Πανεπιστήμιο Μακεδονίας
ΔΠΜΣ Πληροφοριακά Συστήματα
Δίκτυα Υπολογιστών
Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia
Master Information Systems
Computer Networks
Professor: A.A. Economides

Εργαλεία οπτικοποίησης των επιθέσεων σε δίκτυα

Network attack visualization tools

Ζαχαριάδου Μάρθα
Α/Μ: 4/13

Ιανουάριος 2014

Πίνακας περιχομένων

1. Περίληψη

Η ασφάλεια των δικτύων αποτελεί στις μέρες μας ένα άκρως επίκαιρο ζήτημα καθώς οι τύποι και οι ζημίες από επιθέσεις διαρκώς πληθαίνουν. Βασικό μέρος του θέματος αυτού αποτελούν και οι τεχνικές οπτικοποίησης των επιθέσεων καθώς βοηθούν στην λήψη μέτρων για την προστασία των δικτύων.

Στην παρούσα εργασία θα αναλύσουμε αρχικά τους όρους «επίθεση» και «οπτικοποίηση» και στην συνέχεια θα γίνει αναφορά σε σχετικά εργαλεία. Πρόκειται για ενδεικτικά συστήματα της πρόσφατης βιβλιογραφίας που αναπτύχθηκαν για να την δημιουργία γραφημάτων και απεικονίσεων των επιθέσεων σε δίκτυα. Παράλληλα με την παρουσίαση των εργαλείων γίνεται αξιολόγησή τους, πάντα σε σύγκριση με αντίστοιχα δείγματα της βιβλιογραφίας.

Abstract

Visualization security helps analysts identify unusual behavior in order to implement the suitable network security policy. Recent studies show that many researchers are working in this field.

In this study we are explaining the terms “network attack”, “visualization” and “network attack visualization tools”. Our main goal though is to present recently developed visualization tools. In addition, we are evaluating them basing our assumptions on recent bibliography.

The above-mentioned tools visualize network traffic and flows using an intuitive way. The produced graphs allow network operators to analyze and fully understand network security vulnerabilities and threats in order to deal with them effectively.

2. Παρουσίαση θέματος

Το θέμα της προστασίας των δικτύων από κακόβουλες επιθέσεις είναι πιο επίκαιρο από ποτέ. Συνεχώς εμφανίζονται νέοι τύποι επιθέσεων ή εξελίσσονται οι ήδη γνωστοί. Οι υπεύθυνοι δικτύων και υποδομών πρέπει να βρίσκονται διαρκώς σε ετοιμότητα για την έγκαιρη αντιμετώπισή τους. Εκτός αυτού, οφείλουν να λαμβάνουν όλα τα απαραίτητα μέτρα πρόληψης για την προστασία των δικτύων.

Η οπτικοποίηση των επιθέσεων σε δίκτυα έρχεται να δώσει λύση στους αναλυτές βοηθώντας τους να κατανοήσουν άμεσα και πλήρως τους τρόπους και τα μέσα με τα οποία ξεκινάει, εξελίσσεται και τελειώνει μια επίθεση. Κλειδί σε αυτή την οπτικοποίηση αποτελεί ο εντοπισμός ασυνήθιστων γεγονότων και ανωμαλιών σε ένα δίκτυο (Best, Bohn,Love, Wynne & Pike, 2010).

Τα εργαλεία οπτικοποίησης επιθέσεων σε δίκτυα αναπτύσσονται τα τελευταία χρόνια έχοντας σαν στόχο την δυναμική αναπαράσταση της κίνησης των δεδομένων σε ένα δίκτυο και την παροχή πολλαπλών προβολών στον χρήστη. Οι προβολές αυτές αφορούν το φιλτράρισμα των δεδομένων σύμφωνα με τις επιλογές του χρήστη και την δυνατότητα παροχής αναλυτικότερων πληροφοριών (Sowmya, Guruprakash, & Siddappa, 2012).

3. Επιθέσεις

1. Ορισμός

Επίθεση σε δίκτυο αποτελεί οποιαδήποτε προσπάθεια μη εξουσιοδοτημένης εισόδου σε ένα σύστημα με σκοπό την οριστική ή μη διακοπή της λειτουργίας του, την κλοπή δεδομένων ή την χρησιμοποίησή του για εξαπόλυση επιθέσεων σε άλλα δίκτυα (Attack (computing)).

Με μια σύντομη αναζήτηση στο διαδίκτυο θα μπορούσε κανείς να ανακαλύψει ένα μεγάλο πλήθος διαφορετικών επιθέσεων που μπορεί να δεχθεί ένα δίκτυο. Μια πρώτη κατηγοριοποίηση θα μπορούσε να γίνει με βάση το σκοπό της επίθεσης σε ενεργητική και παθητική. Ως ενεργητική ορίζεται η επίθεση που έχει στόχο την μετατροπή του τρόπου λειτουργίας των πόρων του δικτύου (δρομολογητές, διακομιστές, εξυπηρετητές κλπ) ή την τροποποίηση ή και καταστροφή των αρχείων του. Ως παθητική ορίζεται η επίθεση που επιδιώκει την κλοπή και χρήση δεδομένων (όπως αρχεία, κωδικοί κλπ) που υπάρχουν στο σύστημα, χωρίς όμως να επηρεάζει την λειτουργικότητα των πόρων του δικτύου. Μια ακόμη κατηγοριοποίηση γίνεται με βάση τον πηγή απ' όπου εξαπολύεται η επίθεση σε εσωτερική και εξωτερική (Attack (computing)).

2. Τύποι επιθέσεων

Παρ' όλα αυτά, επειδή όπως αναφέρθηκε και πιο πάνω το πλήθος των επιθέσεων είναι μεγάλο, θα ήταν πιο χρήσιμο να παρουσιάσουμε σύντομα τους πιο πιο συχνά συναντώμενους τύπους επιθέσεων.

1. Άρνηση εξυπηρέτησης (Denial of Service)

   Ο επιτιθέμενος αποστέλλει ταυτόχρονα ένα τεράστιο πλήθος αιτημάτων για εξυπηρέτηση στον διακομιστή (server) του δικτύου. Αποτέλεσμα αυτού είναι η επιβράδυνση διακοπή της λειτουργίας του συστήματος λόγω της αδυναμίας του να εξυπηρετήσει όλα τα αιτήματα (Διακονικολάου,2007).
2. Ιοί (Viruses)

   Η γνωστότερη μέθοδος επίθεσης σε ένα δίκτυο. Οι ιοί είναι προγράμματα που προσκολλούνται σε άλλα και έτσι μπορούν να προκαλέσουν από μερική μέχρι

ολοκληρωτική καταστροφή των δεδομένων καθώς και βλάβη του λογισμικού ενός συστήματος.

