

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

Διαχείριση Ασφαλείας - Security Management (I)

Απειλές Ασφαλείας - Security Threats

Συμμετρική & Ασύμμετρη Κρυπτογραφία - Public & Private Keys

Ψηφιακά Πιστοποιητικά & Υπογραφή - Digital Certificates & Signature

Έλεγχος Πρόσβασης Χρήστη - Access Control, Single Sign-On (SSO)

Authentication & Authorization Infrastructures (AAI)

Πάροχοι Ταυτότητας - Digital ID Providers (IdP)

Security Assertion Markup Language (SAML)

Ασφαλής Πρόσβαση σε Web Servers - Πρωτόκολλο QUIC

B. Μάγκλαρης

maglaris@netmode.ntua.gr

www.netmode.ntua.gr

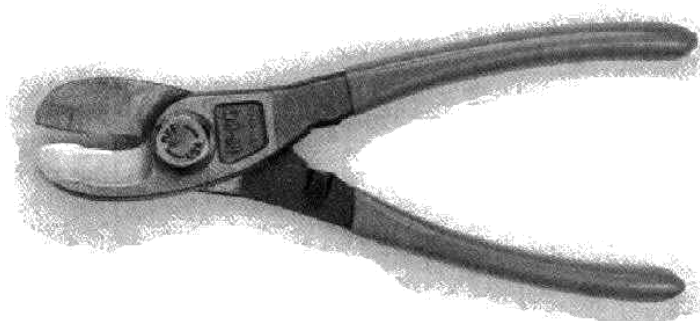
Νέα Κτίρια ΣΗΜΜΥ - Αίθουσα Συνεδριάσεων B.3.21

28/11/2022

ΘΕΜΑΤΙΚΕΣ ΠΕΡΙΟΧΕΣ ΑΣΦΑΛΕΙΑΣ

Network Security Thematic Areas

- Είδη Απειλών και Επιθέσεων
- Προστασία
 - Πολιτικές
 - Αρχιτεκτονικές Ελέγχου Πρόσβασης (**Authentication & Authorization Infrastructures - AAI**) & Διαχείρισης Δημοσίων Κλειδιών (**Public Key Infrastructures - PKI**)
 - Εργαλεία (**Access Control Lists – ACLs, Firewalls**)
 - Συστήματα Εντοπισμού Επιθέσεων (**Intrusion Detection Systems – IDS**) & Ανωμαλιών (**Anomaly Detection Systems**)
- Κρυπτογραφία
- Η **σίγουρη** μέθοδος εξασφάλισης ενός δικτύου:



ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

Network Security Threats

- **Απόκτηση πληροφοριών συστήματος & τελικών χρηστών**
 - Port Scanning
 - Fingerprinting
 - Υποκλοπή κωδικών, Phishing
- **Μη εξουσιοδοτημένη πρόσβαση**
 - Λάθος διαμορφώσεις (ανοικτά συστήματα)
 - Από μη εξουσιοδοτημένα σημεία (π.χ. ανοιχτά σημεία ασύρματης πρόσβασης)
- **Επιθέσεις Άρνησης Υπηρεσίας**
 - Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks
- **Υποκλοπή και παραποίηση επικοινωνιών**
 - Packet sniffing
 - "Man-in-the-Middle" attacks
- **Κακόβουλο λογισμικό (malware)**
 - Ιοί, Δούρειοι ίπποι (trojans)
 - Αυτόματα διαδιδόμενοι ιοί (worms)

ΥΠΟΚΛΟΠΗ & ΠΑΡΑΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

Eavesdropping & Data Falsification

- **Packet sniffing**

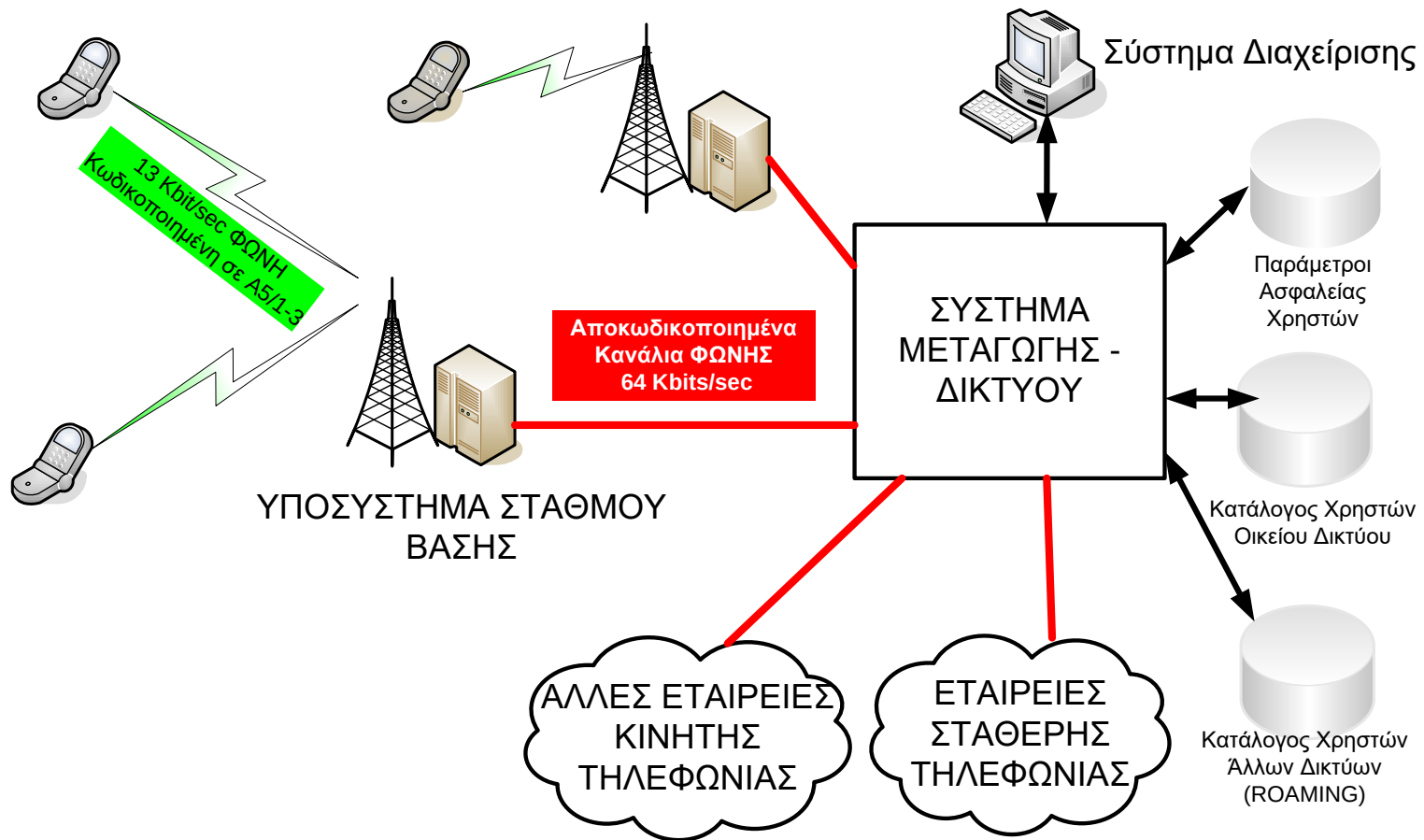
- Μπορεί να συμβεί σε δίκτυα με Hub, μη ασφαλισμένα ασύρματα δίκτυα ή σε περιπτώσεις υπερφόρτωσης του MAC Table ενός Switch
- Κάθε πληροφορία που κυκλοφορεί μη κρυπτογραφημένη είναι διαθέσιμη σε αυτόν που παρακολουθεί
 - *Telnet passwords*
 - *Web passwords*
 - *Οικονομικά και προσωπικά στοιχεία (π.χ. προσωπικά email, αριθμοί πιστωτικών καρτών κ.λπ.)*

