφορες τεχνικές:
  - Χρήση εργαλείων αυτόματης ανίχνευσης απάτης
  - Χειροκίνητη εξέταση παραγγελιών
  - Απόρριψη ύποπτων παραγγελιών
  - Απαίτηση επιπρόσθετων επιπέδων ασφαλείας για email, CCV κοκ

Κλοπή ταυτότητας

- Περιλαμβάνει τη μη εξουσιοδοτημένη χρήση προσωπικών δεδομένων άλλου ατόμου για παράνομα οικονομικά οφέλη

Spoofing, pharming & spam

- **Παραπλάνηση (spoofing)**: η προσποίηση κάποιου ότι είναι κάποιος άλλος χρησιμοποιώντας πλαστές διευθύνσεις email ή IP
- **Pharming**: αυτόματη ανακατεύθυνση ενός συνδέσμου σε άλλη διεύθυνση σε ένα site που προσποιείται ότι είναι σκόπιμος προορισμός
- **Spam website**: αναφέρεται επίσης ως φάρμα συνδέσμων και υπόσχεται την παροχή προϊόντων ή υπηρεσιών, αλλά στην πραγματικότητα είναι απλώς συλλογές διαφημίσεων

Επιθέσεις υποκλοπής και ενδιάμεσων ατόμων

- Sniffer: προγράμματα ιχνηλάτησης που παρακολουθούν τις πληροφορίες που διακινούνται σε ένα δίκτυο
- Επίθεση ενδιάμεσου ατόμου (man in the middle): επίθεση κατά την οποία ο επιτιθέμενος είναι σε θέση να αναχαιτίσει επικοινωνίες μεταξύ δύο μερών που επικοινωνούν απευθείας μεταξύ τους όταν στην πραγματικότητα ο έλεγχος της επικοινωνίας γίνεται από τον επιτιθέμενο

DOS & DDOS

- DOS (Denial of Service): επίθεση άρνησης υπηρεσίας όπου συμβαίνει υπερφόρτωση ενός Website με άχρηστη κυκλοφορία ώστε να΄κατακλυστεί ή να υπερχειλιστεί το δίκτυο
- DDOS (Distributed Denial of Service): επίθεση κατανεμημένης άρνησης υπηρεσίας όπου χρησιμοποιεί πολλούς υπολογιστές για να σημειωθεί σε ένα δίκτυο-στόχο από αμέτρητα σημεία επίθεσης

Επιθέσεις εκ των έσω

- Οι μεγαλύτερες οικονομικές απειλές δεν προέρχονται από έξω αλλά από την εσωτερική κατάχρηση μέσω:
  - Διακοπές υπηρεσιών
  - Καταστροφή site
  - Κλοπές στοιχείων για πιστωτικές κάρτες και προσωπικά δεδομένα πελατών

- IBM Security (2017): στους κλάδους των χρηματοοικονομικών υπηρεσιών και της ιατρικής περίθαλψης για το 2016 υπήρχαν μεγαλύτερα ποσοστά επιθέσεων από ενέργειες εκ των έσω

Κακά σχεδιασμένο λογισμικό

- **Επίθεση έγχυσης κώδικα SQL**: εκμεταλλεύεται κακά σχεδιασμένο λογισμικό εφαρμογών Web που δεν καταφέρνει να επαληθεύσει σωστά ή να φιλτράρει δεδομένα που εισάγει ένας χρήστης σε μια ιστοσελίδα
- **Τρωτό σημείο μηδενικής ημέρας**: τρωτό σημείο λογισμικού που δεν έχει αναφερθεί προηγουμένως και για το οποίο δεν υπάρχει ακόμη διόρθωση
- **Heartbleed bug:** ατέλεια στο σύστημα κρυπτογράφησης OpenSSL που επέτρεπε σε χάκερ να αποκρυπτογραφούν συνόδους SSL και να ανακαλύπτουν ονόματα χρηστών, κωδικούς πρόσβασης και άλλα στοιχεία χρηστών.

Θέματα ασφαλείας στα κοινωνικά δίκτυα

- Ιδιαίτερα προσφιλή μέσα σε κάθε είδους ζητήματα ασφαλείας
- Τεχνικές επίθεσης:
  - **Χειροκίνητη κοινοχρησία**, όταν μοιραζόμαστε άθελά μας κακόβουλο περιεχόμενο ενώ αναζητούμε προσφορές και δωρεάν παροχές στο διαδίκτυο
  - **Πλαστά κουμπιά αντίδρασης**, με το πάτημα των οποίων εγκαθίστανται κακόβουλα προγράμματα και αναρτώνται ενημερώσεις στο χρονολόγιο που εξαπλώνουν ουσιαστικά την επίθεση

Θέματα ασφαλείας πλατφόρμας φορητότητας

- Εντεινόμενα ζητήματα ακόμη και για πολύ επώνυμες εταιρείες (πχ Starbucks app)
- Τεχνικές επιθέσεων:
  - **Vishing**: στοχεύουν σε εύπιστους χρήστες κινητών με φωνητικά μηνύματα που τους προτρέπουν να καλέσουν ένα συγκεκριμένο αριθμό για πχ μια φιλανθρωπική δωρεά
  - **Smishing**: εκμεταλλεύονται τα μηνύματα SMS αποκρύπτοντας το τηλέφωνο του αποστολέα
  - **Madware**: εφαρμογές που δείχνουν αθώες αλλά περιέχουν adware που εμφανίζουν αναδυόμενες διαφημίσεις και μηνύματα κειμένου

Θέματα ασφαλείας στο Cloud

- Όσο όλο και περισσότερες εταιρείες θα βασίζονται στο cloud, τόσο θα αυξάνονται και
  - Οι απειλές από επιθέσεις DDOS
  - Οι επιθέσεις κατά εφαρμογών Web (κυρίως έγχυσης SQL)
  - Παράδειγμα η υποκλοπή φωτογραφιών της Jennifer Lawrence μέσω του iCloud της Apple