3. Δούρειοι ίπποι (Trojan horses)

   Παρουσιάζονται σαν ένα χρήσιμο πρόγραμμα το οποίο όμως όταν εγκατασταθεί εκτελεί "ύποπτες" λειτουργίες (Διακονικολάου,2007). Ως επί το πλείστον μέσω των δούρειων ίππων, το σύστημα γίνεται υπολογιστής-ζόμπι και χρησιμοποιείται για την εξαπόλυση επιθέσεων σε άλλα δίκτυα.

4. Σκουλήκια (Worms)

   Πρόκειται για αυτόνομα προγράμματα που όταν εισέλθουν σε ένα σύστημα αναπτύσσονται πλήρως και είναι προγραμματισμένα να καταστρέψουν συγκεκριμένα δεδομένα του συστήματος αυτού (Διακονικολάου,2007).

5. Ωτακουστές (Sniffers)

   Οι sniffers παρακολουθούν την κίνηση των πακέτων σε ένα δίκτυο και με ειδικά εργαλεία έχουν την δυνατότητα να ανακτήσουν και να διαβάσουν τα μηνύματα που μεταδίδονται, εάν αυτά δεν είναι κρυπτογραφημένα (Common Types of Network Attacks n.d.).

6. Μεταμφίεση (Spoofing)

   Μέσω του spoofing ο επιτιθέμενος αλλάζει την IP διεύθυνση προέλευσης (source IP) όταν αποστέλλει ένα πακέτο ώστε να το θεωρήσει ο παραλήπτης ως αξιόπιστο. Και η επίθεση που αναφέρεται στην βιβλιογραφία ως «Man in the middle» θα μπορούσε να υπαχθεί σε αυτή την κατηγορία. Και εδώ ο επιτιθέμενος, χρησιμοποιώντας το spoofing, παρεισφρέει ανάμεσα στον αποστολέα και τον παραλήπτη κατά την διάρκεια της επικοινωνίας τους και έχει την δυνατότητα να υποδυθεί έναν από τους δύο για να αποσπάσει πληροφορίες (Common Types of Network Attacks, n.d.).

7. Σάρωση θυρών (Port Scan)

   Πρόκειται για μια προσπάθεια του επιτηθέμενου να ανακαλύψει την κατάσταση των θυρών ενός συστήματος, να δει δηλαδή ποιες είναι ανοιχτές και ποιες κλειστές.

4. Οπτικοποίηση των επιθέσεων σε δίκτυα

1. Ορισμός

Οπτικοποίηση είναι η διαδικασία μετατροπής δεδομένων σε οπτική μορφή (Sowmya, Guruprakash & Siddappa, 2012). Ο όρος αυτός είναι συχνά συναντώμενος στον χώρο το δικτύων σε ό,τι αφορά την προστασία από επιθέσεις. Έτσι προκύπτει ο όρος «οπτικοποίηση των επιθέσεων σε δίκτυα» (Network Attack Visualization) ο οποίος αναφέρεται στην γραφική και εικονική αναπαράσταση δεδομένων και γεγονότων που αφορούν ένα δίκτυο εντοπίζοντας μοτίβα στην κίνηση δεδομένων. Στόχος της οπτικοποίησης είναι να μπορέσει ο παρατηρητής να αναγνωρίσει ασυνήθιστες συμπεριφορές ώστε να δράσει είτε προληπτικά είτε κατασταλτικά απέναντι σε μία επίθεση.

2. Οφέλη

1. Μέσω της οπτικοποίησης παρέχεται ένας διαισθητικός τρόπος αναπαράστασης δεδομένων. Το ανθρώπινο μάτι είναι εκπαιδευμένο στον εντοπισμό μοτίβων μέσα από σύνθετες εικόνες (Choi, Lee & Kim, 2009).
2. Ο όγκος της ροής δεδομένων σε ένα σύστημα είναι τεράστιος και η οπτικοποίηση των ροών διευκολύνει την αναπαράσταση και κατανόησή τους.
3. Η εξαγωγή ενός γραφήματος που βασίζεται σε τρέχοντα δεδομένα παρέχει την δυνατότητα άμεσης κατανόησης του προβλήματος (της επίθεσης) και αντιμετώπισής του.

5. Εργαλεία και τεχνικές οπτικοποίησης

1. Εισαγωγή

Έχουν προταθεί πολλά εργαλεία και τεχνικές οπτικοποίησης των επιθέσεων σε δίκτυα. Άλλες τεχνικές παρουσιάζουν γραφικά τις πιθανές διαδρομές ενός επιτιθέμενου σε ένα δίκτυο, άλλες απεικονίζουν τις αδυναμίες (vulnerabilities) ενός δικτύου, άλλες ταξινομούν πρώτα τις ανωμαλίες σε ένα δίκτυο και στην συνέχεια οπτικοποιούν τα αποτελέσματα (Riad, Elhenawy, Hassan & Awadallah, 2013) κλπ.

Η πλειοψηφία των γραφημάτων στηρίζεται σε δεδομένα από τα συστήματα ανίχνευσης ή πρόληψης εισβολών. Τα συστήματα αυτά παράγουν ειδοποιήσεις για αναμενόμενες επιθέσεις βασιζόμενα είτε σε κάποια αποθηκευμένη υπογραφή (attack signature) είτε σε ανωμαλίες του δικτύου (Evans et al., 2009).

Υπάρχουν βέβαια και εργαλεία που δεν βασίζονται σε συστήματα ανίχνευσης εισβολών, αλλά έχουν αναπτύξει δικά τους μοντέλα και μηχανισμούς για τον εντοπισμό ασυνήθιστων συμπεριφορών ή και επιθέσεων, τις οποίες στην συνέχεια οπτικοποιούν. Η ανάλυση των δεδομένων μπορεί να ξεκινήσει από την ανάλυση της συμπεριφοράς των δραστών του δικτύου ή την επεξεργασία πληροφοριών σχετικά με την κίνηση δεδομένων σε ένα δίκτυο (network traffic) (Best, Bohn, Love, Wynne & Pike, 2010).