- **"Man-in-the-Middle" attacks**

- Κάποιος μπορεί να παρεμβληθεί σε μια επικοινωνία και είτε να υποκλέψει τα στοιχεία είτε να "υποκριθεί" ότι είναι κάποιος τρίτος φορέας
 - *ARP "poisoning"*
 - *TCP "session hijacking"*
 - *DNS "poisoning" – URL redirection*
 - *Υποκλοπή περιεχομένου κλήσεων κινητής τηλεφωνίας GSM*

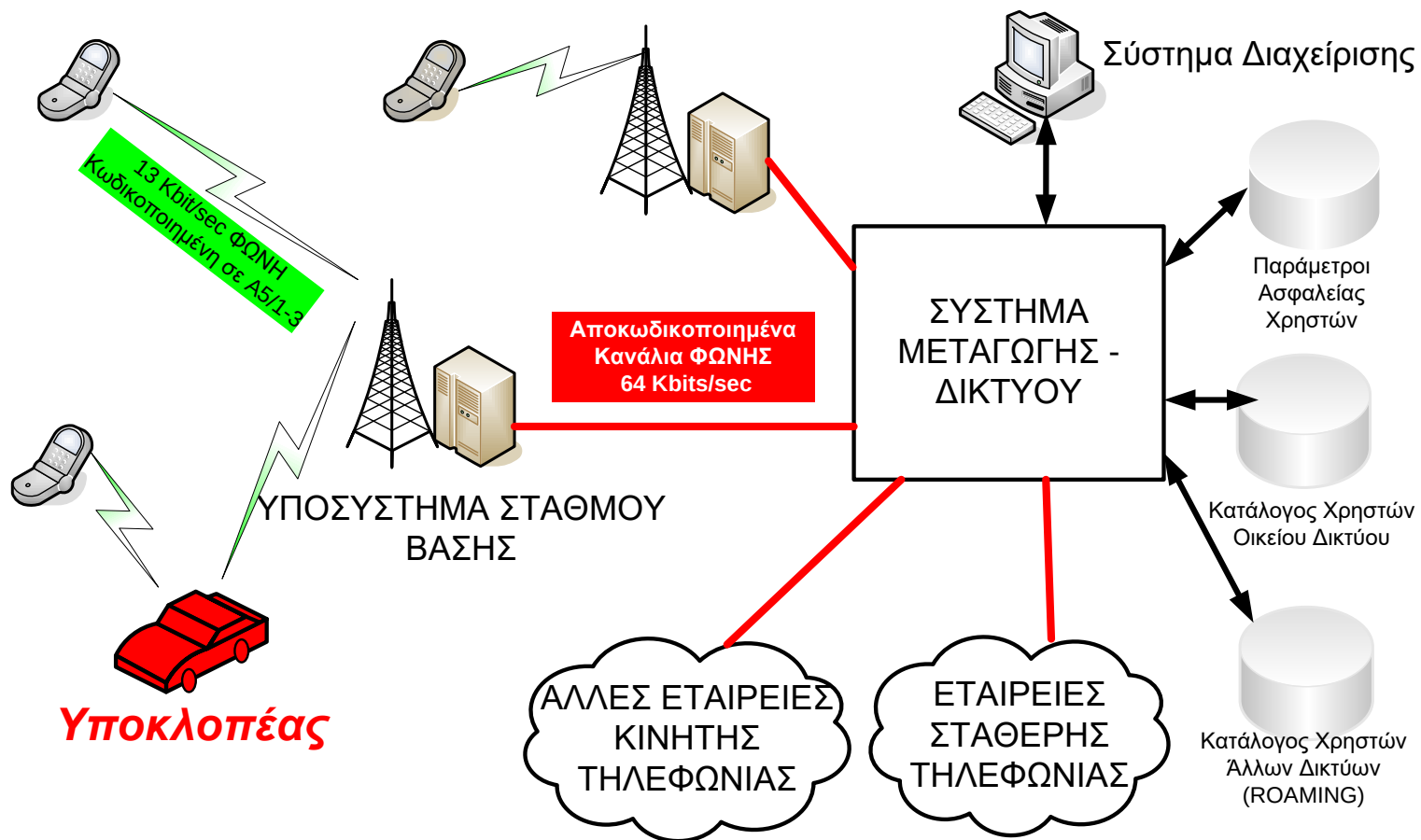
ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

Eavesdropping in GSM Mobile Telephony (1/4)



