ΑΝΑΠΤΥΞΗ ΚΙΝΗΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΟΠΤΙΚΗΣ ΕΠΙΘΕΩΡΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ

Βασίλειος Μαυρουδής, Ιωάννης Μαυρίδης
Πανεπιστήμιο Μακεδονίας, Τμήμα Εφαρμοσμένης Πληροφορικής
Εγνατία 156, 54006, Θεσσαλονίκη
it0867@uom.gr, Mavridis@uom.gr

ΠΕΡΙΛΗΨΗ

Η ολοένα αυξανόμενη χρήση των διαδικτυακών διακομιστών απαιτεί την ύπαρξη κατάλληλων μηχανισμών και τεχνικών για την απρόσκοπτη και ελεγχόμενη λειτουργία τους. Η επιθυμία για πρόβλεψη και αποτροπή κακόβουλων ενεργειών που επιχειρούν να απειλήσουν την ομαλή λειτουργία υπολογιστικών συστημάτων στο διαδίκτυο, συνήθως με τη χρήση κατάλληλων διατάξεων αναχωμάτων ασφάλειας, οδηγεί στην ανάγκη για συνεχή καταγραφή και ανάλυση σε πραγματικό χρόνο των δεδομένων που δημιουργούνται κατά τη λειτουργία τους και τη χρήση των παρεχόμενων υπηρεσιών. Σε αυτή την εργασία, παρουσιάζεται η ανάπτυξη ενός κινητού συστήματος οπτικής επιθεώρησης ασφάλειας σε πραγματικό χρόνο, με την ονομασία ΚΑΣΣΙΟΠΕΙΑ (CASSIOPEIA), που αποσκοπεί στη βελτίωση των συνθηκών επίβλεψης και ελέγχου ενός διαδικτυακού διακομιστή από το διαχειριστή του, ώστε να ενισχύεται η δυνατότητα άμεσης αντίδρασης, ακόμη και από απόσταση, σε περίπτωση κρίσιμων για την ασφάλεια του συστήματος συμβάντων.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Ασφάλεια πληροφοριών, οπτικοποίηση δεδομένων, κινητά υπολογιστικά συστήματα, αναχώματα ασφάλειας.

1. ΕΙΣΑΓΩΓΗ

Η εργασία της διαχείρισης ενός δικτυακού αναχώματος (firewall) απαιτεί καλή γνώση του ρόλου του στο υπό προστασία υπολογιστικό σύστημα, καθώς και επαρκή τεχνική κατάρτιση και εμπειρία για θέματα που αφορούν τη διαμόρφωση και λειτουργία του. Οι διαχειριστές αναχωμάτων πρέπει να παρακολουθούν συνεχώς και με όσο το δυνατόν μεγαλύτερη λεπτομέρεια την κατάσταση του συστήματος και να επεμβαίνουν, ρυθμίζοντάς το εκ νέου, σε περίπτωση που αυτό δεν ανταποκρίνεται ικανοποιητικά στις εργασίες που του έχουν ανατεθεί. Γενικότερα, η συμπεριφορά ενός συστήματος μπορεί να μην είναι η αναμενόμενη είτε γιατί η παραμετροποίησή του δεν είναι επαρκής, είτε γιατί κάποιος αστάθμητος παράγοντας (χρήστες, απαιτήσεις εργασιών, κ.ά.) έχει μεταβληθεί (Frisch, 2002). Η παρακολούθηση της λειτουργίας ενός αναχώματος σε πραγματικό χρόνου επιβαρύνεται από παράγοντες όπως η συνεχής ροή συχνά τεράστιου όγκου δεδομένων που διακινούνται από και προς το εσωτερικό του υπό προστασία υπολογιστικού συστήματος (Canavan, 2001), αλλά κυρίως η ανάγκη μετακίνησης του διαχειριστή προκειμένου να ασχοληθεί και με άλλες εργασίες.