Θέματα ασφαλείας στο IoT

ΠΡΟΚΛΗΣΗ	ΠΙΘΑΝΕΣ ΣΥΝΕΠΕΙΕΣ
Πολλές συσκευές IoT, όπως οι αισθητήρες, προορίζονται για εφαρμογή σε μεγαλύτερη κλίμακα συγκριτικά με τις παραδοσιακές συσκευές που συνδέονται στο Internet, δημιουργώντας μία τεράστια ποσότητα εκμεταλλεύσιμων διασυνδεδεμένων συνδέσμων.	Υπάρχοντα εργαλεία, μέθοδοι και στρατηγικές πρέπει να αναπτυχθούν ώστε να αντιμετωπιστεί αυτή η δίχως προηγούμενο κλίμακα.
Πολλές περιπτώσεις IoT αποτελούνται από συλλογές από πανομοιότυπες συσκευές οι οποίες έχουν τα ίδια χαρακτηριστικά.	Μεγεθύνει τον πιθανό αντίκτυπο μίας αδυναμίας στο σύστημα ασφαλείας.
Πολλές συσκευές IoT αναμένεται να έχουν μεγαλύτερη διάρκεια ζωής από τον τυπικό εξοπλισμό.	Η διάρκεια ζωής αυτών των συσκευών θα μπορούσε να ξεπεράσει αυτή των κατασκευαστών τους, κάτι που θα τις άφηνε χωρίς υποστήριξη και θα δημιουργούσε συνεχώς αδυναμίες.
Πολλές συσκευές IoT σχεδιάζονται έτσι ώστε να μην μπορούν να αναβαθμιστούν ή η αναβάθμιση τους είναι δύσκολη.	Εγείρει τη πιθανότητα να μην (μπορούν να) επισκευάζονται οι ευάλωτες συσκευές και να παραμένουν ευάλωτες για όλη τη διάρκεια ζωής τους.
Πολλές συσκευές IoT δεν επιτρέπουν στον χρήστη να δει το τρόπο λειτουργίας τους ή τα δεδομένα που παράγουν, ούτε τον ειδοποιούν όταν προκύπτει κάποιο πρόβλημα στην ασφάλεια.	Οι χρήστες θεωρούν ότι η συσκευή IoT λειτουργεί κανονικά ενώ στην πραγματικότητα μπορεί να λειτουργεί με κακόβουλο τρόπο.
Μερικές συσκευές IoT, όπως οι αισθητήρες, είναι τόσο διακριτικά τοποθετημένες στο περιβάλλον που ο χρήστης, πιθανώς, να μην αντιλαμβάνεται την παρουσία τους.	Μία πιθανή παραβίαση της ασφάλειας μπορεί να επιμείνει για αρκετή ώρα πριν γίνει αντιληπτή.

Πηγή: Laudon and Traver (2018)

Δραστηριότητα

- Πιστεύετε ότι το smartphone σας είναι ασφαλές;
- Μελετήστε την σχετική μελέτη περίπτωσης που έχει αναρτηθεί στην Eclass προκειμένου να απαντήσετε.

Τεχνολογικές λύσεις

Εργαλεία για επίτευξη ασφάλειας

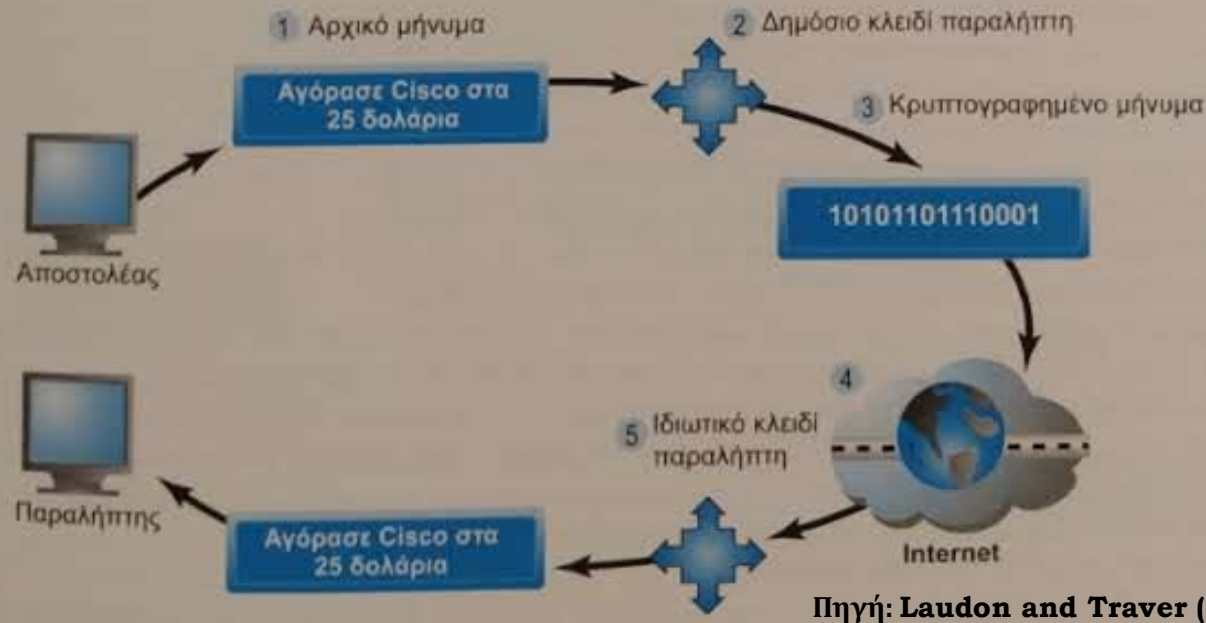
Πηγή: **Laudon and Traver (2018)**

Κρυπτογραφία

- Κρυπτογραφία: διαδικασία τροποποίησης ενός απλού κειμένου ή δεδομένων σε κρυπτογραφημένο κείμενο που δεν μπορεί να διαβαστεί από κανέναν άλλο παρά από τον αποστολέα και τον παραλήπτη
- Σκοπός: να διασφαλίσει αποθηκευμένες πληροφορίες και να διασφαλίσει τη μεταφορά των πληροφοριών
- Πολύ σημαντική γιατί καλύπτει 4 στις 6 βασικές διαστάσεις ασφαλείας στο ηλεκτρονικό εμπόριο:
  - Ακεραιότητα μηνύματος
  - Μη αποκήρυξη
  - Αυθεντικοποίηση
  - Εμπιστευτικότητα