Μια ενδιαφέρουσα κατηγοριοποίηση των τεχνικών και των εργαλείων οπτικοποίησης έχει γίνει από τους H.Shiravi, A.Shiravi και A.Ghorbani (2012) η οποία και παρουσιάζεται παρακάτω. Οι ερευνητές έχουν εντοπίσει τα πιο πρόσφατα εργαλεία οπτικοποίησης, έχουν βρει τα κοινά τους χαρακτηριστικά και τα έχουν χωρίσει σε πέντε υποκατηγορίες (Shiravi, Shiravi & Ghorbani, 2012):

1. Αναπαράσταση των hosts/servers (Host/Server Monitoring)
   Τα εργαλεία αυτά αναπαριστούν τους servers και τις συσκευές (hosts) σε ένα δίκτυο με σκοπό να αναδείξουν ασυνήθιστες δραστηριότητες που μπορεί να λαμβάνουν χώρα μεταξύ τους.
2. Εξωτερική/εσωτερική παρακολούθηση (Internal/External Monitoring)
   Οι τεχνικές που ανήκουν στην συγκεκριμένη κατηγορία απεικονίζουν την αλληλεπίδραση των εσωτερικών συσκευών (hosts) με τις εξωτερικές IP.
3. Δραστηριότητα των θυρών (ports)
   Με τις τεχνικές που στοχεύουν στην οπτικοποίηση της δραστηριότητας των θυρών (ports) εντοπίζονται κυρίως ιοί, δούρειοι ίπποι και σκουλίκια. Αυτά τα τρία είδη επιθέσεων έχουν την ιδιότητα να γίνονται αντιληπτά μέσα από την ασυνήθιστη δραστηριότητα των θυρών (ports).
4. Μοτίβα επιθέσεων (attack patterns)
   Τα εργαλεία που ανήκουν σε αυτή την κατηγορία βοηθούν στον εντοπισμό πολλών ειδών επιθέσεων, είτε αυτές ακολουθούν ένα βήμα είτε περισσότερα. Απεικονίζουν όλες τις φάσεις μιας επίθεσης, από της αναγνώριση και το σκανάρισμα του στόχου, μέχρι την

κάλυψη του ίχνους που μπορεί να άφησαν. Είναι η πολυπληθέστερη κατηγορία, προφανώς επειδή απεικονίζουν και αναλύουν σε βάθος όλα τα στάδια μιας επίθεσης.

5. Συμπεριφορά δρομολόγησης (routing behavior)
   Στην συγκεκριμένη κατηγορία, τα εργαλεία παράγουν γραφήματα και απεικονίσεις των μοτίβων δρομολόγησης (routting patterns) σε σχέση με τον χρόνο. Αυτό είναι εφικτό μέσω εργαλείων που χρησιμοποιούν το πρωτόκολλο BGP* (Border Gateway Protocol).

Στην συνέχεια παρουσιάζονται ορισμένα εργαλεία και τεχνικές που αναπτύχθηκαν πρόσφατα για την οπτικοποίηση των επιθέσεων σε δίκτυα.

2. NFlowVis (Fischer, Mansmann, Keim, Pietzko, Waldvogel, 2008)

Σύμφωνα με την κατηγοριοποίηση των H.Shiravi, A.Shiravi και A.Ghorbani (2012) που παρουσιάζεται στην ενότητα 5.1, το NFlowVis είναι ένα σύστημα που χρησιμοποιείται για να απεικονιστούν μοτίβα επιθέσεων σε μεγάλα συστήματα. Πρόκειται για ένα εργαλείο το οποίο εξειδικεύεται στην αποθήκευση και αναπαράσταση μεγάλου όγκου στοιχείων αναφορικά με τις ροές σε ένα δίκτυο. Ακολουθεί την παρακάτω διαδικασία:

1. Αποθηκεύει στοιχεία των ροών δεδομένων σε μεγάλα συστήματα
2. Συνδέει τις ροές με τις ειδοποιήσεις από τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS)
3. Οπτικοποιεί τις παραπάνω ροές συνδέοντας τις εσωτερικές και τις εξωτερικές συσκευές (hosts) σε μια δενδροειδή αναπαράσταση (TreeMap)

Δίνει την δυνατότητα πέντε διαφορετικών προβολών ώστε να μπορεί ο χρήστης να δει με μεγαλύτερη λεπτομέρεια όποια πληροφορία τον ενδιαφέρει. Οι προβολές είναι οι εξής:

1. Γενική προβολή (Overview)
2. Προβολή των δεδομένων του IDS (Intrusion Detection View)
3. Οπτικοποίηση των ροών (Flow visualization)
4. Προβολή των συσκευών (Host view)
5. Μητρώο των ροών στο δίκτυο (Net Flow Records)

*Εξωτερικό πρωτόκολλο δρομολόγησης που χρησιμοποιείται σε TCP συνδέσεις.

Μία είναι η βασική αδυναμία που παρατηρείται στο συγκεκριμένο εργαλείο: η εξάρτησή του από τις ειδοποιήσεις που παράγονται από τα συστήματα ανίχνευσης εισβολών σε ένα δίκτυο (Intrusion Detection Systems - IDS). Έχει αποδειχθεί ότι συχνά τα IDS παράγουν έναν σχετικά μεγάλο αριθμό λανθασμένων ειδοποιήσεων (false positives) (Choi, H, Lee & Kim, 2009). Αυτό λοιπόν είναι πιθανό να οδηγήσει στην εξαγωγή λανθασμένων απεικονίσεων από το NFlowVis.

3. Security Quad and Cube (SQC) (Chang & Jeong, 2011)

Κατασκευάστηκε για να αναδείξει αναμενόμενες επιθέσεις μέσα από έναν μεγάλο όγκο δεδομένων. Τα δεδομένα αυτά προέρχονται από τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS), τα συστήματα παρεμπόδισης εισβολών (Intrusion Prevention Systems - IPS), τα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks - VPN), τα αντιικά προγράμματα και τις συσκευές ενός δικτύου.