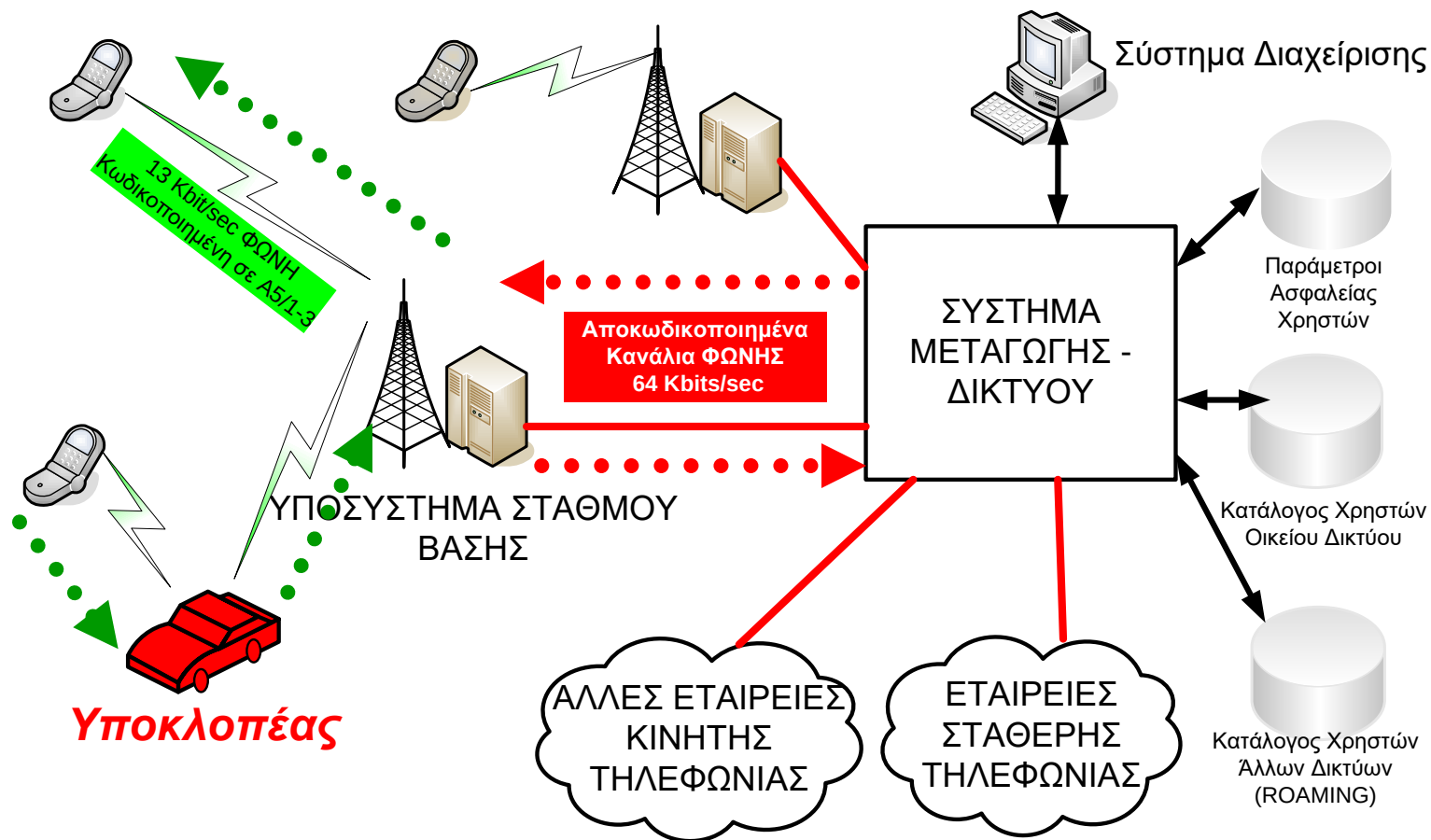
ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

Eavesdropping in GSM Mobile Telephony (2/4)



ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

Eavesdropping in GSM Mobile Telephony (4/4)



ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

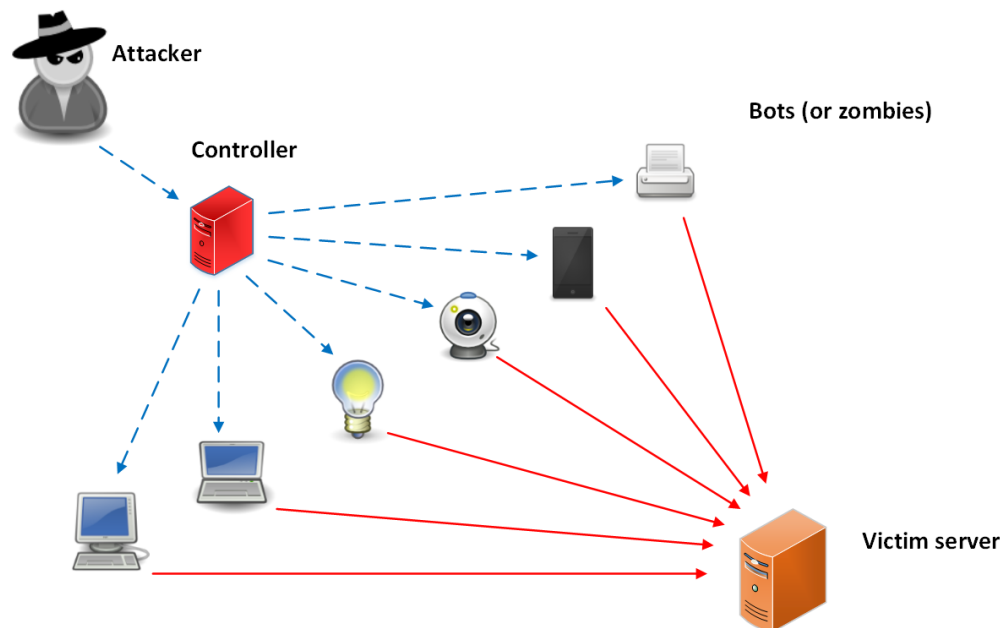
malware

- **Αυτόματα Διαδιδόμενοι Ιοί (worms)**
 - Εκμεταλλεύονται συνήθως άγνοια του τελικού χρήστη ή προβλήματα λογισμικού (**vulnerabilities**) σε Λειτουργικά Συστήματα ή εφαρμογές για να μεταδοθούν στο **Internet**
 - Διαδίδονται σε υπολογιστές με γειτονικές διευθύνσεις **IP** και το ίδιο πρόβλημα ή από προκαθορισμένη λίστα διευθύνσεων
 - Σε ορισμένες περιπτώσεις χρησιμοποιούνται παραπλανητικά μηνύματα **e-mail** που παρασύρουν το χρήστη στο να εκτελέσει συγκεκριμένες ενέργειες στον υπολογιστή του
 - Εφόσον χρησιμοποιήσουν ιδιαίτερα διαδεδομένο πρόβλημα είναι δυνατόν να εξαπλωθούν με μεγάλη ταχύτητα σε ολόκληρο το **Internet**
- **Δούρειοι Ίπποι (trojans – executable προγράμματα "σε απόκρυψη")**
 - Έχουν συνήθως αργή μετάδοση, προσκείμενοι σε εκτελέσιμα προγράμματα
 - Συνήθεις τρόποι διάδοσης: Εγκατάσταση/εκτέλεση λογισμικού από **USB Flash**, δικτυακά με **e-mail attachments**