Κρυπτογράφηση δημοσίου κλειδιού – απλό παράδειγμα

ΒΗΜΑ	ΠΕΡΙΓΡΑΦΗ
1. Ο αποστολέας δημιουργεί ένα ψηφιακό μήνυμα.	Το μήνυμα μπορεί να είναι έγγραφο, υπολογιστικό φύλλο ή οποιοδήποτε ψηφιακό αντικείμενο.
2. Ο αποστολέας λαμβάνει το δημόσιο κλειδί του παραλήπτη από ένα δημόσιο κατάλογο και το εφαρμόζει στο μήνυμα.	Τα δημόσια κλειδιά διανέμονται ευρέως και μπορούν να αποκτηθούν απευθείας από τους παραλήπτες.
3. Η εφαρμογή του κλειδιού του παραλήπτη παράγει ένα κρυπτογραφημένο μήνυμα.	Από τη στιγμή που θα κρυπτογραφηθεί με το δημόσιο κλειδί, το μήνυμα δεν μπορεί να χρησιμοποιηθεί αντίστροφα για αποκρυπτογράφηση ή να αποκρυπτογραφηθεί με το ίδιο δημόσιο κλειδί. Η διαδικασία είναι μη αναστρέψιμη.
4. Το κρυπτογραφημένο μήνυμα στέλνεται στο Internet.	Το κρυπτογραφημένο μήνυμα «σπάει» σε πακέτα και στέλνεται μέσω διαφορετικών οδών, καθιστώντας δύσκολη (όχι όμως αδύνατη) την υποκλοπή ολόκληρου του μηνύματος.
5. Ο παραλήπτης χρησιμοποιεί το ιδιωτικό κλειδί του για να αποκρυπτογραφήσει το μήνυμα.	Το μόνο άτομο που μπορεί να αποκρυπτογραφήσει το μήνυμα είναι αυτό που κατέχει το ιδιωτικό κλειδί του παραλήπτη. Ευελπιστούμε, βέβαια, ότι αυτός είναι και ο νόμιμος παραλήπτης.



Πηγή: **Laudon and Traver (2018)**

Κρυπτογραφία

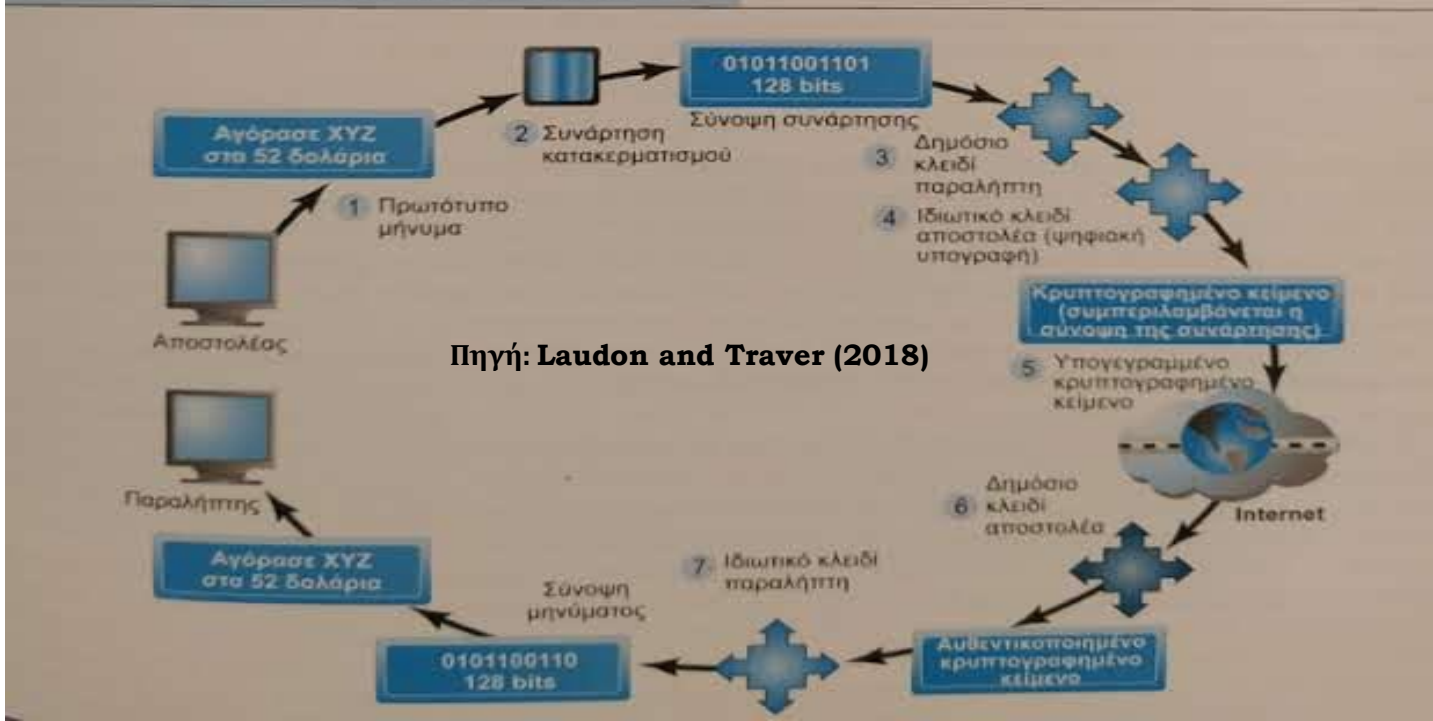
- Μέθοδοι:
  - Cipher: κλειδί, μέθοδος μετασχηματισμού απλού κειμένου σε κρυπτογραφημένο μήνυμα
  - Κρυπτογράφημα αντικατάστασης: κάθε γράμμα αντικαθίσταται συστηματικά από ένα άλλο
  - Κρυπτογράφημα αντιμετάθεσης: η σειρά των γραμμάτων σε κάθε λέξη τροποποιείται με συστηματικό τρόπο
  - Κρυπτογράφηση συμμετρικού κλειδιού: αποστολέας και παραλήπτης χρησιμοποιούν το ίδιο κλειδί για να (απο)κρυπτογραφήσουν και μήνυμα
  - Κρυπτογράφηση δημοσίου κλειδιού: χρησιμοποιούνται δύο μαθηματικά συναφή ψηφιακά κλειδιά, ένα δημόσιο το οποίο μεταδίδεται ευρέως και ένα ιδιωτικό, το οποίο παραμένει μυστικό στον ιδιοκτήτη, και χρησιμοποιούνται για την κρυπτογράφηση ή αποκρυπτογράφηση του μηνύματος
  - Κρυπτογράφηση δημοσίου κλειδιού με ψηφιακές υπογραφές και σύνοψη κατακερματισμού: συμπληρώνει τα κενά ασφαλείας του προηγούμενου
  - Ψηφιακοί φάκελοι: τεχνική που χρησιμοποιεί τη συμμετρική (από)κρυπτογράφηση δημοσίου κλειδιού για την κρυπτογράφηση και αποστολή του συμμετρικού κλειδιού