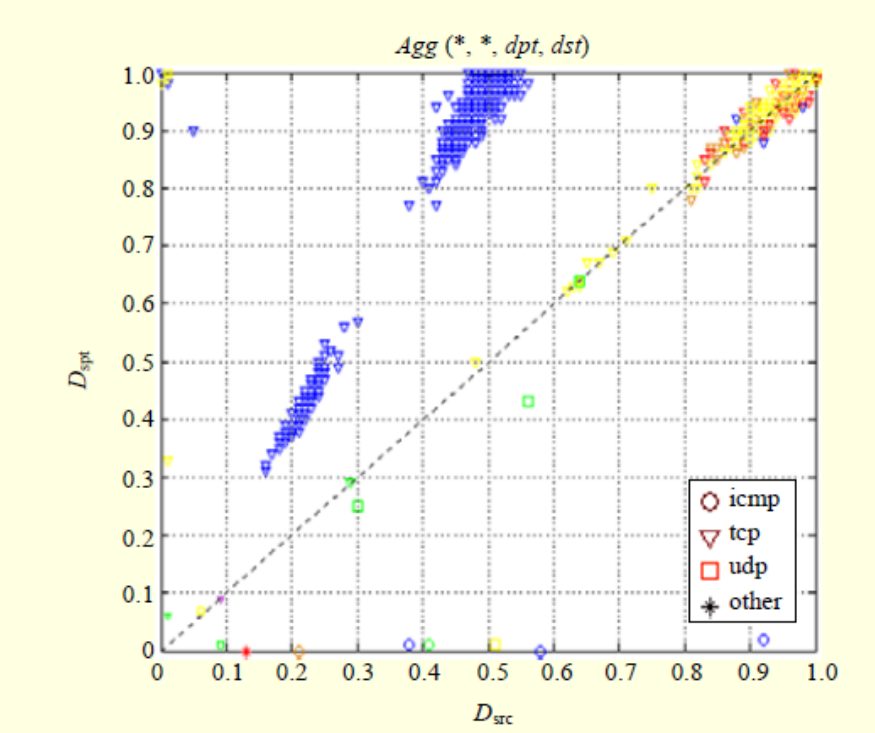
Για κάθε ένα γεγονός που εντοπίζεται αποθηκεύονται πέντε στοιχεία:

1. Αριθμός πρωτοκόλλου* (protocol number - prt)
2. Διεύθυνση IP της πηγής (source IP - src)
3. Αριθμός της θύρας της πηγής (source ort number - spt)
4. Διεύθυνση IP του προορισμού (destination IP address - dst)
5. Αριθμός της θύρας του προορισμού (destination port number - dpt)

Όλα τα γεγονότα (security events) ομαδοποιούνται αρχικά με βάση τον αριθμό πρωτοκόλλου (prt) και στην συνέχεια αθροίζονται με βάση δύο από τα υπόλοιπα στοιχεία.

Quad - Τετράγωνο
Τα δύο επιλεγμένα στοιχεία που αναφέρονται πιο πάνω αποτελούν τον κάθετο και τον οριζόντιο άξονα του γραφήματος. Στο εσωτερικό του αναπαρίστανται όλα τα γεγονότα που παρουσιάζουν κάποια σχέση μεταξύ τους με βάση τα επιλεγμένα χαρακτηριστικά.

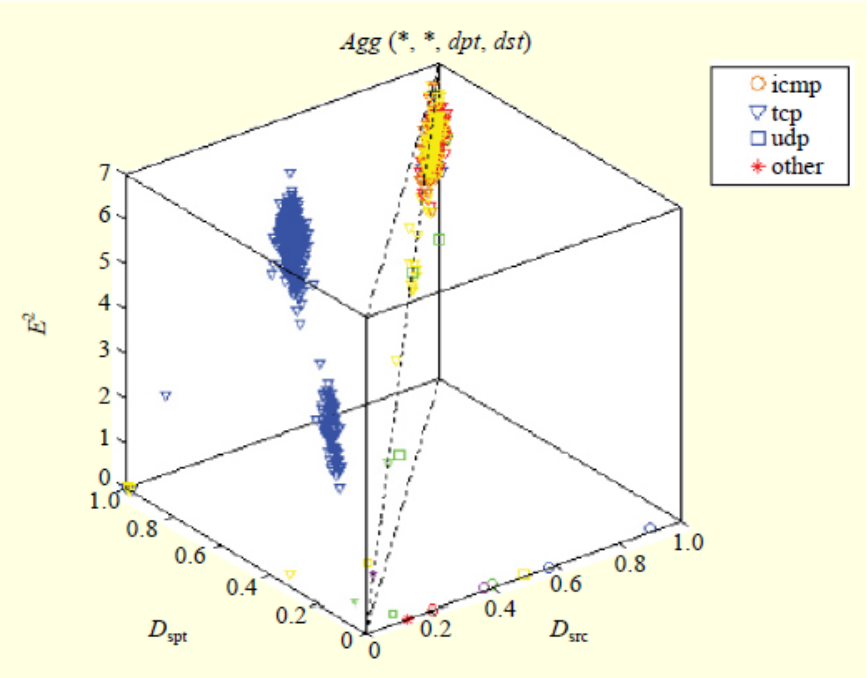
*Προσδιορίζει το πρωτόκολλο διαδικτύου που χρησιμοποιείται σε μία σύνδεση



Εικόνα 1 (Chang & Jeong, 2011)

Cube - Κύβος

Αναδείχθηκε η ανάγκη προσθήκης μίας ακόμα διάστασης γιατί στην αναπαράσταση σε τετράγωνο υπάρχει μία βασική αδυναμία: δεν εμφανίζεται η σταθμισμένη τιμή κάθε γεγονότος που αφορά στην σοβαρότητα της πιθανής επίθεσης. Έτσι δημιουργείται ο κύβος ο οποίος στον άξονα z έχει το E^2. Ο παράγοντας αυτός υπολογίζεται με βάση την πιθανότητα το αποτέλεσμα του γεγονότος να έχει μαζικές επιπτώσεις στο σύστημα. Ουσιαστικά υποδηλώνει το πλήθος των επιθέσεων που επιχειρεί ένας hacker ή cracker. Όσο μεγαλύτερος είναι ο παράγοντας E^2, τόσο μεγαλύτερος ο κίνδυνος από μία επίθεση.



