Αντιμετώπιση Ευπαθειών του Πρωτοκόλλου SS7 σε Δίκτυα Κινητής Τηλεφωνίας

Μανιάτης Σωτήρης, Ειδικό Επιστημονικό Προσωπικό ΑΔΑΕ
Τρακάδας Παναγιώτης, Αν. Καθηγητής ΤΕΙ Στερεάς Ελλάδας

Νομοθετικό Πλαίσιο

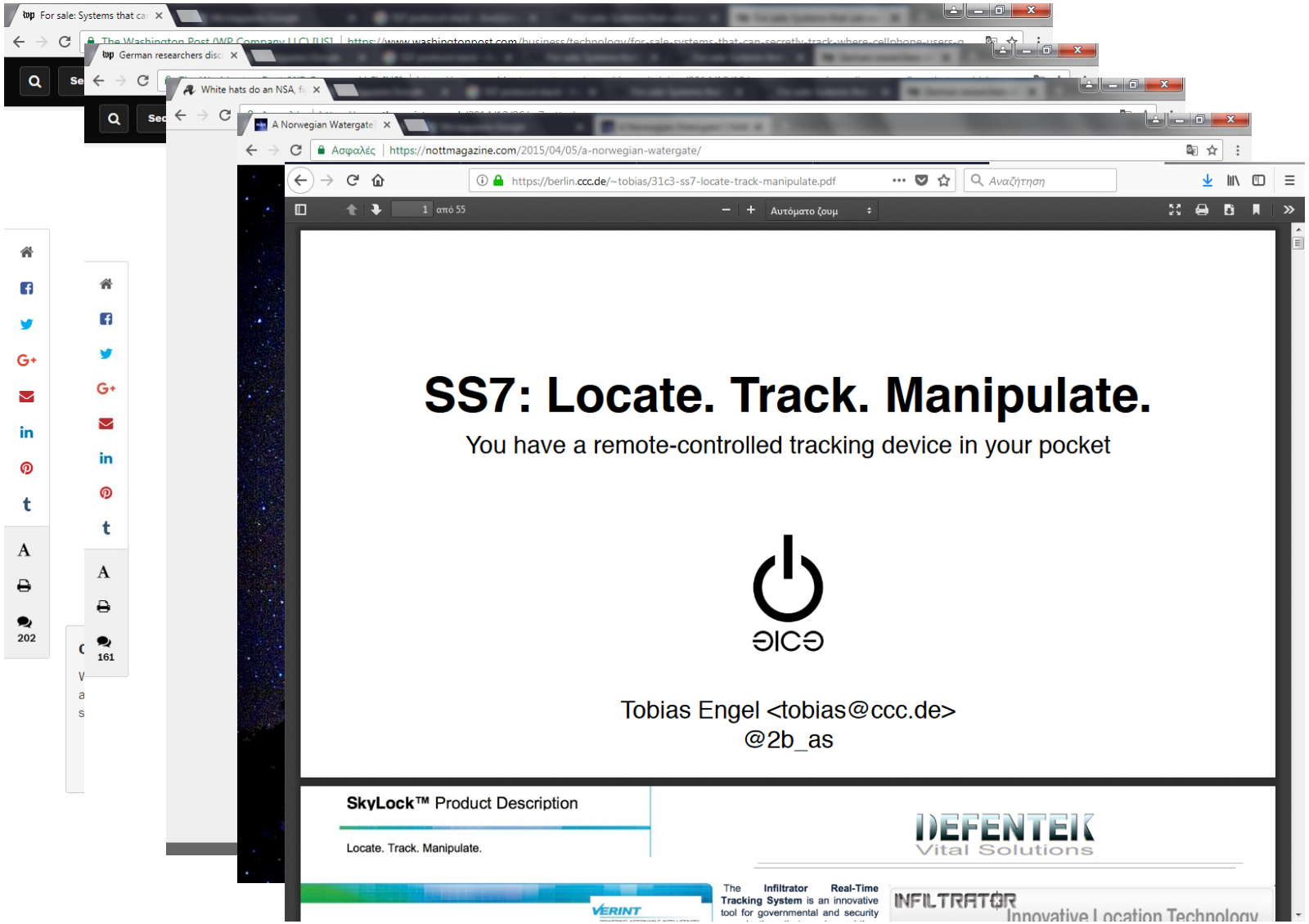
Απόφαση 165/2011
Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών.
(ΦΕΚ 2715/Β/17.11.2011)