DISTRIBUTED DENIAL OF SERVICE ATTACKS

DDoS Attacks

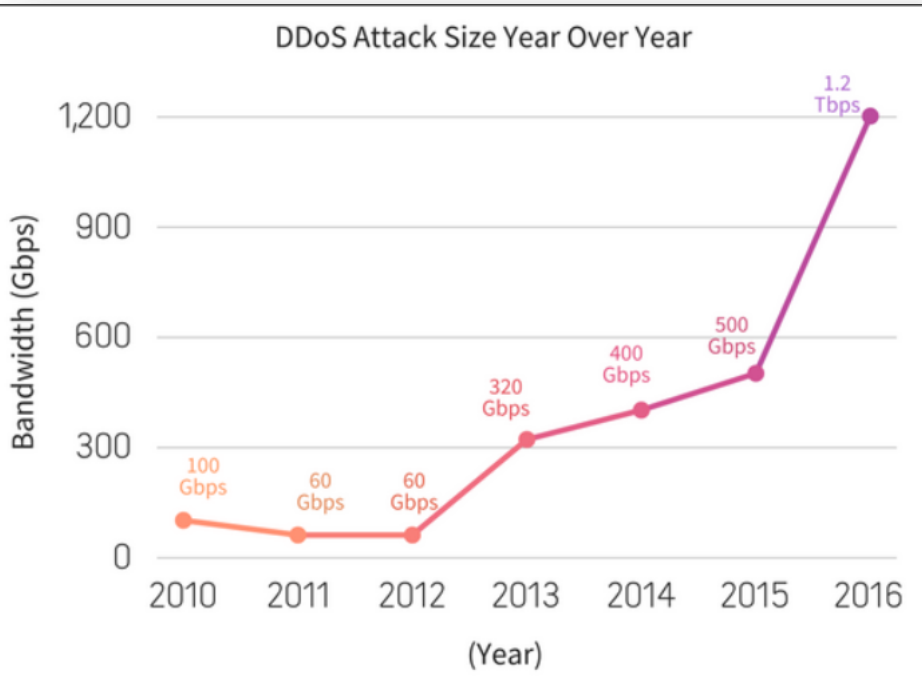
- **Bots ή Zombies:** *Μολυσμένοι* (π.χ. μέσω **worms** ή **Trojans**) *κόμβοι στο Internet (υπολογιστές - smart phones - sensors...) που ενεργοποιούνται σε ορισμένη χρονική στιγμή σαν bots ή zombie μαζικών Επιθέσεων Άρνησης Υπηρεσίας (Distributed Denial of Service Attacks, DDoS)*
- *Δρομολογείται μεγάλος όγκος κίνησης προς ένα θύμα με στόχο την κατασπατάληση του εύρους ζώνης της σύνδεσης του θύματος ή των πόρων του (επεξεργαστική ισχύς, μνήμη) ώστε να παρεμποδίζεται η όποια παρεχόμενη υπηρεσία*



ΣΤΑΤΙΣΤΙΚΕΣ ΕΠΙΘΕΣΕΩΝ DDoS

Evolution of DDoS Attacks

<https://blogs.haltdos.com/wp-content/uploads/2017/02/2015.png>



DDoS Statistics

<https://horizon.netscout.com/?atlas=summary>

Διάρκεια Επιθέσεων:

< 5 min:	22.97%
5 - 10 min:	35.92%
10 min - 1 hour:	31.72%
> 1 hour:	9.40%

Μέγεθος Επιθέσεων:

(packets/sec - pps)

< 10 kpps:	19.79%
10 kpps - 1 Mpps:	73.48%
> 1 Mpps:	6.73%

NOVEMBER 2021

Highlights:

ISPs:	544
Routers:	10162
Attacks:	739 k
Peak Volume:	612 Gbps
Peak Speed:	802 Mpps
Peak Duration:	7 days (6 days, 21 hours)
Top Attack Types:	Total Traffic
	UDP
	IP Fragmentation

ISPs by Region:

APAC	95
EMEA	296
LATAM	59
NAMER	94



ΕΠΙΘΕΣΗ DDoS ΣΕ ΠΑΡΟΧΟ ΥΠΗΡΕΣΙΩΝ DNS

DDoS Attack στον πάροχο Dyn (21/10/2016)

- Μέγεθος κίνησης: **1.2 Tbps**
- Πηγή της επίθεσης **100.000** παραβιασμένες συσκευές Internet of Things
- Αδυναμία πρόσβασης μεγάλου αριθμού χρηστών σε σημαντικές υπηρεσίες επιχειρήσεων: **Amazon, CNN, Twitter, PayPal, Visa, GitHub, Spotify, Netflix,...**