Εικόνα 2 (Chang & Jeong, 2011)

Όπως βλέπουμε στην εικόνα 2, η συνάθροιση (aggregation) γίνεται με βάση την διεύθυνση IP του προορισμού (dst) και τον αριθμό της θύρας του προορισμού (dpt). Στο υπόμνημα πάνω δεξιά βλέπουμε τα πρωτόκολλα απ' όπου προέρχονται τα γεγονότα (icmp, tcp, udp, other) και τα οποία απεικονίζονται χωριστά. Πρόκειται ουσιαστικά για την πρώτη ομαδοποίηση που αναφέραμε με βάση τον αριθμό πρωτοκόλλου. Η συγκέντρωσή τους σε διάφορα σημεία του γραφήματος υποδεικνύει ύποπτη συμπεριφορά. Ως προς τον παράγοντα E^2, τα συγκεντρωμένα κίτρινα σημεία στο επάνω μέρος του γραφήματος, εμφανίζονται να είναι τα πιο επικίνδυνα.

Μετά την παραγωγή των γραφημάτων, το εργαλείο SQC, δίνει την δυνατότητα ομαδοποίησης των επιθέσεων χρησιμοποιώντας δύο αλγόριθμους:

- Με βάση την τοποθεσία (Location Based Clustering)
- Με βάση τα χαρακτηριστικά του δικτύου (Grid-Map Clustering)

Σύμφωνα με την κατηγοριοποίηση των H.Shiravi, A.Shiravi και A.Ghorbani [5], το εργαλείο SQC θα μπορούσε να ενταχθεί στην δεύτερη κατηγορία «εξωτερική/εσωτερική παρακολούθηση (Internal/External Monitoring)» λόγω των δεδομένων βάσει των οποίων παράγονται τα γραφήματα.

Το SQC είναι ένα πολυπαραγοντικό εργαλείο καθώς βασίζεται σε πολλά στοιχεία για την εξαγωγή απεικονίσεων. Αυτό βελτιώνει την εγκυρότητα των εξαγόμενων αποτελεσμάτων καθώς δεν επηρεάζεται μόνο από έναν παράγοντα για να οπτικοποιήσει πιθανές επιθέσεις.

4. RAVEN (Real-time Attack Visualization through Examining Network flows) (Singleton, Young, Harbort, Louthan, Hartney, Pollet, & Hale, 2010)

Βασικός του στόχος είναι η αναπαράσταση των ροών δεδομένων ενός δικτύου σε πραγματικό χρόνο ώστε να εντοπισθούν τυχόν αδυναμίες και ασυνήθιστες συμπεριφορές.
Περιλαμβάνει τρία εργαλεία:

1. Παραγωγή γραφημάτων (Attack Graph Generation)
   Τα δεδομένα που χρησιμοποιούνται για την εξαγωγή γραφημάτων αφορούν κάθε συσκευή (host) του δικτύου, το λειτουργικό σύστημα, τις διευθύνσεις IP με τις οποίες συνδέεται άμεσα μία συσκευή και τις ανοιχτές θύρες (ports) μιας συσκευής. Όλα αυτά τα συνδυάζει ώστε να εντοπίσει τις αδυναμίες του δικτύου αλλά και τα μονοπάτια που μπορεί να ακολουθήσει ένας επιτιθέμενος και στην συνέχεια τις οπτικοποιεί.
2. Ανίχνευση των ροών (Stream Aware Network Detection - SAND)
   Αναγνωρίζει τα πρωτόκολλα επικοινωνίας στο δίκτυο καθώς και τις διευθύνσεις IP τις οποίες συνδέουν και στην συνέχεια αποθηκεύει τις σχετικές ροές σε μία βάση δεδομένων. Οι ροές παραμένουν αποθηκευμένες έως ότου σταματήσει η επικοινωνία ή αλλάξει κάποιο από τα πρωτόκολλα. Έτσι ουσιαστικά συλλέγει τις πληροφορίες που αφορούν τις ροές των δεδομένων σε πραγματικό χρόνο.
3. Δυναμική οπτικοποίηση του δικτύου (Dynamic Visualization of Network Environments - DVNE)
   Απεικονίζει όλους του σταθμούς (nodes) σε ένα δίκτυο και τις μεταξύ του διασυνδέσεις. «Πάνω» σε αυτή την απεικόνιση ενσωματώνονται τα δεδομένα κυκλοφορίας στο δίκτυο (traffic data) που είναι αποθηκευμένα στην βάση δεδομένων. Δίνει την δυνατότητα στον χρήστη να επιλέξει έναν σταθμό (node) ώστε να πάρει περισσότερες πληροφορίες αλλά και να εξάγει ένα αναλυτικότερο γράφημα χρησιμοποιώντας το πρώτο εργαλείο.

Πρόκειται για ένα εργαλείο που συνδυάζει τις ροές δεδομένων σε ένα δίκτυο με τα στοιχεία του συστήματος και πληροφορίες σχετικά με τις αδυναμίες του για την παραγωγή γραφημάτων. Επειδή η απεικόνιση που παρέχει είναι καθαρά εσωτερική (εντός του δικτύου), θα μπορούσε να