Απόφαση 205/2013
Κανονισμός για την
Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών
(ΦΕΚ 1742/Β/15.7.2013)

Αυτοί οι κανονισμοί επιβάλλουν την εφαρμογή

- Οργανωτικών Δομών
- Τεχνικών Μέτρων
- Διαδικασιών

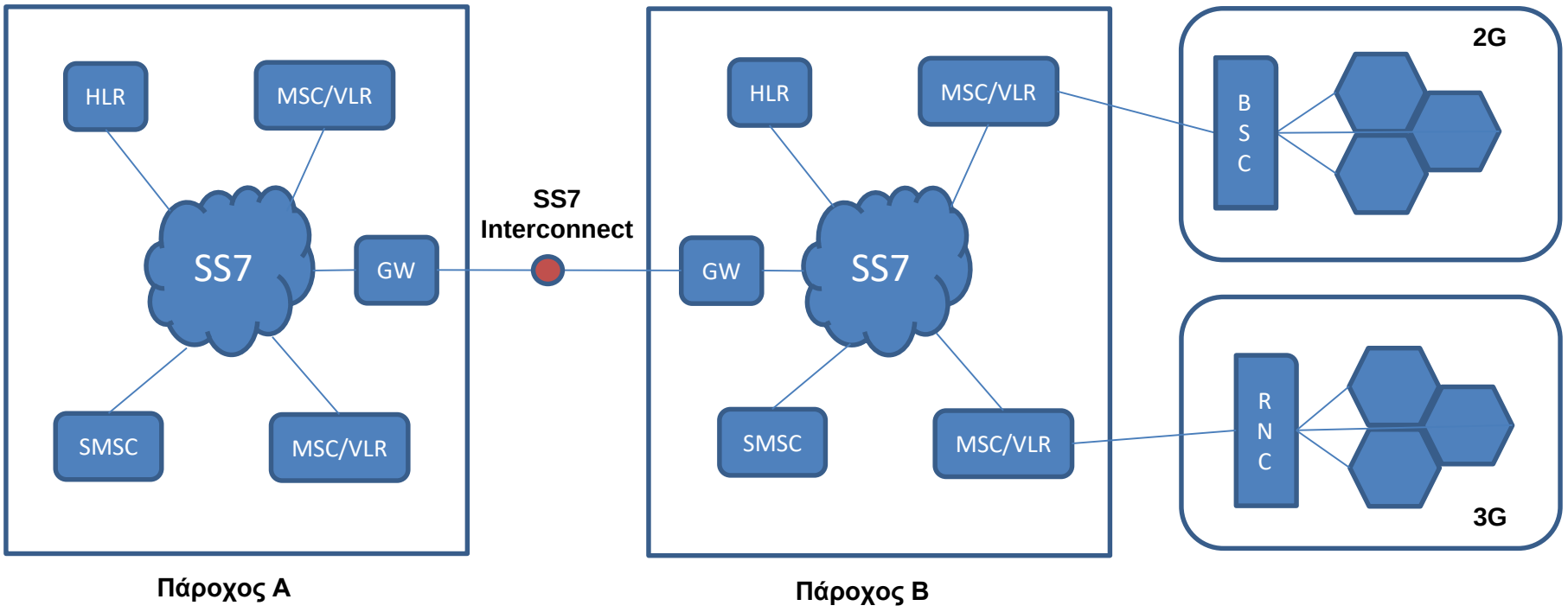
Δημοσιότητα



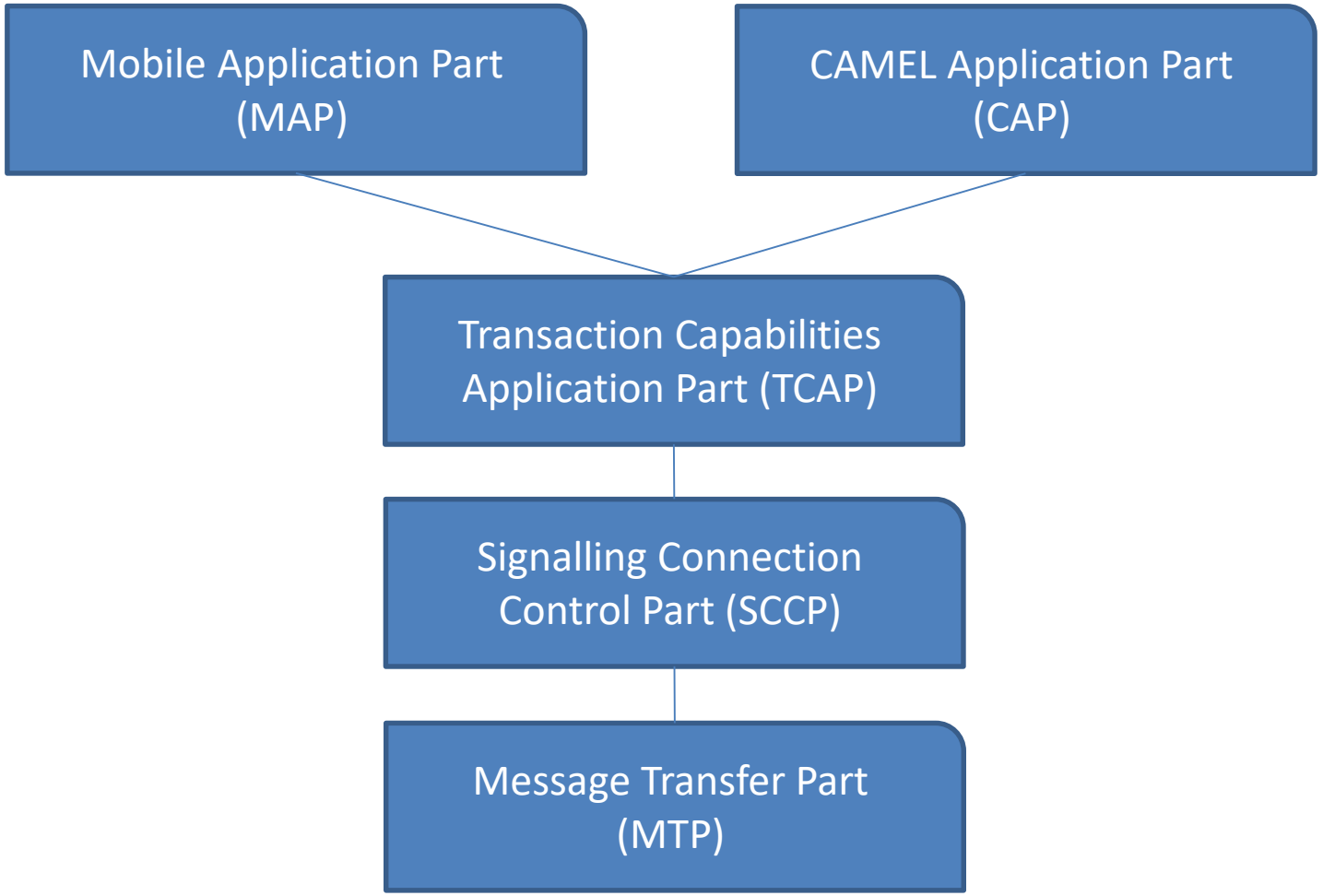
Το πρωτόκολλο SS7 – Γενικά

- Γενικές Πληροφορίες
  - Σύνολο πρωτοκόλλων για παροχή υπηρεσιών σε δίκτυα σταθερής και κινητής τηλεφωνίας
  - Αναπτύχθηκε στις δεκαετίες 70 και 80
  - Χρησιμοποιείται στα δίκτυα κινητής 2G/3G
    - 4G/5G – DIAMETER / …
- Βασική Αιτία Ευπαθειών
  - περιβάλλον εμπιστοσύνης ⇔ ανοιχτό περιβάλλον
    - Παγκοσμίως: 5 δις χρήστες, 2000 πάροχοι, 220 χώρες (πηγή: GSMA)
  - Έλλειψη μηχανισμών ασφάλειας (αυθεντικοποίηση)
  - Πάροχοι: τηλεπικοινωνιακοί, περιεχομένου, υπηρεσίες που βασίζονται στον εντοπισμό θέσης, …