Κρυπτογραφία

- Μέθοδοι:
  - Ψηφιακά πιστοποιητικά: ψηφιακά έγγραφα που παρέχονται από κάποιον διαπιστευμένο τρίτο (Αρχή Πιστοποίησης) που περιέχει μια ποικιλία πληροφοριών ταυτοποίησης, όπως η ταυτότητα για ένα φυσικό πρόσωπο
  - Υποδομή δημόσιου κλειδιού: διαδικασίες αρχών πιστοποίησης και ψηφιακών πιστοποιητικών τις οποίες αποδέχονται όλα τα συμβαλλόμενα
  - Pretty Good Privacy: πρόγραμμα λογισμικού κρυπτογράφησης δημοσίου κλειδιού για email
  - OpenPGP: ανοικτό πρωτόκολλο βάσει του παραπάνω

Κρυπτογράφηση δημοσίου κλειδιού – ψηφιακές υπογραφές

ΒΗΜΑ	ΠΕΡΙΓΡΑΦΗ
1. Ο αποστολέας δημιουργεί ένα πρωτότυπο μήνυμα.	Το μήνυμα θα μπορούσε να είναι ψηφιακό αρχείο.
2. Ο αποστολέας εφαρμόζει μία συνάρτηση κατακερματισμού παράγοντας μία σύνοψη με 128 bit.	Οι συναρτήσεις κατακερματισμού δημιουργούν μία μοναδική σύνοψη του μηνύματος με βάση τα περιεχόμενα του μηνύματος.
3. Ο αποστολέας κρυπτογραφεί το μήνυμα και το αποτέλεσμα κατακερματισμού με το δημόσιο κλειδί του παραλήπτη.	Αυτή η μη αναστρέψιμη διαδικασία δημιουργεί ένα κρυπτογραφημένο κείμενο που μπορεί να διαβαστεί μόνο από τον παραλήπτη με το ιδιωτικό κλειδί του.
4. Ο αποστολέας κρυπτογραφεί το αποτέλεσμα, χρησιμοποιώντας και πάλι το ιδιωτικό κλειδί του.	Το ιδιωτικό κλειδί του αποστολέα είναι μία ψηφιακή υπογραφή. Υπάρχει μόνο ένα άτομο που θα μπορούσε να δημιουργήσει αυτό το ψηφιακό σημάδι.
5. Το αποτέλεσμα αυτής της διπλής κρυπτογράφησης στέλνεται στο Internet.	Το μήνυμα διασχίζει το Internet σαν μία σειρά ανεξάρτητων πακέτων.
6. Ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να πιστοποιήσει το μήνυμα.	Μόνο ένα άτομο θα μπορούσε να στείλει αυτό το μήνυμα, ο αποστολέας.
7. Ο παραλήπτης χρησιμοποιεί το ιδιωτικό κλειδί του για να αποκρυπτογραφήσει τη συνάρτηση κατακερματισμού και το πρωτότυπο μήνυμα. Ο αποδέκτης ελέγχει ότι το πρωτότυπο μήνυμα και τα αποτελέσματα από τη συνάρτηση κατακερματισμού συμφωνούν μεταξύ τους.	Η συνάρτηση κατακερματισμού χρησιμοποιείται εδώ για τον έλεγχο του πρωτότυπου μηνύματος. Αυτό διασφαλίζει ότι το μήνυμα δεν τροποποιήθηκε κατά τη μεταφορά.



Πηγή: Laudon and Traver (2018)