Η δυνατότητα καταγραφής συμβάντων σε ένα δικτυακό ανάχωμα αποτελεί σημαντικό εργαλείο για το διαχειριστή συστήματος, αφού έτσι μπορούν να εντοπίζονται ύποπτες δραστηριότητες που πιθανώς απειλούν την ομαλή και ασφαλή λειτουργία των εφαρμογών. Με σκοπό την καταγραφή όλων των συμβάντων που λαμβάνουν χώρα σε ένα διακομιστή και την μετέπειτα επιθεώρησή τους από το διαχειριστή, για κάθε νέο αίτημα δημιουργείται μια εγγραφή στο σχετικό αρχείο καταγραφής (log file). Οι καταγραφές (logs), που δημιουργεί κάθε αίτηση σε μια εφαρμογή, αποτελούν πολύτιμη πηγή δεδομένων για τη διασφάλιση της λειτουργίας της, μέσω της συνεχούς επιθεώρησης της κατάστασης του συστήματος. Έτσι, ο διαχειριστής συστήματος καλείται να εξετάζει τις καταγραφές αυτές και αναλύοντάς τις να διαμορφώνει μια αντιπροσωπευτική εικόνα της κατάστασης του συστήματος. Λόγω όμως του μεγάλου αριθμού δεδομένων, πολλές φορές το έργο της εξαγωγής χρήσιμων πληροφοριών από την εξέταση του περιεχομένου των αρχείων καταγραφής κρίνεται από πολύ δύσκολο έως σχεδόν αδύνατο, κυρίως λόγω του πλήθους των αιτημάτων. Πράγματι, σε ένα αρχείο καταγραφής αποτυπώνεται η δραστηριότητα του συστήματος με λεπτομέρεια που όμως μπορεί να καταλήγει σε μακροσκελείς και δυσανάγνωστες λίστες στοιχείων και τελικά να χάνεται η χρήσιμη πληροφορία για κάποιο ύποπτο συμβάν που εξελίσσεται παράλληλα με άλλα κανονικά αιτήματα (Schweitzer, 2003).

Σε αυτή την εργασία παρουσιάζεται η ανάπτυξη ενός κινητού συστήματος οπτικής επιθεώρησης ασφάλειας σε πραγματικό χρόνο, με την ονομασία ΚΑΣΣΙΟΠΕΙΑ (CASSIOPEIA). Πιο συγκεκριμένα, το σύστημα επεξεργάζεται τις καταγραφές ενός διαδικτυακού διακομιστή που εξυπηρετεί αιτήματα χρηστών, ενώ στη συνέχεια μεταφέρει στη φορητή συσκευή του διαχειριστή συστήματος κατάλληλα διαμορφωμένη και οπτικοποιημένη αναπαράσταση της δραστηριότητας του συστήματος σε πραγματικό χρόνο. Για την επίτευξη των παραπάνω, γίνεται αξιοποίηση διαφόρων τεχνολογιών που αφορούν τη διεπιφάνεια χρήστη, την οπτικοποίηση των καταγεγραμμένων δεδομένων, την ασφαλή διακίνηση δεδομένων μέσω ενσύρματων και ασύρματων (WiFi, 3G) καναλιών επικοινωνίας. Όσον αφορά την οπτικοποίηση και την ανάλυση των δεδομένων, μπορούν να χρησιμοποιούνται εργαλεία δημιουργίας κλαδογραμμάτων (cladogram), δένδρων (dendrogram), χαρτών θερμότητας (heat map) και απεικόνισης σε πολλαπλές διαστάσεις (multidimensional scaling). Με τις παραπάνω μεθόδους (infographics) μπορούν να αναπαρίστανται οπτικά δυσνόητες λίστες κειμενικών καταγραφών, δίνοντας μια πλήρη εικόνα στο πλαίσιο μιας αφαιρετικής απεικόνισης της κατάστασης του συστήματος. Το σύστημα οπτικής επιθεώρησης ασφάλειας ΚΑΣΣΙΟΠΕΙΑ δέχεται ως είσοδο τα δεδομένα καταγραφών, τα οποία αφορούν τη δραστηριότητα του διακομιστή που επιθυμούμε να επιθεωρούμε. Στη συνέχεια, τα δεδομένα μεταφέρονται σε πραγματικό χρόνο στο ενδιάμεσο σύστημα οπτικοποίησης, μέσω ενός ασφαλούς καναλιού μεταφοράς (με χρήση κρυπτογράφησης). Η διαδικασία οπτικοποίησης περιλαμβάνει τη δημιουργία κατάλληλων αναπαραστάσεων της δραστηριότητας του εξυπηρετητή στη βάση κανόνων. Στη συνέχεια, αποστέλλονται τα οπτικοποιημένα αποτελέσματα με κρυπτογραφημένη μορφή στη φορητή συσκευή του διαχειριστή συστήματος.