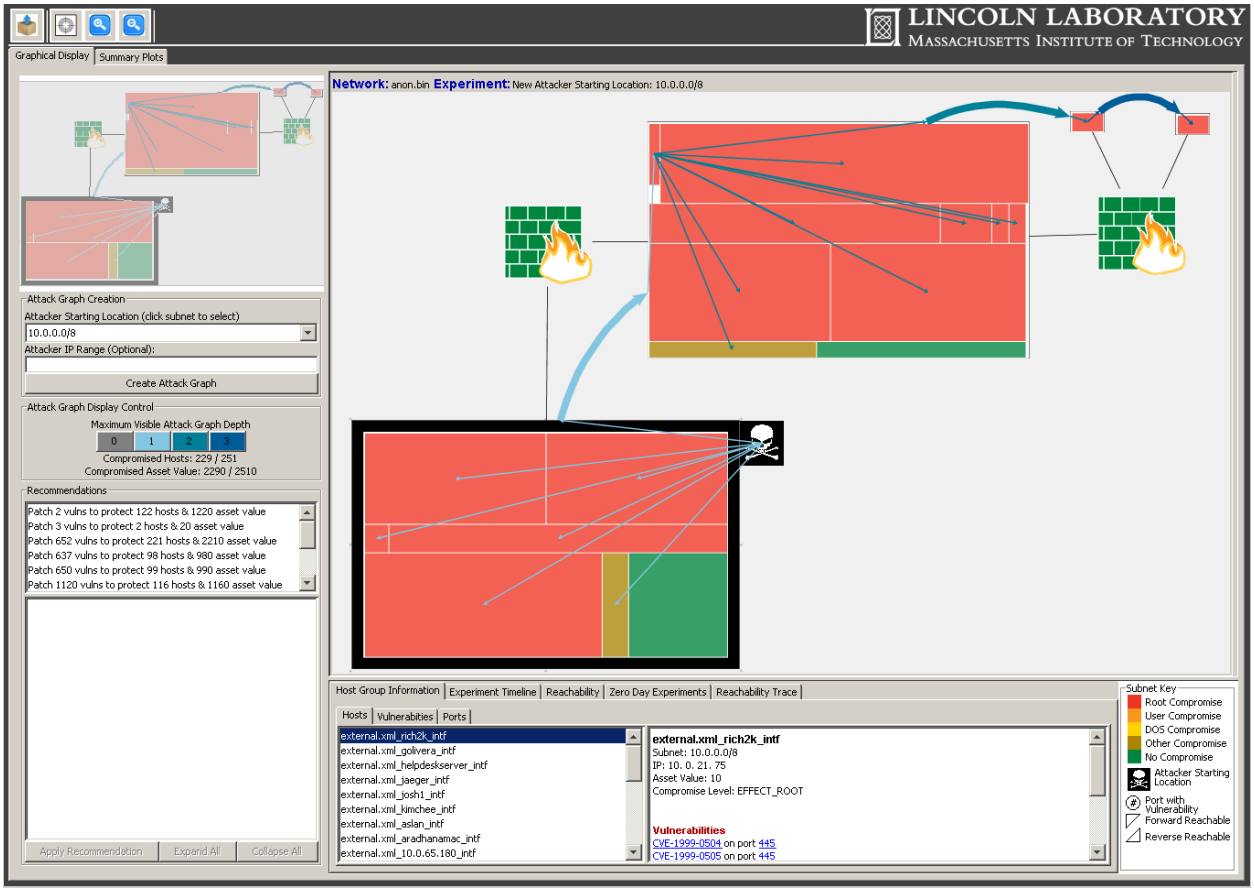
ενταχθεί στην κατηγορία «αναπαράσταση των hosts/servers (Host/Server Monitoring)» σύμφωνα με τους H.Shiravi, A.Shiravi και A.Ghorbani (2012).

5. NAVIGATOR (Network Asset Visualization: Graphs Attacks Operational Recommendations) (Chu, Ingols, Lippmann, Webster & Boyer, 2010)

Το NAVIGATOR χρησιμοποιεί λειτουργικότητες από δύο εργαλεία που αναπτύχθηκαν παλαιότερα τις οποίες εμπλουτίζει με νέα χαρακτηριστικά. Τα εργαλεία αυτά είναι:

1. NetSpa (Network Security Planning Architecture)
   Πρόκειται για ένα εργαλείο οπτικοποίησης επιθέσεων που αναπαριστά τα πιθανά βήματα ενός επιτιθέμενου σε ένα δίκτυο. Με άλλα λόγια ανήκει στην κατηγορία “μοτίβα επιθέσεων (attack patterns)”, όπως αναφέρονται στην ενότητα 5.1. Εκτός αυτού, δέχεται ακατέργαστα δεδομένα ως είσοδο, εφαρμόζει μοντέλα και παράγει αναλυτικές και εξειδικευμένες πληροφορίες.
2. GARNET
   Χρησιμοποιεί τις πληροφορίες που παράγονται από το NetSpa για να εξάγει συμπεράσματα σχετικά με πιθανές επιθέσεις και τρόπους με τους οποίους μπορεί να αμυνθεί το σύστημα.

Στην συνέχεια παραθέτουμε μια εικόνα από το σύστημα ώστε να γίνει καλύτερα αντιληπτή η λειτουργία του.



Εικόνα 3 (Chu, Ingols, Lippmann, Webster & Boyer, 2010)

Στην εικόνα 3, τα υποδίκτυα απεικονίζονται με τετράγωνα και η υποδομή του δικτύου με τα εικονίδια (όπως το τοίχος προστασίας). Με τα διαφορετικά χρώματα διαχωρίζονται τα είδη επιθέσεων όπως αυτά είχαν ήδη οριστεί από το NetSpa. Τα βέλη δείχνουν τα βήματα που μπορεί να ακολουθήσει ένας hacker κατά την διάρκεια μιας επίθεσης.

Γενικότερα οι δυνατότητες που παρέχει το NAVIGATOR είναι οι εξής:

- Ο χρήστης μπορεί να επιλέξει σε τι βάθος θα εμφανιστεί γραφικά μια επίθεση αλλά και ποιο μοντέλο θα εφαρμοστεί. Μπορεί για παράδειγμα να εμφανίσει μόνο τις συσκευές (hosts) του δικτύου κατά ομάδες αλλά και ξεχωριστά.
- Μπορεί να εντοπίσει από ποιο υποδίκτυο θα μπορούσε ένας επιτιθέμενος να εισχωρήσει στο δίκτυο αλλά και πως θα φτάσει εκεί.
- Ο χρήστης μπορεί να εφαρμόσει “what..if” ερωτήματα ώστε να εντοπίσει αν μια «αμυντική τακτική» ενδείκνυται για μια συγκεκριμένη αδυναμία του δικτύου ή προβλεπόμενη επίθεση.

Όπως είναι εύκολα αντιληπτό, σύμφωνα με την κατηγοριοποίηση της ενότητας 5.1, το NAVIGATOR θα μπορούσε να ενταχθεί στην κατηγορία «Εξωτερική/εσωτερική παρακολούθηση (Internal/External Monitoring)».

Τέλος να σημειώσουμε πως το βασικό του πλεονέκτημα είναι πως μπορεί να οπτικοποιεί διαφορετικούς τύπους επιθέσεων.

6. Parallel Coordinate Attack Visualization (PCAV) (Choi, Lee & Kim, 2009)

Πρόκειται για ένα εργαλείο οπτικοποίησης που χρησιμοποιεί ως δεδομένα τις ροές μέσα σε ένα δικτυο και αναπαριστά γραφικά τα στοιχεία τους σε παράλληλους άξονες (parallel coordinates) ωστε να αναδειχθούν πιθανές επιθέσεις. Κάθε είδος επίθεσης σχηματίζει ένα διαφορετικό μοτίβο γραφική απεικόνισης. Με αυτό τον τρόπο είναι δυνατόν να εντοπισθούν επιθέσεις από σκουλίκια, κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (distributed denial of service) αλλά και προσπάθειες σκαναρίσματος των θυρών του συστήματος (port scan).