Διασφάλιση καναλιών επικοινωνίας

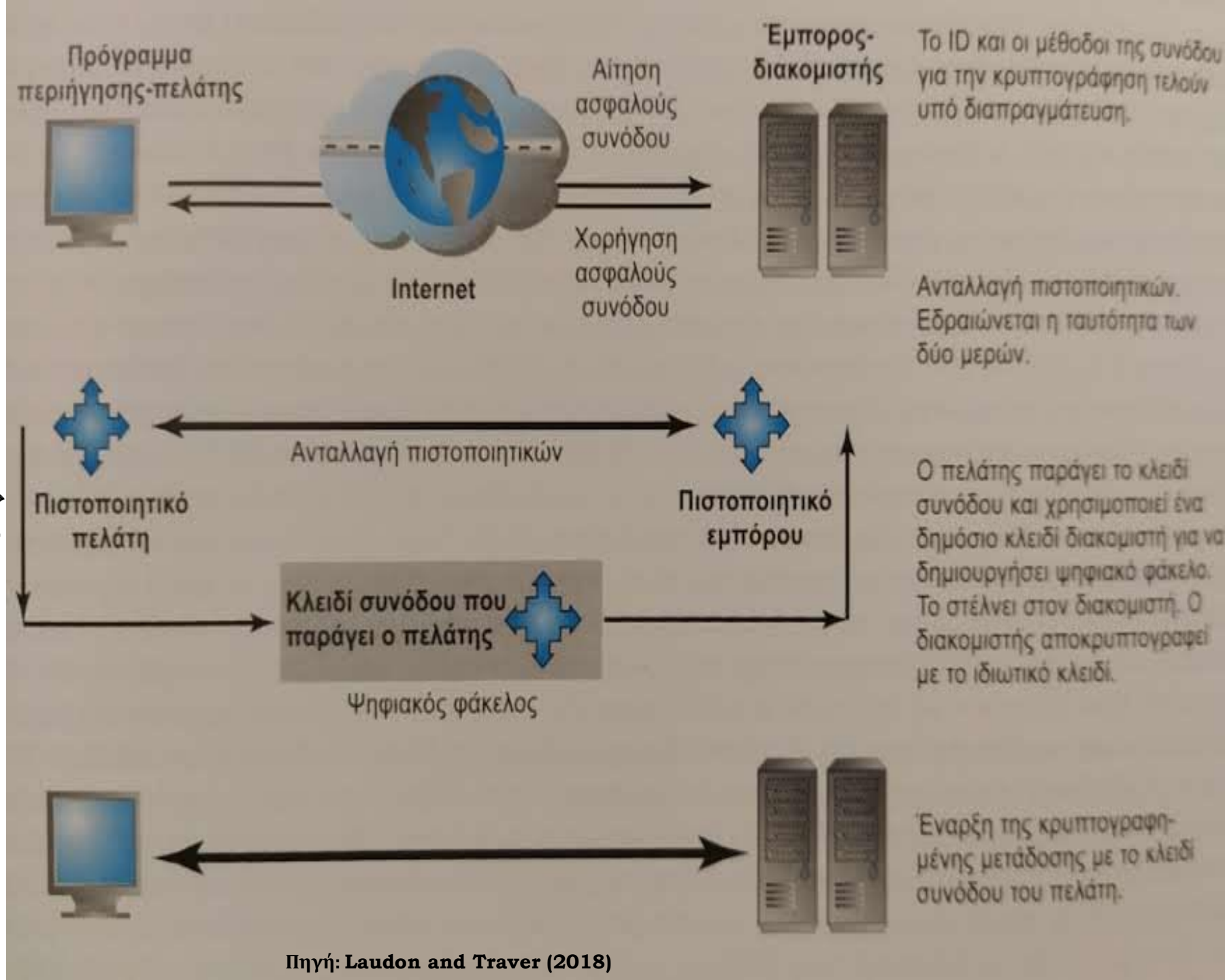
- Πρωτόκολλα SSL (Secure Sockets Layer)
- Πρωτόκολλα TLS (Transport Layer Security)

Ασφαλής σύνοδος διαπραγμάτευσης όπου το URL, το περιεχόμενο και τα cookies είναι κρυπτογραφημένα

➢ Τα URL αλλάζουν από HTTP σε HTTPS

- Εικονικό ιδιωτικό δίκτυο (VPN): για ασφαλή απομακρυσμένη πρόσβαση
- WPA2: πρότυπο ασύρματης ασφάλειας για WiFi