<https://blogs.haltdos.com/wp-content/uploads/2017/02/2015.png>

ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΛΕΙΔΙΟΥ

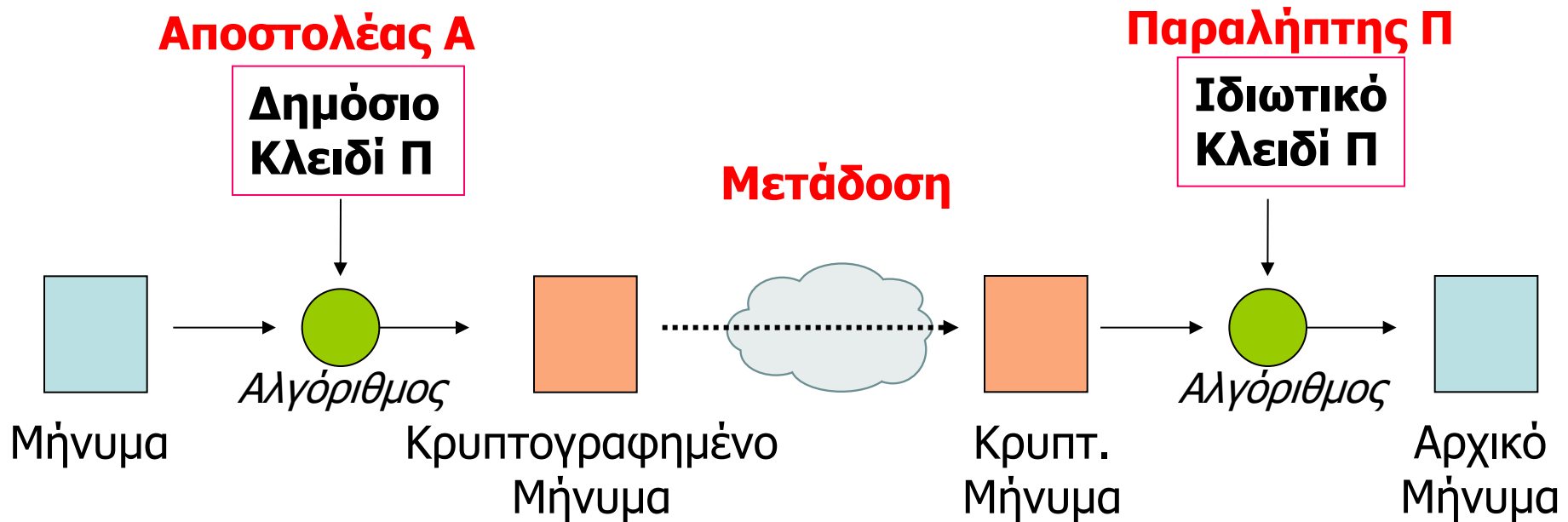
Key Encryption Methods

- Συμμετρική (Ιδιωτικού Κλειδιού, **Private Key Cryptography**)
 - Χρήση μοναδικού κλειδιού και από τα δύο μέρη
 - Κρυπτογράφηση με συγκεκριμένου μήκους κομμάτια κειμένου (**block cipher**) ή ανά bit σε συνεχή ροή δεδομένων (**stream cipher**)
 - Αλγόριθμοι κρυπτογράφησης: **DES, triple DES, RC2, RC4, RC5, IDEA, AES**
 - Γρήγορη αλλά έχει προβλήματα στην ασφάλεια διανομής του κλειδιού
 - Έχει πολλαπλή χρήση: **Encryption, authentication, non-repudiation**
- Μη Συμμετρική (Δημόσιου Κλειδιού, **Public Key Cryptography**)
 - Κάθε μέρος έχει ιδιωτικό και δημόσιο κλειδί. Διανέμει το τελευταίο ελεύθερα
 - Αλγόριθμοι κρυπτογράφησης: **RSA, Diffie-Hellman**
 - Αλγόριθμοι κατακερματισμού (hash functions) για εξαγωγή περίληψης μέρους ή του συνόλου ενός μηνύματος: **SHA & SHA-1, MD2, MD4, MD5**
 - Ισχυρά σημεία:
 - Δεν διανέμονται ιδιωτικά κλειδιά – μόνο τα δημόσια κλειδιά
 - Αδύνατα σημεία:
 - Αργή στην εκτέλεση
 - Αμφισβήτηση εμπιστοσύνης στα δημόσια κλειδιά: Συνιστάται η εγκατάσταση Αρχών Πιστοποίησης (**Certification Authorities, CA**) και οργανωμένων υποδομών Δημοσίου Κλειδιού (**Public Key Infrastructures, PKI**)
 - Έχει πολλαπλή χρήση: **Encryption, authentication, non-repudiation**

ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Pubic Key Encryption: Confidentiality

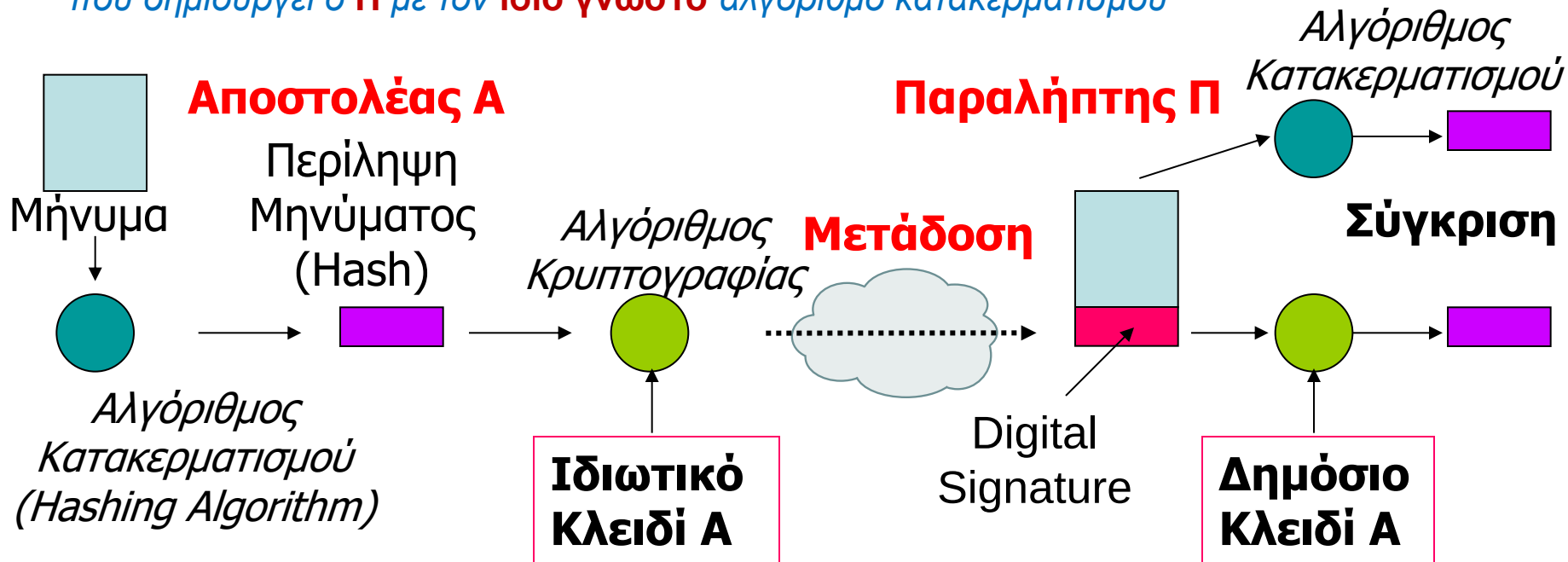
- Ο Αποστολέας **A** γνωρίζει το **Δημόσιο Κλειδί** του Παραλήπτη **Π** (π.χ. με Ψηφιακό Πιστοποιητικό από Certification Authority **CA**, self-signed ή υπογραμμένο από 3^{ης} έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια Υποδομής Δημοσίου Κλειδιού - **Public Key Infrastructure PKI**)
 - *Κρυπτογράφηση στον **A**: Με το Δημόσιο Κλειδί του **Π***
 - *Αποκρυπτογράφηση στον **Π**: Με το Ιδιωτικό Κλειδί του **Π***



ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ:

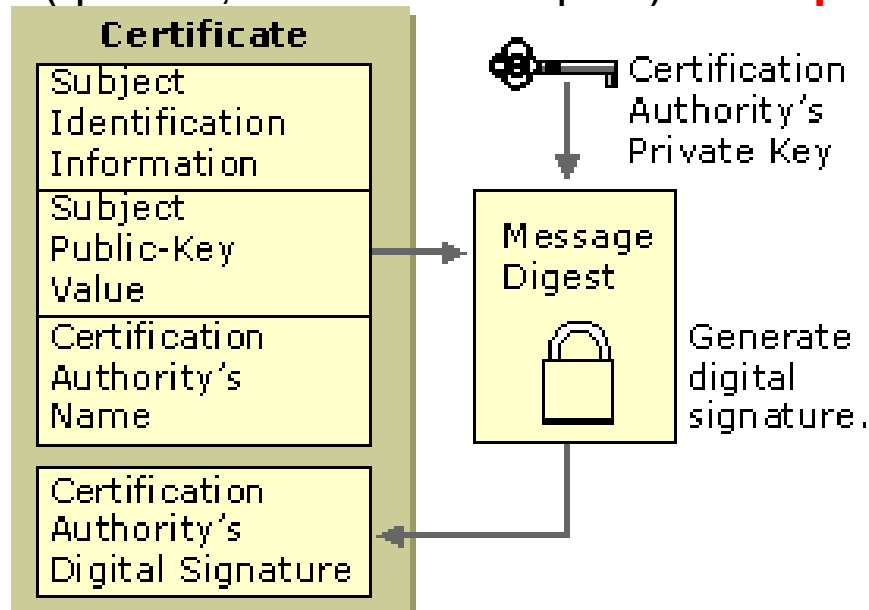
Sender Authentication / Non Repudiation – Message Integrity

- Οι Αποστολέας **A** και Παραλήπτης **Π** κατέχουν ζεύγη Δημοσίου & Ιδιωτικού Κλειδιού και έχουν αμοιβαία γνώση των **Δημοσίων Κλειδιών** & αλγορίθμων κρυπτογράφησης - κατακερματισμού
- Ο Αποστολέας **A** προσθέτει Ψηφιακή Υπογραφή (**Digital Signature**) στο μήνυμα με κρυπτογράφηση με το Ιδιωτικό του κλειδί περίληψης (**hash**) του μηνύματος που προκύπτει με αλγόριθμο κατακερματισμού (**hashing algorithm**)
- Ο Παραλήπτης **Π** επιβεβαιώνει (**authenticate**) την ταυτότητα του **A**, χωρίς δυνατότητά του **A** άρνησης της αποστολής (**non-repudiation**) & επιβεβαιώνει την μη αλλοίωση του μηνύματος (**message integrity**) με βάση την σύγκριση:
 - Ψηφιακής Υπογραφής, αποκρυπτογραφημένης στον **Π** με το **γνωστό** Δημόσιο Κλειδί του **A**
 - Νέας περίληψης του ληφθέντος (**μη κρυπτογραφημένου, clear text**) κυρίως μηνύματος που δημιουργεί ο **Π** με τον **ίδιο γνωστό** αλγόριθμο κατακερματισμού



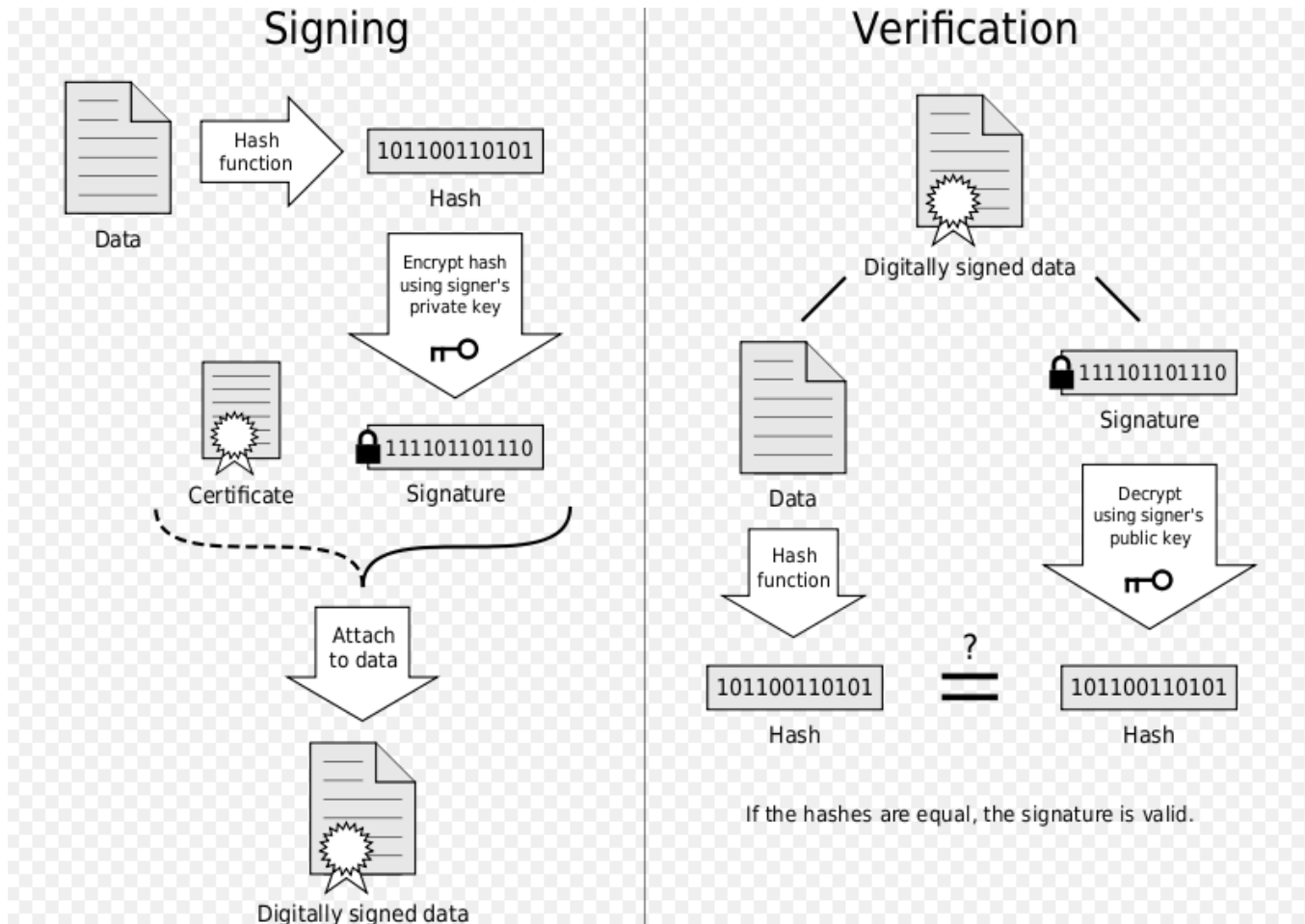
ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ X.509

