Γενικές αρχές

κρυπτογράφησης

μέσα από ένα

Case study

Επίθεση σε προσωπική 3G συσκευή μέσω μολυσμένου 3G πυρήνα.

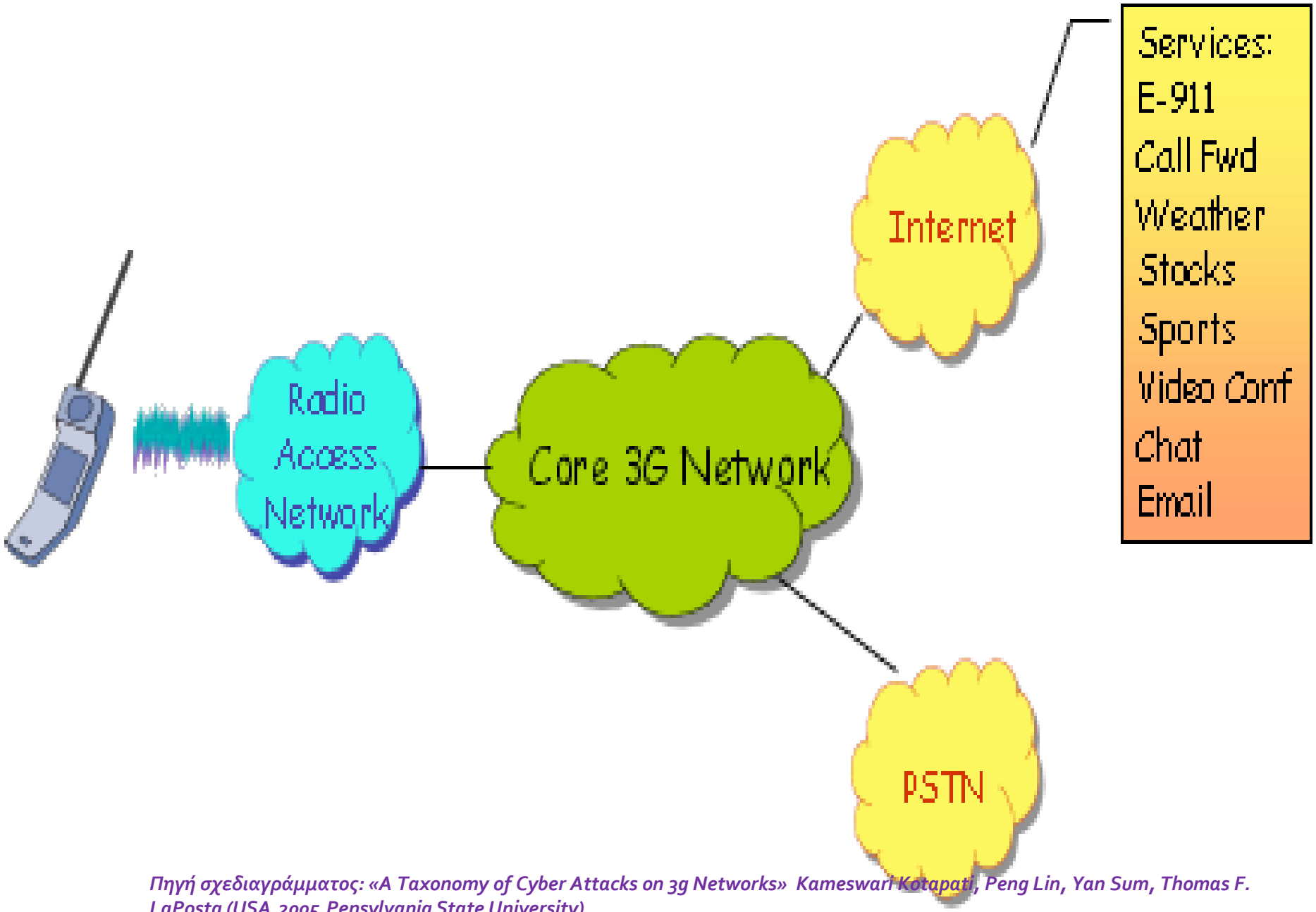
Στοχοποιούμε το άτομο που θέλουμε (π.χ. Διευθυντικό στέλεχος ανταγωνίστριας εταιρίας)

Συλλέγουμε πληροφορίες σχετικά με αυτό από οποιαδήποτε διαθέσιμη πηγή (έρευνα πεδίου, διαδίκτυο, ιστοσελίδες κοινωνικής δικτύωσης κλπ)

Εντοπίζουμε τις περιοχές στις οποίες κινείται το άτομο στόχος (π.χ. περιοχή που βρίσκεται η εταιρία στην οποία εργάζεται και περιοχή κατοικίας του) και την εταιρία κινητής τηλεφωνίας στην οποία είναι συνδρομητής.

Στη συνέχεια εντοπίζουμε τους 3G πυρήνες της εταιρίας κινητής τηλεφωνίας στην οποία είναι συνδρομητής, στις περιοχές που μας ενδιαφέρουν.

Με συγκεκριμένες τεχνικές μολύνουμε τους εν λόγω πυρήνες και αποκτούμε δικαιώματα διαχειριστή σε αυτούς.



Πηγή σχεδιαγράμματος: «A Taxonomy of Cyber Attacks on 3g Networks» Kameswari Kotapati, Peng Lin, Yan Sum, Thomas F. LaPosta (USA,2005,Pensylvania State University).

Εφόσον το επιτύχουμε αυτό, κάθε φορά που ο στόχος μας χρησιμοποιεί τους συγκεκριμένους πυρήνες για την επικοινωνία του, αποκτούμε πρόσβαση στη 3G συσκευή του και στις πληροφορίες που διακινεί μέσω αυτής.

Το τελευταίο ίσως μέσο άμυνας ενάντια σε τέτοιου είδους επιθέσεις, συνιστούν οι τεχνικές κρυπτογράφησης, ειδικά όταν αναφερόμαστε σε ασύρματη διακίνηση δεδομένων όπου η υποκλοπή τους θεωρείται αρκετά εύκολη.

Η κρυπτογράφηση εξασφαλίζει ότι ακόμα και αν κάποιος αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, δεν θα μπορέσει να δει το περιεχόμενό τους.

Προκειμένου η κρυπτογράφηση να είναι λειτουργική θα πρέπει:

-Να παρέχεται «end to end» ασφάλεια στις τελικές συσκευές.
-Να υπάρχει «Point to Point» Κρυπτογράφηση.

Ερωτήσεις;