Διασφάλιση καναλιών επικοινωνίας

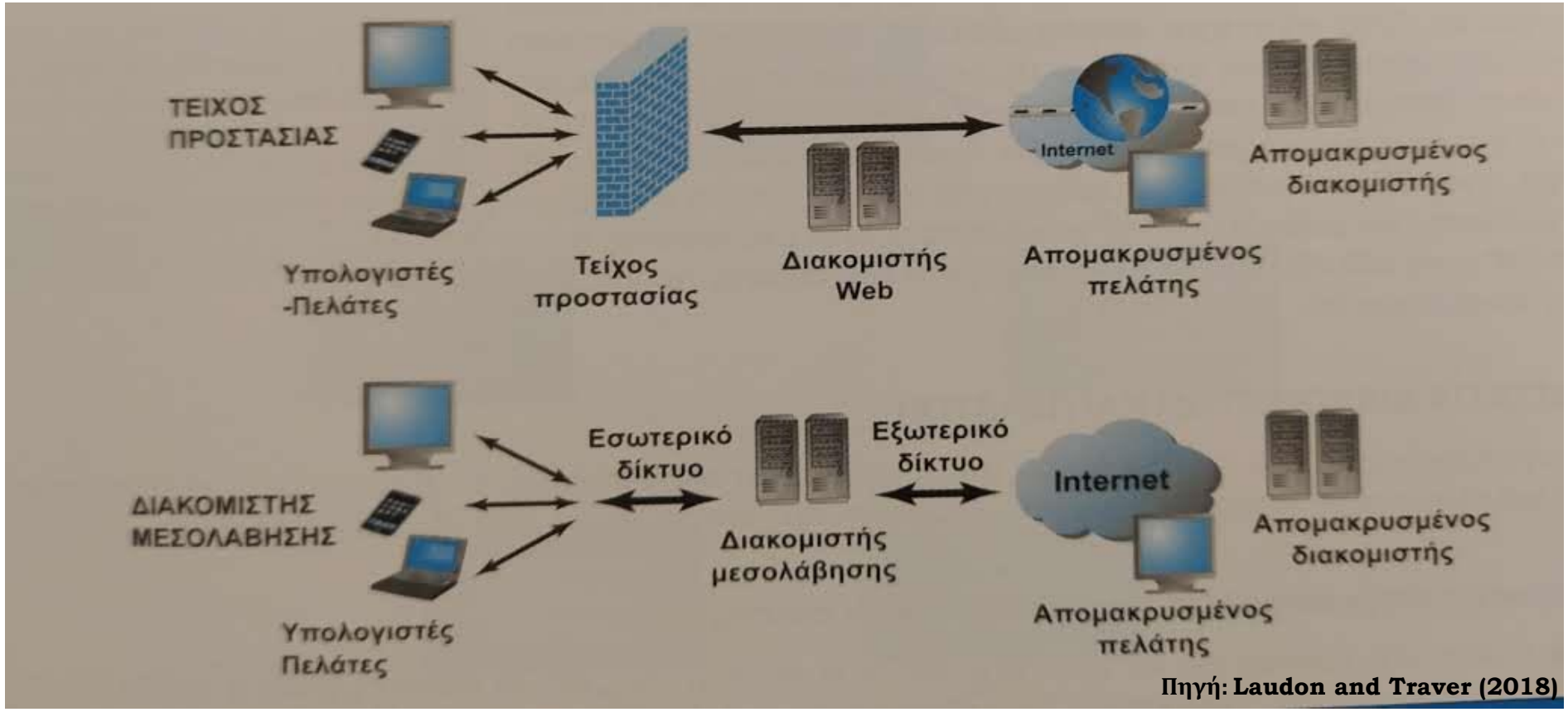


Πηγή: **Laudon and Traver (2018)**

Προστασία δικτύων

- Τείχος προστασίας: υλικό ή λογισμικό που φιλτράρει τα πακέτα επικοινωνίας και εμποδίζει την είσοδο σύμφωνα με μια πολιτική ασφαλείας
- Διακομιστής μεσολάβησης (proxy): διακομιστής λογισμικού που χειρίζεται όλες τις επικοινωνίες που προέρχονται ή στέλνονται στο internet, λειτουργώντας σαν σωματοφύλακας της επιχείρησης
- Συστήματα ανίχνευσης και παρεμπόδισης εισβολής (IDS): εξετάζουν την κυκλοφορία εξετάζοντας την ύπαρξη μοτίβων που συνιστούν επίθεση
- Σύστημα παρεμπόδισης εισβολής (IPS): όπως το προηγούμενο συν την ανάληψη δράσης για την αποτροπή και τον αποκλεισμό ύποπτων δραστηριοτήτων

Προστασία δικτύων



Πηγή: **Laudon and Traver (2018)**

Προστασία διακομιστών και πελατών

- Βελτιώσεις στην ασφάλεια των λειτουργικών συστημάτων
- Λογισμικό προστασίας από ιούς

Πολιτικές διαχείρισης & νομικό πλαίσιο

Τεχνικές διαχείρισης

- Σχέδιο ασφάλειας και πολιτικές διαχείρισης
  - Εκτίμηση κινδύνου
  - Πολιτική ασφαλείας
  - Σχέδιο υλοποίησης
  - Οργανισμός ασφαλείας
  - Έλεγχοι πρόσβασης
  - Διαδικασίες αυθεντικοποίησης
  - Βιομετρία
  - Τεκμήρια ασφαλείας
  - Πολιτικές εξουσιοδότησης
  - Σύστημα διαχείρισης εξουσιοδότησης
  - Έλεγχος ασφλαλείας

Σχέδιο ασφάλειας για το ηλεκτρονικό εμπόριο

Συνέργεια για την διαχείριση

- Συνεργασία ιδιωτών και δημοσίου (πχ US-CERT στις ΗΠΑ)
- Κυβερνητικές πολιτικές και έλεγχοι στην κρυπτογράφηση (χώρες ΟΟΣΑ, ΗΠΑ)

Νομικό πλαίσιο - Ελλάδα

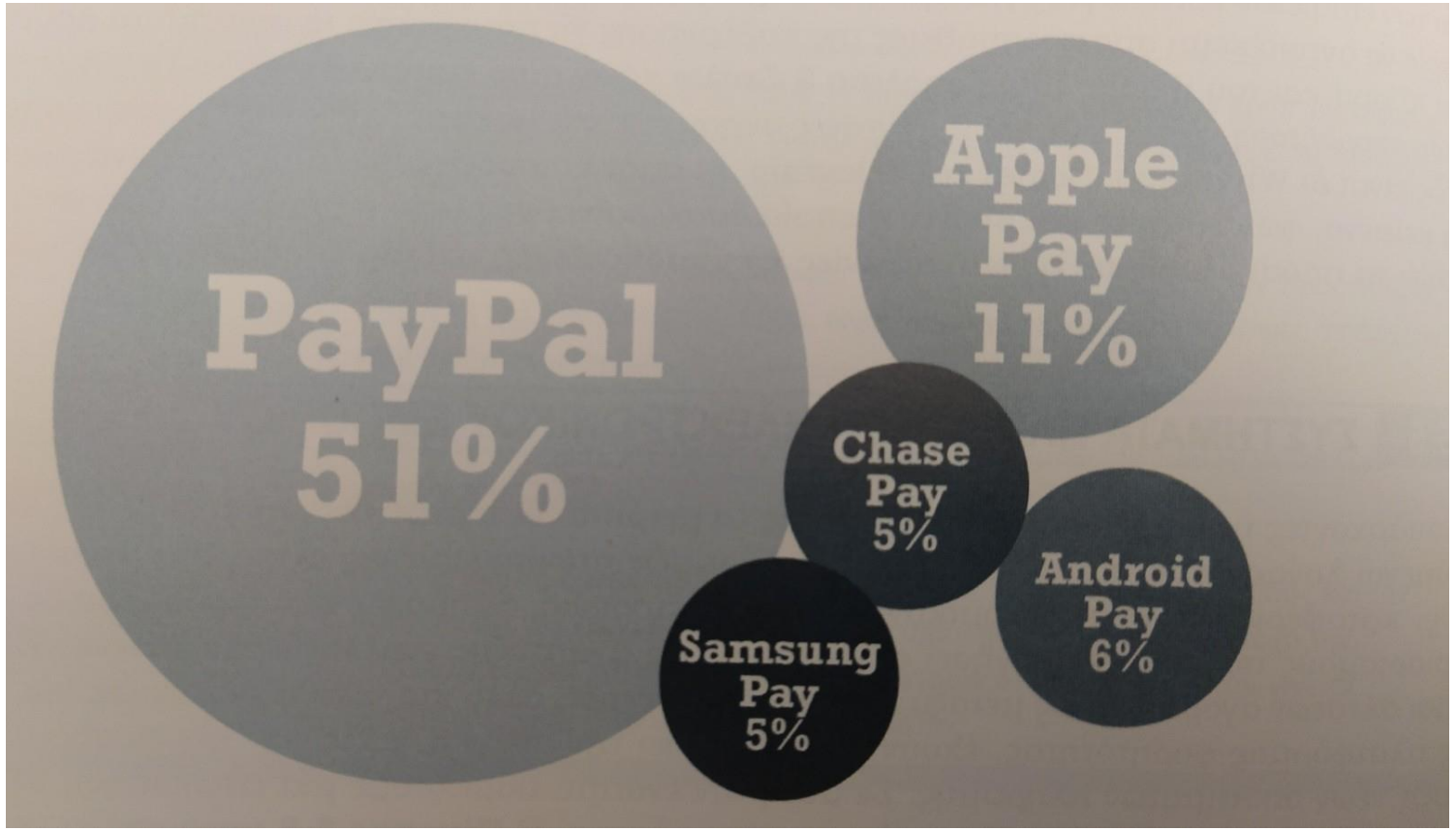
Διάλεξη της Αναπληρώτριας Καθηγήτριας Πανεπιστημίου Αιγαίου κας Λίλιαν Μήτρου «Ηλεκτρονικό Έγκλημα και Κυβερνοέγκλημα»