Το πρωτόκολλο SS7 – Αρχιτεκτονική



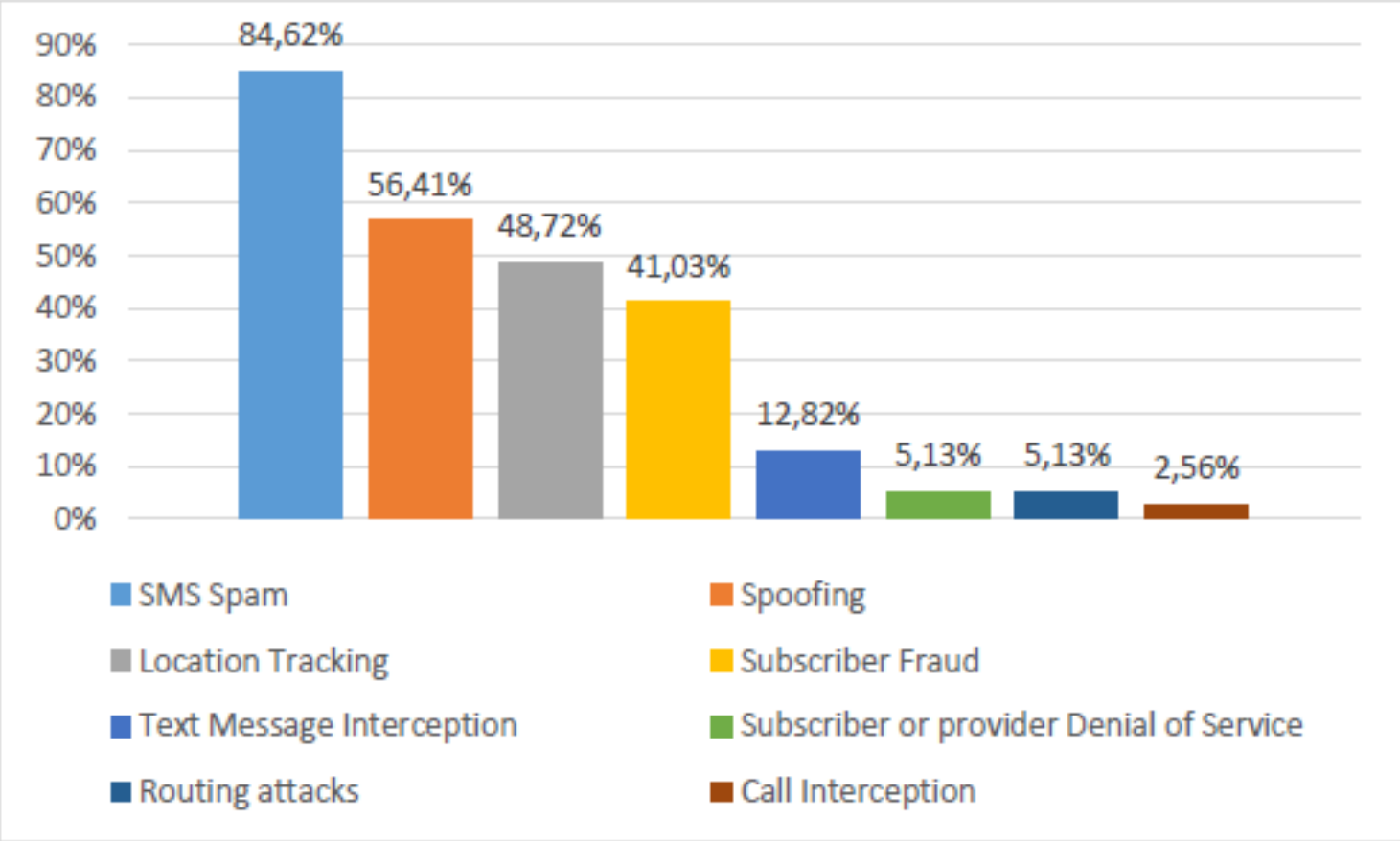
Το πρωτόκολλο SS7 – Στοίβα



Το πρωτόκολλο SS7 – Απειλές

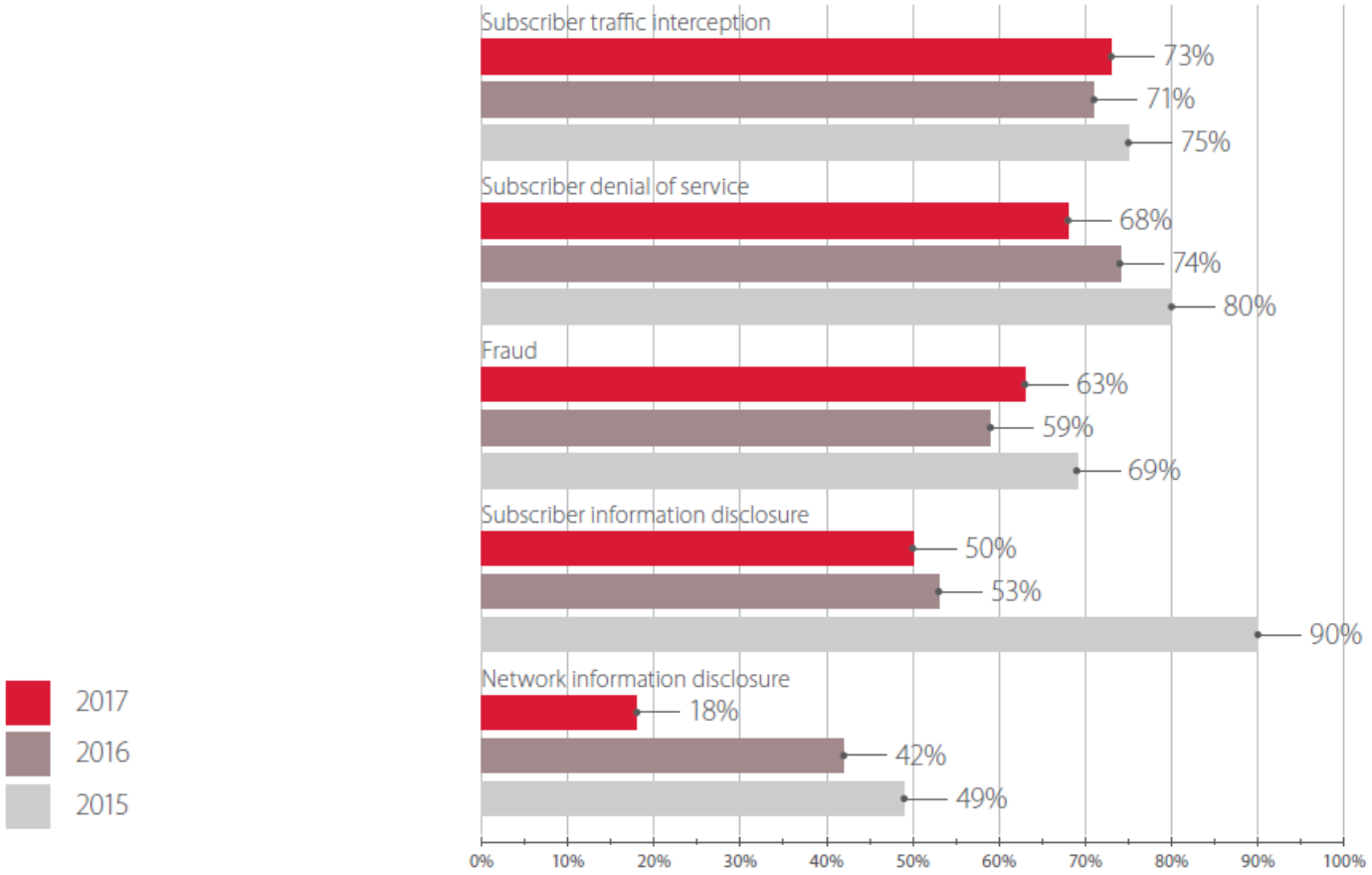
Αποκάλυψη Πληροφοριών Δικτύου	Ανάκτηση δεδομένων διαμόρφωσης δικτύου
Αποκάλυψη Πληροφοριών Χρηστών/Συνδρομητών	Εντοπισμός γεωγραφικής θέσης Ανάκτηση IMSI Εύρεση Υπολοίπου
Υποκλοπή (Interception)	Κλήσεις, SMS, κίνηση διαδικτύου,…
Άρνηση Υπηρεσίας (DoS)	Διαθεσιμότητα υπηρεσιών δικτύου Συνδεσιμότητα χρήστη
Απάτη (Fraud)	Αποφυγή Χρέωσης Απενεργοποίηση ορίων τιμολόγησης Χρέωση τρίτων
Ανεπιθύμητη Αλληλογραφία (Spam)	Ογκώδης αποστολή SMS & κλήσεων