Το σύστημα ΚΑΣΣΙΟΠΕΙΑ αποσκοπεί στη βελτίωση των συνθηκών επίβλεψης και ελέγχου ενός συστήματος από τον διαχειριστή του, καθώς και στην άμεση αντίδραση σε περίπτωση κρίσιμων για την ασφάλεια του συστήματος συμβάντων.

2. ΟΠΤΙΚΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

Στη σύγχρονη εποχή της πληθώρας πληροφοριών, η απλή επισκόπηση των στοιχείων συχνά αδυνατεί να δώσει μια ολοκληρωμένη εικόνα αυτού που περιγράφουν. Για τον λόγο αυτό, σε περιπτώσεις μεγάλου όγκου δεδομένων επιλέγεται η χρήση κατάλληλων τεχνικών οπτικοποίησης. Με μια τέτοια τεχνική, γίνεται η επεξεργασία των πρωτογενών δεδομένων (raw data) με σκοπό την παραγωγή οπτικών αναπαραστάσεων που περιλαμβάνουν μέρος ή όλα τα στοιχεία που συγκεντρώθηκαν σε μορφή εύκολα κατανοητή από τον άνθρωπο (Θεοχάρης, Παπαϊωάννου, Πλατής & Πατρικαλάκης 2010). Πολύ σημαντική είναι η επιλογή της μορφής με την οποία θα οπτικοποιηθούν τα δεδομένα έτσι ώστε να μην δημιουργηθεί ένα νέο πολύπλοκο αποτέλεσμα αλλά μία περιεκτική αναπαράσταση.

Πέρα από τις συνηθισμένες μορφές διαγραμμάτων που συναντούμε συχνά, είναι δυνατόν να δημιουργηθούν και νέες που θα καλύπτουν απόλυτα τις ανάγκες περιγραφής της τρέχουσας κατάστασης ενός συστήματος και θα είναι βολικότερες για μια γρήγορη επισκόπηση. Στην επιστήμη των υπολογιστών τίθεται συχνά η απαίτηση ώστε η οπτικοποίηση των δεδομένων να ακολουθεί των ροή παραγωγής των πρωτογενών δεδομένων, να συμβαίνει δηλαδή σε πραγματικό χρόνο (realtime). Αυτό οδηγεί σε δυναμικά μεταβαλλόμενες αναπαραστάσεις που αντί να μεταβάλλονται συνολικά δίνοντας έτσι μια εντύπωση μη-συνέχειας, δημιουργούν αντικείμενα για κάθε στοιχείο ή ομάδα αυτών και ανανεώνουν μόνον όσα από αυτά μεταβάλλονται (Moere & Andrew 2004). Οφείλουμε να επισημάνουμε ότι η πραγματικού χρόνου οπτικοποίηση των δεδομένων στην πράξη δεν υφίσταται και συνεπώς έχουμε να κάνουμε με μια «κοντά στον πραγματικό χρόνο» (near-real-time) προσέγγιση. Είναι επιθυμητό, μια τέτοια προσέγγιση να παρουσιάζει μόνο μια μικρή χρονική απόκλιση, η οποία δεν θα επηρεάζει καθόλου την εγκυρότητα της αναπαριστώμενης πληροφορίας (Clark et al, 1992).

3. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ

Το σύστημα ΚΑΣΣΙΟΠΕΙΑ περιλαμβάνει τρία υποσυστήματα: τον επιτηρούμενο διακομιστή, το διακομιστή οπτικοποίησης και την κινητή συσκευή. Η διασύνδεση αυτών των υποσυστημάτων γίνεται μέσω ασφαλών καναλιών μονόδρομης ή αμφίδρομης επικοινωνίας, κατά περίπτωση, μέσω διαδικτύου.

Εικόνα 1. Λειτουργική αρχιτεκτονική - υποσυστήματα.

Τα πρωτογενή δεδομένα παράγονται από τον επιτηρούμενο διακομιστή και στη συνέχεια οπτικοποιούνται από τον αρμόδιο διακομιστή, ο οποίος με τη σειρά του μεταβιβάζει τα αποτελέσματα αυτής της επεξεργασίας στο διαχειριστή μέσω της κινητής συσκευής, που είναι και ο τελικός αποδέκτης (Εικόνα 1).

3.1 Επιτηρούμενος διακομιστής

Ο επιτηρούμενος διακομιστής είναι συνδεμένος με το διαδίκτυο και εξυπηρετεί αιτήματα χρηστών δημιουργώντας ταυτόχρονα μια καταγραφή για κάθε γεγονός, στην οποία περιλαμβάνονται τα στοιχεία του αποστολέα, του αιτήματος και λεπτομέρειες των διακινούμενων πακέτων (Εικόνα 2).

```
204.31.113.138 - - [03/Jul/2006:06:56:12 -0800]"GET /PowerBuilder/Compny3.htm
HTTP/1.0" 200 5593
```

Εικόνα 2. Παράδειγμα καταγραφής γεγονότος.

Στο προτεινόμενο σύστημα, κάνουμε χρήση του λογισμικού αναχώματος που είναι προεγκατεστημένο στην διανομή Ubuntu 10.04 του Linux. Συγκεκριμένα, χρησιμοποιείται το Linux kernel firewall σε συνδυασμό με την εφαρμογή iptables. Η εφαρμογή iptables αποτελεί ένα εργαλείο του διαχειριστή για την παραμετροποίηση των πινάκων (tables) του Linux kernel firewall. Στο σύστημα μας, στον επιτηρούμενο διακομιστή λειτουργεί ένας apache webserver. Οι καταγραφές γεγονότων σε ένα διακομιστή Apache (server) βρίσκονται σε δύο αρχεία στον κατάλογο /var/log/apache2/. Το αρχείο access.log περιλαμβάνει τα αιτήματα που έλαβε και εξυπηρέτησε ο διακομιστής. Στο αρχείο error.log καταγράφονται όλα τα σφάλματα (errors) που δημιουργούνται κατά τη λειτουργία του διακομιστή. Σε περίπτωση που ανιχνευθεί κάποια απειλή για το σύστημα, η εφαρμογή iptables ενημερώνει τον διακομιστή οπτικοποίησης για την ύπαρξή της.

Για την ασφαλή επικοινωνία του αναχώματος με το διακομιστή οπτικοποίησης, χρησιμοποιείται μια υλοποίηση του πρωτοκόλλου SSH (Barett & Silverman, 2003). Ακόμη, γίνεται χρήση ψηφιακών υπογραφών (DSA) κατά την σύνδεση μέσω SSH, με σκοπό την αυτοματοποιημένη σύνδεση των εφαρμογών του διακομιστή οπτικοποίησης με τον επιτηρούμενο διακομιστή (όπου παράγονται τα πρωτογενή δεδομένα καταγραφής συμβάντων), χωρίς να απαιτείται η εισαγωγή ζεύγους ονόματος και συνθηματικού (username – password).