Νομικό πλαίσιο - Ευρώπη

https://www.consilium.europa.eu/el/policies/cybersecurity/#

Συστήματα πληρωμών ηλεκτρονικού εμπορίου

Κύριες τάσεις

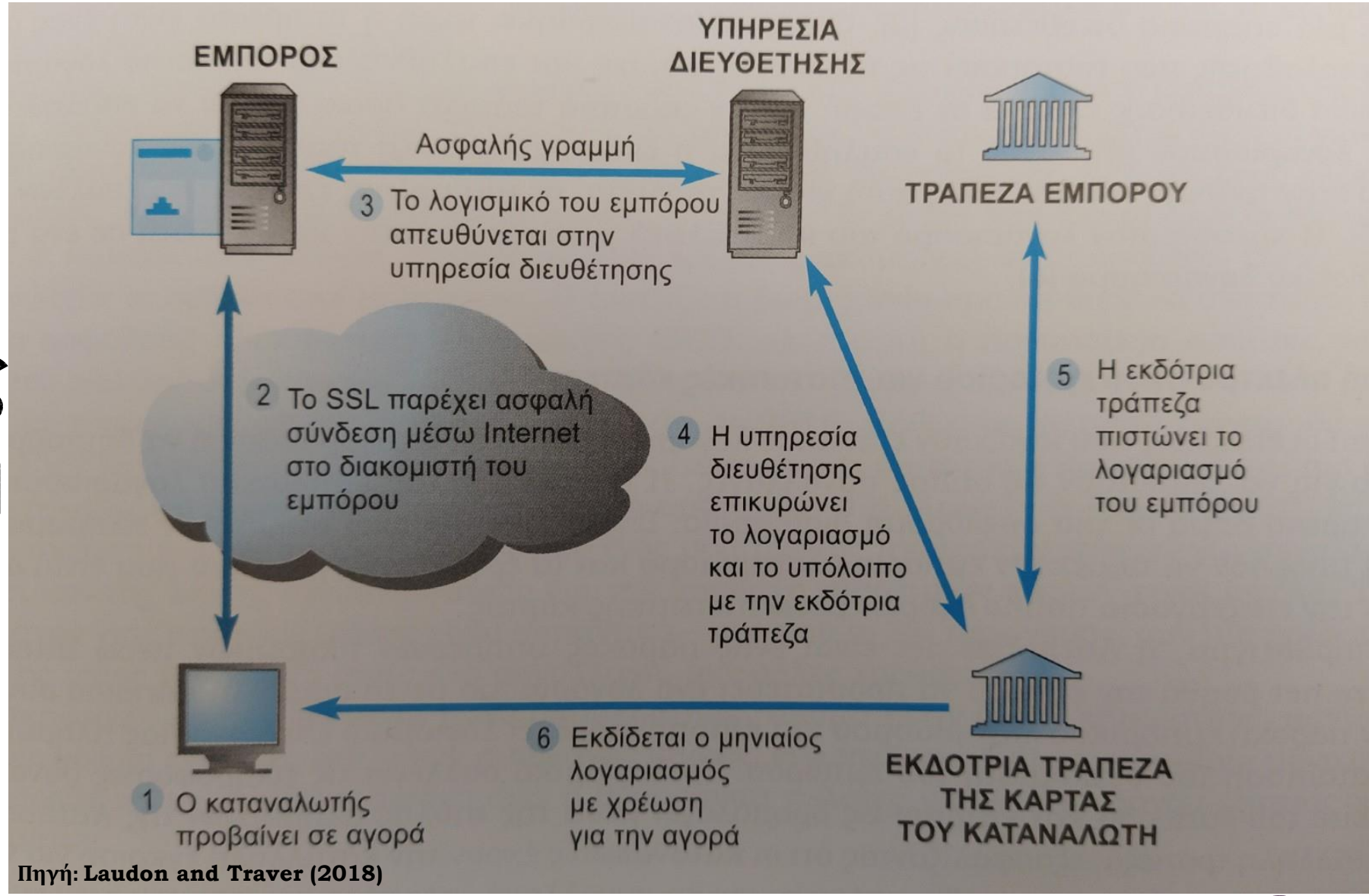


eMarketer 2017

Online συναλλαγές με πιστωτικές κάρτες

- Εμπορικός λογαριασμός
- Υποδομή ηλεκτρονικού εμπορίου για πιστωτικές κάρτες (πχ Authorize.net, CyberSource)
- Συμβατότητα με το PCI-DSS: πρότυπο προστασίας δεδομένων που ορίζονται από τις 5 μεγάλες εταιρείες πιστωτικών καρτών
- Περιορισμοί των Online συστημάτων πληρωμών με πιστωτικές:
  - Ασφάλεια, υψηλά ποσοστά απάτης
  - Κόστος διαχείρισης και συναλλαγών (περίπου 3% επί της κάθε αγοράς + κάποια πάγια χρέωση ανά συναλλαγή)
  - Κοινωνική δικαιοσύνη, αφού δεν μπορούν να τις αποκτήσουν όλοι

Διαδικασία συναλλαγής με πιστωτική κάρτα



Πηγή: Laudon and Traver (2018)