- Αν συνοδεύουν υπογραμμένο μήνυμα, βεβαιώνουν τη γνησιότητα του **Δημοσίου Κλειδιού** του αποστολέα (subject) κατά μια Τρίτη Έμπιστη Οντότητα **TTP - Third Trusted Party**: Την Αρχή Πιστοποίησης, **Certification Authority – CA**
- **Μη Κρυπτογραφημένα Πεδία Ψηφιακού Πιστοποιητικού**: Πληροφορίες για τον αποστολέα (subject) μηνύματος (**ID, Public Key,...**) και της **CA**
- **Κρυπτογραφημένο Πεδίο**: Ψηφιακή Υπογραφή Πιστοποιητικού από **CA**
- Η **CA** υπογράφει με το **Ιδιωτικό Κλειδί** της. Το **Δημόσιο Κλειδί** της πρέπει να είναι γνωστό στους παραλήπτες (π.χ. ενσωματωμένο στον Web Browser) ή αποδεκτό λόγω σχέσης εμπιστοσύνης (π.χ. σε περιπτώσεις **Self-Signed CA**)
- Αν χρειάζεται και έλεγχος του **Δημοσίου Κλειδιού** της **CA**, μπορεί να αποστέλλεται και 2^ο (ή και 3^ο, 4^ο ...πιστοποιητικό) από **ιεραρχικά δομημένες CA**



ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

http://en.wikipedia.org/wiki/Digital_signature



ΜΕΙΚΤΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΟΥΣ ΠΡΟΣΒΑΣΗΣ

Access Control, Mixed Schema

SSL/TLS: Secure Sockets Layer/Transport Layer Security

• 1^η Φάση: Handshaking

- Ο χρήστης (User) **U** λαμβάνει γνώση του **Δημοσίου Κλειδιού** του εξυπηρετητή (Server) **S** με Ψηφιακό Πιστοποιητικό από Certification Authority **CA** self-signed ή υπογραμμένο από 3^{ης} έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια αρχιτεκτονικής **Public Key Infrastructure PKI**
- Ο **U** δημιουργεί Κοινό **Συμμετρικό Κλειδί** με τυχαίο αλγόριθμο και το κοινοποιεί στον **S** κρυπτογραφημένο με το **Δημόσιο Κλειδί** του **S**

• 2^η Φάση: Κρυπτογραφημένος Διάλογος με Κοινό Συμμετρικό Κλειδί

- Γρήγορη συμμετρική κρυπτογραφία σε **Secure Channel** μεταξύ **S – U** (το Συμμετρικό Κλειδί ισχύει μόνο για το συγκεκριμένο session)

• ΠΑΡΑΤΗΡΗΣΗ:

- Ο **U** δεν απαιτείται να έχει Πιστοποιητικό με **Δημόσιο Κλειδί** (ψηφιακή υπογραφή), μόνο ο **S** έχει Πιστοποίηση μέσω TTP ή self-signed (**Server Based Authentication**)
- Για Ταυτοποίηση – Εξουσιοδότηση του **U** από τον **S** (**Client & Server Based Authentication**) απαιτείται μετάδοση από το secure channel της **Digital Identity** του Client (συνήθως **User_Name/Password** ή **Client Certificates** αν υπάρχουν, εναλλακτικά **PIN** για ταυτοποίηση με e-mail ή SMS σε κινητό του **U**) → έλεγχος στον **S** σε Βάση Δεδομένων Χρηστών (με πρωτόκολλο **LDAP - TCP** για εφαρμογές Web, Mail... ή με πρωτόκολλο **RADIUS - UDP** αν μεσολαβεί **Remote Access Server** π.χ. για πρόσβαση σε υπηρεσία DSL, WiFi roaming...)

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΧΡΗΣΤΗ

User Access Control, Authentication & Authorization Infrastructure (AAI) Single Sign-On (SSO), Identity Providers (IdP)