Το PCAV χρησιμοποιεί τέσσερις παραμέτρους για την ανάλυση των ροών:

- IP διευθύνσεις της πηγής και του προορισμού.
- Αριθμός θύρας (port number) του προορισμού. Βοηθά στο εντοπισμό επιθέσεων από σκουλίκια επειδή συνήθως έχουν ως στόχο μία ή περισσότερες θύρες του δικτύου.
- Μέσο μέγεθος πακέτων. Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης και οι επιθέσεις port scanning χρησιμοποιούν άδεια πακέτα και με την χρήση αυτής της παραμέτρου είναι εύκολο να εντοπιστούν.

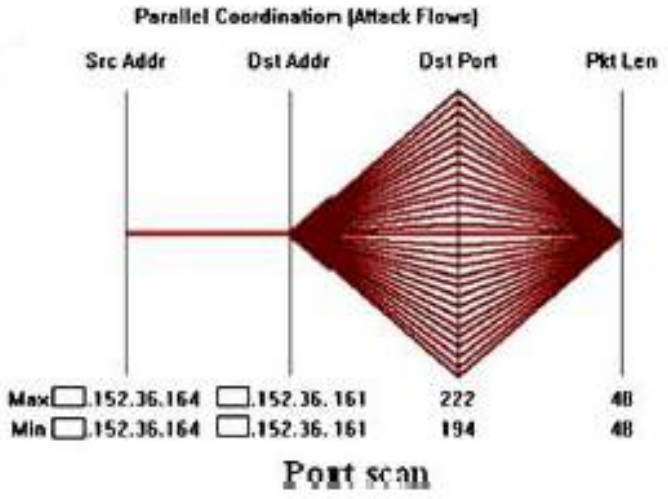
Με βάση τα παραπάνω προκύπτουν εννέα διαφορετικές γραφικές «υπογραφές» (signatures) επιθέσεων οι οποίες φαίνονται στον παρακάτω πίνακα.

Table 1 – Graphical signatures of nine attacks.

Implied Attack	Signature	Divergences
Portscan		1:1:m:1
Hostscan		1:m:1:1
Worm		1:m:1:1
Source-spoofed DoS (port fixed)		m:1:1:1
Backscatter		1:m:m:1
Source-spoofed DoS (port varied)		m:1:m:1
Distributed hostscan		m:m:1:1
Network-directed DoS		m:m:m:1
Single-source DoS		1:1:1:1

Πίνακας 1 (Choi, Lee & Kim, 2009)

Για να αντιληφθούμε πως προκύπτουν τα παραπάνω σχήματα, καλό θα ήταν να δούμε ένα από αυτά με μεγαλύτερη λεπτομέρεια.



Εικόνα 4 (Choi, Lee & Kim, 2009)

Στην εικόνα 4 βλέπουμε την υπογραφή της επίθεσης σάρωσης των θυρών του συστήματος (port scan). Οι παράμετροι που αναφέρονται πιο πάνω αποτελούν τους τέσσερις κάθετους άξονες του γραφήματος. Στο port scan υπάρχει ένα θύμα και ένας επιτιθέμενος ο οποίος επιδιώκει να ανακαλύψει ποιες θύρες (ports) του συστήματος είναι ανοιχτές. Γι' αυτό το λόγο ελέγχει τις θύρες μία προς μία. Με αυτό τον τρόπο προκύπτει το σχήμα της εικόνας 4.

Κλείνοντας, το PCAV ανήκει στην τέταρτη κατηγορία (μοτίβα επιθέσεων) σύμφωνα με την κατηγοριοποίηση των H.Shiravi, A.Shiravi και A.Ghorbani (2012) για προφανείς λόγους. Πρόκειται για ένα εργαλείο αρκετά απλό και αντιληπτό από τον χρήστη. Επειδή όμως το μέγεθος των ροών σε ένα σύστημα είναι συχνά τεράστιο, ίσως να γίνει δύσκολη η αναπαράσταση τους γραφικά και να χρειαστεί κάποιου είδους ομαδοποίηση.

7. Βελτίωση των γραφημάτων

Τα εργαλεία οπτικοποίησης επιθέσεων που αναφέρονται στις προηγούμενες ενότητες είναι ενδεικτικά της σύγχρονης βιβλιογραφίας. Έχουν γίνει όμως και μελέτες οι οποίες προτίνουν τρόπους βελτίωσης των οπτικοποιήσεων μειώνοντας τον όγκο των απεικονιζόμενων πληροφοριών. Έχουμε εντοπίσει δύο τρόπους βελτίωσης και τις παρουσιάζουμε παρακάτω.

- Μείωση των απεικονιζόμενων βημάτων που ακολουθεί ο επιτιθέμενος όταν αυτά δεν βοηθούν τον χρήστη να αντιληφθεί καλύτερα το γράφημα ή την επίθεση. Γι' αυτό το σκοπό έχει προταθεί ένας αλγόριθμος ο οποίος χρησιμοποιεί την απόσταση (μετρημένη σε αριθμό βημάτων) από τον τελικό στόχο ως κριτήριο για την απλοποίηση των γραφημάτων (Hommer, Varikuti, Ou & McQueen, 2008).
- Ομαδοποίηση των παρόμοιων επιθέσεων και απεικόνισή τους ως μία. Μια τεχνική που έχει προταθεί είναι η εφαρμογή αλγορίθμων που χωρίζει τις επιθέσεις σε υποομάδες (Riad, Elhenawy, Hassan & Awadallah, 2013).

6. Συμπεράσματα

Κλείνοντας λοιπόν, θα μπορούσαμε να πούμε πως η πρόσφατη βιβλιογραφία παρουσιάζει ιδιαίτερα χρήσιμα εργαλεία και τεχνικές για την οπτικοποίηση των επιθέσεων σε δίκτυα. Ορισμένα από τα εργαλεία αυτά ωστόσο εμφανίζουν αδυναμία στον εντοπισμό μικρών, πολύπλοκων ή άγνωστων επιθέσεων μέσα από μεγάλους όγκους δεδομένων. Κάποια άλλα αναλύουν και παρουσιάζουν τις ασυνήθιστες ροές χωρίς να εντοπίζουν μοτίβα επιθέσεων, αφήνοντάς το στον χρήστη.