Το πρωτόκολλο SS7 – Απειλές



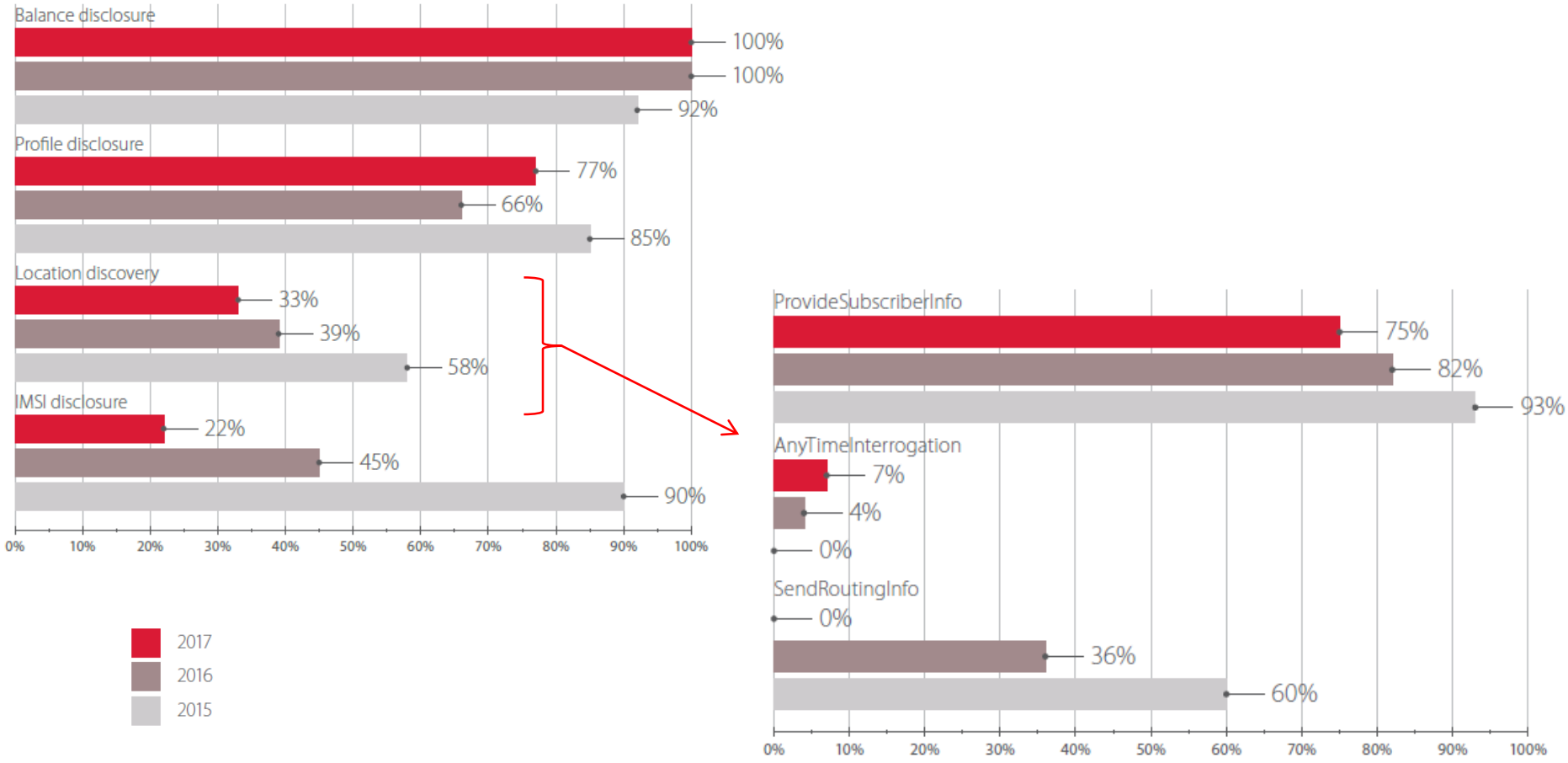
Πηγή: "*Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation*", ENISA, March 2018