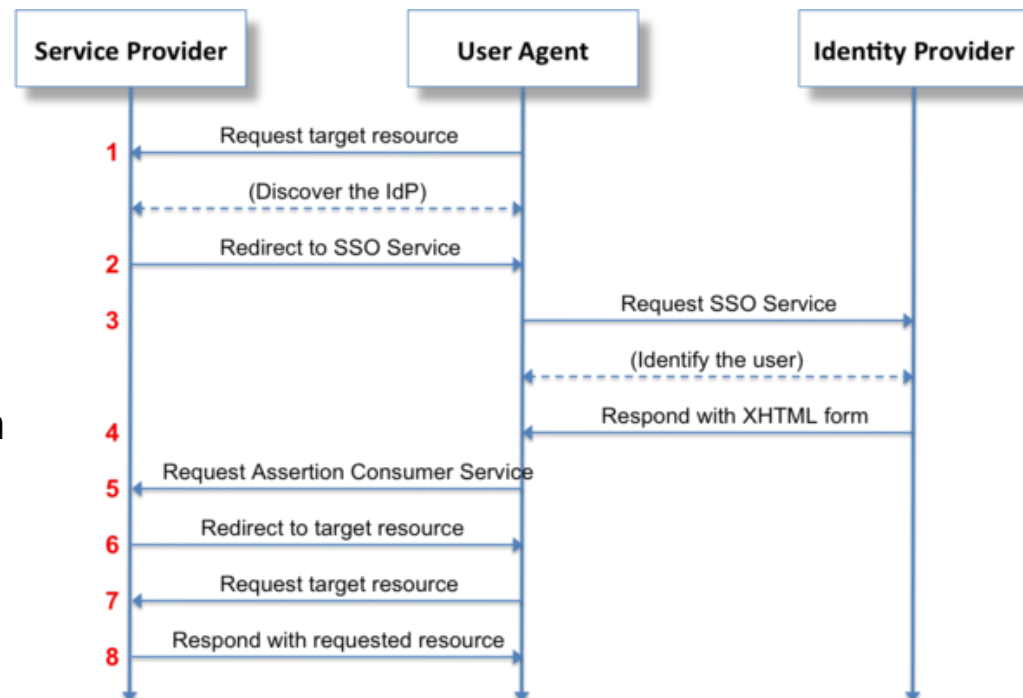
- Ταυτοποίηση (**Authentication**) & Εξουσιοδότηση (**Authorization**) χρήστη με:
 - Username, Password
 - LDAP Server (Lightweight Directory Access Protocol)
 - RADIUS (Remote Authentication Dial-In User Service)
 - Active Directory (MS Windows)
- Οι Υποδομές Ταυτοποίησης & Εξουσιοδότησης (**AAI**) επιτρέπουν πρόσβαση **Single Sign-On (SSO)** σε χρήστες διαδικτυακών πόρων κατανεμημένων σε παρόχους με αμοιβαία εμπιστοσύνη:
 - Ταυτοποίηση (Authentication) μια φορά
 - Εξουσιοδότηση (Authorization) ξεχωριστά με κάθε πάροχο
- Μεσολάβηση Παρόχου Ταυτότητας (**Identity Provider - IdP**) π.χ. **Facebook, Twitter, Google User Accounts** για
 - Εξουσιοδότηση Single Sign-On σε υπηρεσίες με σχετικό security token συνδρομητή από IdP σε **Service Providers** που το εμπιστεύονται (π.χ. **OAuth** – Open standard for Authorization, **SAML** - Security Assertion Markup Language)
 - Επιβεβαίωση Ισχυρισμών Ταυτότητας (**Identity Assertion**) από **WAYF** (Where Are You From) servers μέσω πρωτοκόλλου **SAML** ή από **LDAP** servers με πιστοποιητικά **X509**
- Συνέργεια **IdP** σε ομόσπονδα σχήματα **AAI** (π.χ. US Internet2 **Shibboleth**, GÉANT **eduGAIN**)

ΠΡΟΣΒΑΣΗ Single Sign-On (SSO) ΜΕΣΩ SAML

SAML - Security Assertion Markup Language

https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

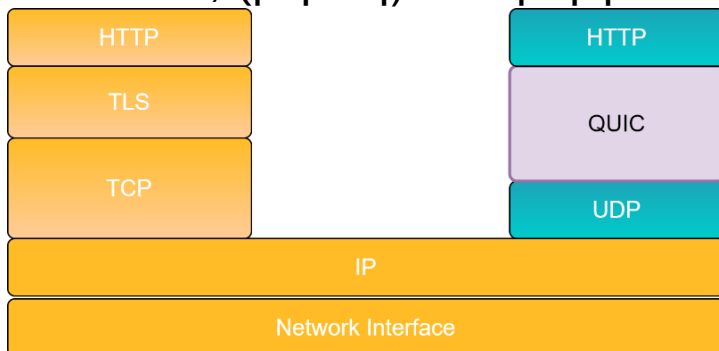
- Ρόλοι οριζόμενοι στο πρότυπο **SAML** (OASIS Standard):
 - Τελικός χρήστης (Principal User, **P**)
 - Πάροχος Υπηρεσιών (Service Provider, **SP**)
 - Πάροχος Ταυτότητας (Identity Provider, **IdP**)
- **SAML**: Μηχανισμός Επιβεβαίωσης Ισχυρισμών Ταυτοποίησης & Εξουσιοδότησης (**Authentication & Authorization Assertions**) Τελικού Χρήστη (**P**) προς Πάροχο Υπηρεσιών (**SP**) με την βοήθεια Παρόχων Ταυτότητας (**IdP**)
 - Ανταλλαγή μηνυμάτων SAML μεταξύ **P** (User Agent), **SP**, **IdP**
 - Μηνύματα κωδικοποιημένα σε φόρμες **XML** και μεταφορά (συνήθως) με πρωτόκολλα **HTTP** & **SOAP** (Simple Object Access Protocol)
 - Για σιγουριά προστασία με πρωτόκολλα TLS και XML encryption



ΑΣΦΛΕΙΑ ΠΡΟΣΒΑΣΗΣ WEB (http) ΣΕ ΠΑΡΟΧΟΥΣ

Πρωτόκολλα QUIC (Quick UDP Internet Connection)

- Παραδοσιακά μοντέλα για συνδέσεις Web (browser – server): HTTP/1, HTTP/2 πάνω από παράλληλες συνδέσεις **TCP**
- Νέα γενιά πρωτοκόλλων HTTP/3: Πρωτόκολλα client – server **QUIC** πάνω από **UDP**
 - Αρχική έκδοση Google 2012: **gQUIC**
 - Τυποποίηση IETF 2021: **RFC 9000**
- Τείνει να υποκαταστήσει το HTTP/2 για υπηρεσίες streaming των **FAANG** (Facebook, Amazon, Apple, Netflix, Google)
- Υποστήριξη: **Chrome** (Google), **Edge** (Microsoft), **Firefox** (Mozilla), **Safari** (Apple)...
- **Βασική ιδέα QUIC**: Αντί για συνδέσεις TLS/TCP του HTTP/2, χρησιμοποιεί πρωτόκολλα HTTP/3 με πολυπλεξία ασύγχρονων συνδέσεων UDP, με μηχανισμούς ασφαλείας πρόσβασης (τύπου TLS) και συμμετρική κρυπτογράφηση πακέτων (payloads & τμήμα των QUIC headers) από άκρο σε άκρο
- **Πλεονεκτήματα από TLS/TCP**: Ταχύτητα, αντοχή σε απώλειες πακέτων των παραλλήλων συνδέσεων TCP, ενισχυμένη ασφάλεια περιεχομένου και έλεγχος συμφόρησης (congestion control) από άκρο σε άκρο, παράκαμψη ενδιάμεσων middle boxes, (μερική) αποφυγή επιθέσεων & υποκλοπών...



- <https://www.rfc-editor.org/rfc/rfc9000.html>
- https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/07/17/looking_into_quicp_a-pUtF.html
- <https://en.wikipedia.org/wiki/QUIC>