3.2 Διακομιστής οπτικοποίησης

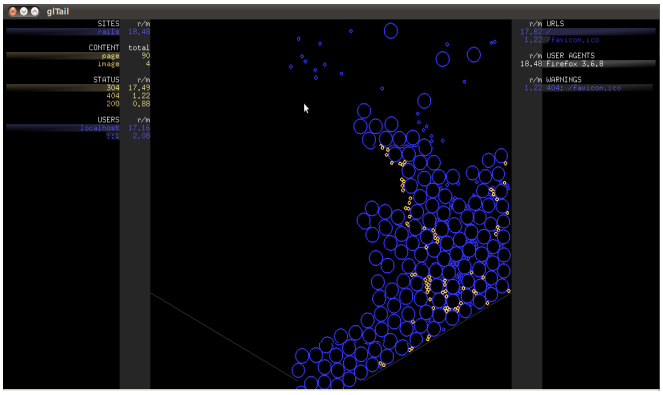
Η διαδικασία της οπτικοποίησης απαιτεί συχνά σημαντικούς υπολογιστικούς πόρους, ανάλογα με τον όγκο των πρωτογενών δεδομένων. Για το λόγο αυτό, επιλέχθηκε να ανατεθεί σε ξεχωριστό υπολογιστικό σύστημα η εργασία αυτή, ώστε να μην επιβαρυνθεί ο επιτηρούμενος διακομιστής.

Ο διακομιστής οπτικοποίησης εκτελεί την εφαρμογή modified gl_tail, που προέκυψε με κατάλληλη παρέμβαση στον κώδικα της αρχικής εφαρμογής gl_tail (Simonsen, 2009), σε περιβάλλον Linux Ubuntu 10.04. Πρόκειται για ένα πρόγραμμα ανοιχτού κώδικα γραμμένο σε Ruby on rails (Bächle & Kirchberg, 2007), που χωρίς να χρειάζεται ιδιαίτερα μεγάλο χώρο για την εγκατάστασή του, είναι ιδιαίτερα αποδοτικό. Διαθέτει διάφορους αναλυτές (parsers), για την ανάλυση των αρχείων καταγραφών ανάλογα με την εφαρμογή από την οποία προέρχονται. Στο σύστημα που αναπτύξαμε, κάναμε χρήση του Apache Webserver Parser, ο οποίος δέχεται ως είσοδο τα δύο αρχεία καταγραφών που διατηρεί κάθε διακομιστής Apache.

Η οπτικοποίηση των καταγεγραμμένων δεδομένων γίνεται με αξιοποίηση του έτοιμου κώδικα της εφαρμογής gl_tail, η οποία αντλεί τα πρωτογενή δεδομένα μέσω μιας σύνδεσης SSH από το απομακρυσμένο σύστημα. Η εικόνα της οπτικοποίησης παράγεται σε πραγματικό

χρόνο, ενώ ταυτόχρονα παρέχονται στατιστικά στοιχεία και πληροφορίες για την δραστηριότητα του συστήματος. Η αναπαράσταση ενός αιτήματος ή σφάλματος γίνεται με την μορφή μιας φυσαλίδας που κινείται στον χώρο και απομακρύνεται. Το χρώμα και το μέγεθος της φυσαλίδας πληροφορούν το διαχειριστή για το είδος και το μέγεθος του αιτήματος. Στο δεξί και στο αριστερό περιθώριο της οθόνης παρουσιάζονται αλφαριθμητικές πληροφορίες που ανανεώνονται συνεχώς, σύμφωνα με τη δραστηριότητα του συστήματος και αφορούν τις ονομασίες των επιτηρούμενων διακομιστών, τον αριθμό σελίδων που εμφανίστηκαν, την κατάσταση (status) για τις απαντήσεις που παρέχει ο επιτηρούμενος διακομιστής στα αιτήματα που δέχεται, τον αριθμό των επισκεπτών, τις διευθύνσεις που ζητήθηκαν και τις ονομασίες των περιηγητών (browsers) που χρησιμοποιούν οι χρήστες (user agents).