Το πρωτόκολλο SS7 – Απειλές



Πηγή: "*SS7 Vulnerabilities and Attack Exposure Report*", Positive Technologies, 2018

Το πρωτόκολλο SS7 – Απειλές

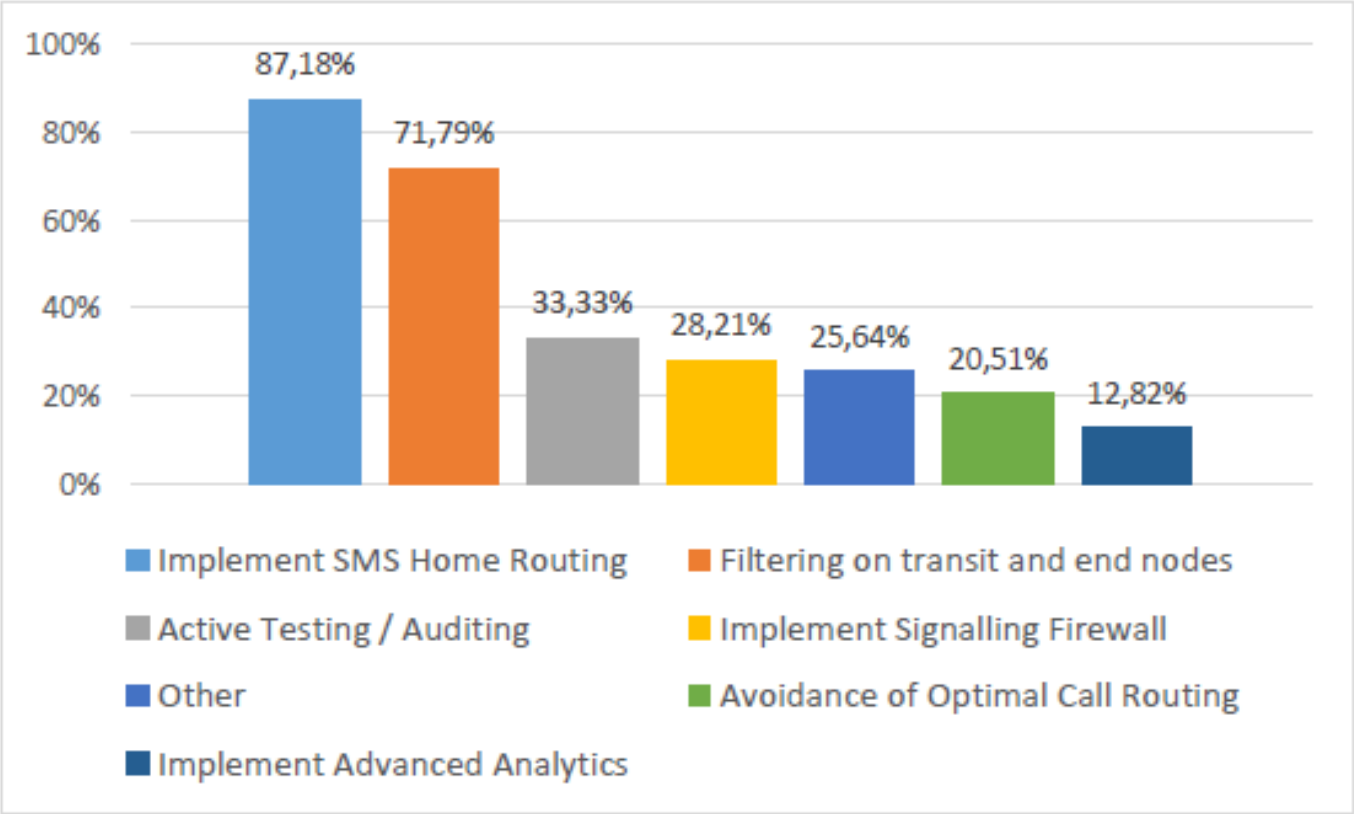


Πηγή: "*SS7 Vulnerabilities and Attack Exposure Report*", Positive Technologies, 2018