Αδιαμφισβήτητα το κυριότερο πρόβλημα στην ανάπτυξης τέτοιους είδους συστημάτων είναι η διαχείριση του τεράστιου όγκου δεδομένων που χρησιμοποιούν για την εξαγωγή συμπερασμάτων και γραφημάτων. Γι' αυτό άλλωστε προτείνεται η ομαδοποίηση των γεγονότων και των ροών που θα διευκολύνει την απεικόνισή τους.

Ένα άλλο ιδιαίτερα σημαντικό χαρακτηριστικό που θα πρέπει να έχουν τα εργαλεία οπτικοποίησης επιθέσεων σε δίκτυα είναι η δυνατότητα εξαγωγής γραφημάτων σε πραγματικό χρόνο. Μια επίθεση μπορεί να εξελιχθεί μέσα σε ελάχιστο χρόνο. Γι' αυτό το λόγο το σύστημα πρέπει να είναι σε ετοιμότητα για τον εντοπισμό οποιασδήποτε ασυνήθιστης συμπεριφοράς.

Μια πρόταση λοιπόν για μελλοντική έρευνα θα ήταν η δημιουργία ενός συστήματος οπτικοποίησης που θα συγκεντρώνει τα εξής χαρακτηριστικά:

- χειρισμό μεγάλου όγκου δεδομένων σε πραγματικό χρόνο
- εντοπισμό πολύπλοκων επιθέσεων
- αναγνώριση μοτίβων επιθέσεων και ασυνήθιστων συμπεριφορών

Βιβλιογραφία

- ✓ Διακονικολάου, Γ., Αγιακάτσικα, Α., & Μπούρας, Η. (2007). *Επιχειρηματική διαδικτύωση* (2η εκδ.). Αθήνα: Κλειδάριθμος
- ✓ Attack (computing). (n.d.). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Attack_(computing)
- ✓ Best, D. M., Bohn, S., Love, D., Wynne, A., & Pike, W. A. (2010). Real-time visualization of network behaviors for situational awareness. *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, 79-90.
- ✓ Chang, B.-H., & Jeong, C. Y. (2011). An Efficient Network Attack Visualization Using Security Quad and Cube. *ETRI*, *30*(5), 770-778. Retrieved from http://etrij.etri.re.kr/Cyber/Download/PublishedPaper/3305/etrij.oct2011.0770.pdf
- ✓ Choi, H., Lee, H., & Kim, H. (2009). Fast detection and visualization of network attacks on parallel coordinates. *Computers and Security*, 267-288. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808001363
- ✓ Chu, M., Ingols, K., Lippmann, R., Webster, S., & Boyer, S. (2010). Visualizing attack graphs, reachability, and trust relationships with NAVIGATOR. *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, 22-33.
- ✓ Common Types of Network Attacks. (n.d.). Retrieved from http://technet.microsoft.com/en-us/library/cc959354.aspx
- ✓ Evans, S. C., Markham, T., Bejtlich, R., Barnett, B., Scholz, B., Mitchell, R. et al. (2009). Network attack visualization and response through intelligent icons. *Military Communications Conference*, 1-7.
- ✓ Fischer, F., Mansmann, F., Keim, D. A., Pietzko, S., & Waldvogel, M. (2008). Large-Scale Network Monitoring for Visual Analysis of Attacks. *Visualization for Computer Security*, *5210*, 111-118.
- ✓ Harrison, L., Dou, W., Lu, A., Ribarsky, W., & Wang, X. (2011). Guiding Security Analysis through Visualization. *VAST 2011 Mini Challenge #2 Award: "High Potential for Scalability"*, 317-318.
- ✓ Hommer, J., Varikuti, A., Ou, X., & McQueen, M. A. (2008). Improving Attack Graph Visualization through Data Reduction and Attack Grouping. *Visualization for Computer Security*, *251*, 68-79. doi: 10.1007/978-3-540-85933-8_7
- ✓ Ingols, K., Chu, M., Lippmann, R., Webster, S., & Boyer, S. (2009). Modeling Modern Network Attacks and Countermeasures Using Attack Graphs. *Computer Security Application*, 117-126.doi: 10.1109/ACSAC.2009.21

- ✓ Kim, H., Kang, I., & Bahk, S. (2004). Real-Time Visualization of Network Attacks on High-Speed Links. *Real-Time Visualization of Network Attacks on High-Speed Links*. Retrieved from http://netlab.snu.ac.kr/paper/radar.pdf
- ✓ Network Security Types of attacks. (n.d.). Retrieved from http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html
- ✓ Noel, S., & Jajodia, S. (2005). Understanding complex network attack graphs through clustered adjacency matrices.*Computer Security Application*. doi: 10.1109/CSAC.2005.58
- ✓ Port scanning (n.d.). *Wikipedia*. Retrieved from http://el.wikipedia.org/wiki/Port_Scanning
- ✓ Riad, A. M., Elhenawy, I., Hassan, A., & Awadallah, N. (2013). Visualize network anomaly detection by using K-means clustering algorithm. *International Journal of Computer Networks and Communications (IJCNC)*, *5*(5), 195-207. Retrieved from http://airccse.org/journal/cnc/5513cnc14.pdf
- ✓ Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2012). A Survey of Visualization Systems for Network Security.*Visualization and Computer Graphics*, *18*(8), 1313-1329.
- ✓ Singleton, E., Young, M., Harbort, Z., Louthan, G., Hartney, C., Pollet, C., & Hale, J. (2010). RAVEN: Real-time Attack Visualization through Examining Network flows. *Annual Computer Security Applications Conference*.
- ✓ Sowmya, C. L., Guruprakash, C. D., & Siddappa, M. (2012). Visualization of network traffic. *International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN)*, *2*(3), 19-22. Retrieved from http://www.idc-online.com/technical_references/pdfs/data_communications/VISUALIZATION%20OF%20NET.pdf
- ✓ Stockman, N., Vamvoudakis, K., & Devendorf, L. (2012). A Mission-Centric Visualization Tool for Cybersecurity Situation Awareness. Retrieved from http://www.cs.ucsb.edu/research/tech_reports/reports/2012-07.pdf
- ✓ Xie, A., Cai, Z., Tang, C., Hu, J., & Chen, Z. (2009). Evaluating Network Security With Two-Layer Attack Graphs.*Computer Security Application*, 127-136.doi: 10.1109/ACSAC.2009.22
- ✓ Εικόνα εξωφύλλου: http://www.gfi.com/blog/how-to-protect-your-network-against-ddos-attacks/