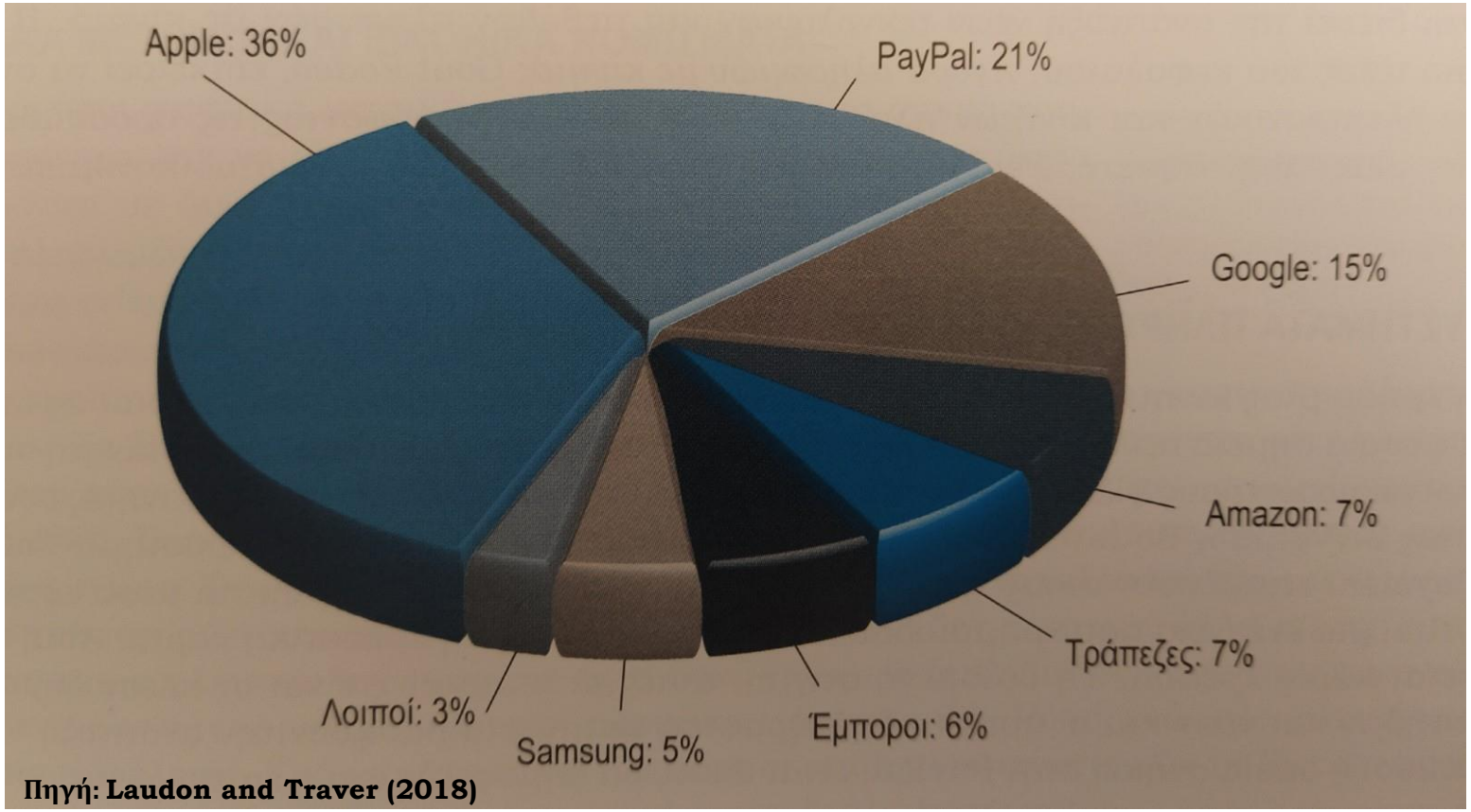
Εναλλακτικά συστήματα πληρωμών στο internet

- Online συστήματα πληρωμών αποθηκευμένης αξίας: επιτρέπουν στους καταναλωτές να κάνουν απευθείας πληρωμές σε εμπόρους και ιδιώτες με βάση την αποθηκευμένη αξία σε ένα λογαριασμό internet
- Πχ Paypal

Δραστηριότητα

- Παρακολουθείστε το παρακάτω βίντεο για το Paypal και σχολιάστε το επιχειρηματικό μοντέλο και τη σημασία του για την ασφάλεια των συναλλαγών https://www.youtube.com/watch?v=sLq3yWJQ6aQ

Συστήματα πληρωμών με κινητά



Πηγή: **Laudon and Traver (2018)**

Ομότιμα συστήματα πληρωμών για κοινωνικά δίκτυα και κινητά

- Οι χρήστες στέλνουν χρήματα με χρεωστική κάρτα και μέσω εφαρμογών για κινητά σε άλλα άτομα δωρεάν (πχ Venmo, Google Wallet, Facebook Messenger Payment κ.α.)

Ψηφιακά μετρητά και εικονικά νομίσματα

- Ψηφιακά μετρητά: εναλλακτικό σύστημα πληρωμής στο οποίο μοναδικά πιστοποιημένα τεκμήρια αναπαριστούν χρηματική αξία
  - Πχ Bitcoin, κρυπτογραφημένο νόμισμα που είναι ανώνυμο και περιέχει 34 χαρακτήρες
- Εικονικό νόμισμα: συνήθως κυκλοφορεί μέσα σε μία εσωτερική κοινότητα εικονικού κόσμου ή εκδίδεται από μία συγκεκριμένη εταιρική οντότητα και χρησιμοποιείται για την αγορά εικονικών αγαθών
  - Πχ Linden Dollars που δημιουργήθηκαν για το παιχνίδι εικονικού κόσμου Second Life

Δραστηριότητα

- Θεωρείτε ότι το Bitcoin θα αντικαταστήσει το χρήμα όπως το γνωρίζουμε σήμερα;
- Μελετήστε την σχετική μελέτη περίπτωσης που έχει αναρτηθεί στην Eclass προκειμένου να απαντήσετε.

Ηλεκτρονική εμφάνιση και πληρωμή λογαριασμών

Ηλεκτρονική εμφάνιση και πληρωμή λογαριασμών

- Μέγεθος και ανάπτυξη της αγοράς
- Επιχειρηματικά μοντέλα EBPP: νέα μορφή online συστημάτων πληρωμών για μηνιαίους λογαριασμούς
- Σημαντικοί παίκτες EBPP :