Το πρωτόκολλο SS7 – Αντιμετώπιση Ευπαθειών

- Παρακολούθηση κίνησης σε πραγματικό χρόνο
  - Φιλτράρισμα Μηνυμάτων
  - Σε ποιους κόμβους; Στα άκρα του δικτύου; SS7 firewall;
- Διατήρηση αρχείων καταγραφής
  - Εισερχόμενη και εξερχόμενη κίνηση
  - Για πόσο χρόνο; Όγκος δεδομένων; Κόστος…
- Δυνατότητα ανάλυσης αρχείων καταγραφής
  - Στατιστική ανάλυση / Stateful analysis
  - Εύρεση ανωμαλιών και αποκλίσεων από τον «μέσο όρο»
  - Συσχετισμός δικτύου προέλευσης με συνδρομητή
  - Ανάλυση Περιστατικών Ασφάλειας
- Ειδικά μέτρα προστασίας
  - Ενεργοποίηση SMS Home Routing
  - Αποφυγή Optimal Call Routing

Το πρωτόκολλο SS7 – Αντιμετώπιση Ευπαθειών



Πηγή: "*Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation*", ENISA, March 2018

Το πρωτόκολλο SS7 – Αντιμετώπιση Ευπαθειών

- Τεχνικές Συστάσεις GSMA
  - GSMA FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines
    - Τρεις Κύριες Κατηγορίες Μηνυμάτων Σηματοδοσίας
      - Κατηγορία 1: μηνύματα εντός του δικτύου (block)
      - Κατηγορία 2: μηνύματα από home network (intra-packet analysis)
      - Κατηγορία 3: μηνύματα από visited network (advanced inter-packet analysis)
  - GSMA FS.07 SS7 and SIGTRAN Network Security Issues
  - GSMA IR.71 SMS SS7 Fraud Prevention
  - GSMA IR.82 SS7 Security Network Implementation Guidelines
- Global Titles (GT) Black Lists
- Συνεργασία και ανταλλαγή πληροφοριών με άλλους παρόχους
- Ανταλλαγή σηματοδοσίας μέσω συγκεκριμένων «ασφαλών» καναλιών με σημαντικούς διασυνδεδεμένους παρόχους
- Αποφυγή λαθών διαμόρφωσης
- *Συμμόρφωση με Κανονιστικό Πλαίσιο ...*

Ο ρόλος της ΑΔΑΕ

- Κανονιστικό Πλαίσιο ΑΔΑΕ
  - Απόφαση 165/2011, Άρθρο 10 «Πολιτική Ασφάλειας Δικτύου», παρ. 10.3.4 «*… το υπόχρεο πρόσωπο οφείλει να επιλέγει, να ενεργοποιεί και να παραμετροποιεί όλους τους κατάλληλους μηχανισμούς ασφάλειας, εκμεταλλευόμενο τις δυνατότητες και μεθόδους ασφάλειας που διαθέτουν (αναφέρεται ενδεικτικά η κρυπτογράφηση), τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα…*»
- Ερωτηματολόγιο προς παρόχους (2015)
  - Παράγοντες που σχετίζονται με ευπάθειες δικτύων 2G/3G (αλγόριθμοι κρυπτογράφησης, αλγόριθμοι αυθεντικοποίησης, …)
  - Παράγοντες που σχετίζονται με ευπάθειες πρωτόκολλου SS7
- Συστάσεις Σκανδιναβικών χωρών (2015)
- Απάντηση σε Ερωτηματολόγιο της Ευρωπαϊκής Επιτροπής (2016) μέσω Υπουργείου Ψηφιακής Πολιτικής
- **Τεχνική Σύσταση της ΑΔΑΕ για την Αντιμετώπιση Ευπαθειών Δικτύων Κινητής Τηλεφωνίας (2017)**
  - Διαβούλευση με ΕΕΤΤ/παρόχους (2016-2017)
  - Ανακοίνωση Σεπτ. 2017 (όχι δημόσια διαθέσιμη)
- Στο μέλλον:
  - Συνεργασία με άλλους φορείς (Ευρωπαϊκή Επιτροπή, ENISA, ρυθμιστικές αρχές)
  - Εποπτεία, Καταγραφή Κατάστασης, Παρεμβάσεις
  - Μελέτη πρωτόκολλων σηματοδοσίας δικτύων νέας γενιάς

www.adae.gr

Ευχαριστούμε για την προσοχή σας !!!