Ο πηγαίος κώδικας της εφαρμογής gl_tail έχει τροποποιηθεί (modified gl_tail) έτσι ώστε τα στατιστικά στοιχεία και οι πληροφορίες για την δραστηριότητα του συστήματος, που εμφανίζονται στην οθόνη να αποθηκεύονται στον σκληρό δίσκο. Αυτή η λειτουργία ενσωματώθηκε για να μπορεί ο application server να έχει άμεση πρόσβαση στις τρέχουσες τιμές των στατιστικών στοιχείων με μία ανάγνωση των περιεχομένων ενός αρχείου και στην συνέχεια να τις προωθεί στην κινητή συσκευή. Ακόμη, προστέθηκε λειτουργία ελέγχου των ενεργοποιημένων αλυσίδων κανόνων (chains of rules) των iptables του επιτηρούμενου διακομιστή.



Εικόνα 3. Οπτικοποίηση αιτημάτων με την εφαρμογή gl_tail.

Ο διακομιστής οπτικοποίησης διαθέτει ένα DSA authentication key, το οποίο προσκομίζει στον επιτηρούμενο διακομιστή που εκτελεί το SSH server, προκειμένου να συνδεθεί με αυτόν. Με αυτό τον τρόπο, αποκτά πρόσβαση στα αρχεία καταγραφών (log files), τα οποία και μεταφέρει μέσω του ίδιου ασφαλούς καναλιού με σκοπό την ανάλυση τους από την εφαρμογή gl_tail. Αφού αναλυθούν τα πρωτογενή δεδομένα (αριθμοί ή ρυθμοί σφαλμάτων, επισκεπτών, status κτλ) από τον αντίστοιχο αναλυτή (parser), αποθηκεύονται σε ξεχωριστά αρχεία και ανανεώνονται κάθε φορά που μεταβάλλονται. Επίσης, περιοδικά λαμβάνονται στιγμιότυπα της οθόνης οπτικοποίησης και αποθηκεύονται ως εικόνες.

Για την αποστολή των αποθηκευμένων στοιχείων (αριθμών, κειμένου και εικόνων) στην κινητή συσκευή, έχει δημιουργηθεί ένας διακομιστής εφαρμογών (application server) στον οποίο εκτελείται η εφαρμογή modified gl_tail που ετοιμάζει τη συμβολοσειρά (string) που αποστέλλεται και περιλαμβάνει όλα τα αλφαριθμητικά στοιχεία. Ακόμη, η εφαρμογή modified gl_tail σε τακτά χρονικά διαστήματα ελέγχει την τρέχουσα κατάσταση του επιτηρούμενου διακομιστή ανάλογα με το κατά πόσον αυτός αποκρίνεται ή έχει ενεργοποιηθεί κάποια αλυσίδα

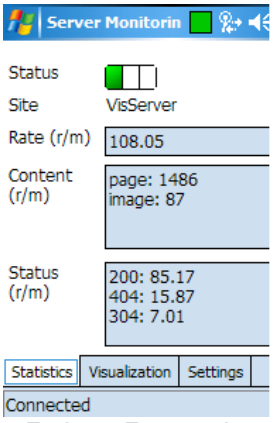
κανόνων (rules chain) των iptables. Ως αποτέλεσμα, διαμορφώνεται ένας κωδικός τρέχουσας κατάστασης του επιτηρούμενου διακομιστή και ενσωματώνεται στη συμβολοσειρά που αποστέλλεται. Οι πιθανές καταστάσεις του επιτηρούμενου διακομιστή τις οποίες αναγνωρίζει το σύστημα ΚΑΣΣΙΟΠΕΙΑ είναι οι ακόλουθες τρεις:

1. Κανονική κατάσταση: είναι η επιθυμητή κατάσταση κατά την οποία ο επιτηρούμενος διακομιστής δεν αντιμετωπίζει κάποια επίθεση και εξυπηρετεί κανονικά τα αιτήματα που δέχεται.
2. Επείγουσα κατάσταση: στην κατάσταση αυτή βρίσκεται ο επιτηρούμενος διακομιστής όταν δέχεται επίθεση. Αν η επίθεση είναι επιτυχημένη το σύστημα περνά σε κατάσταση κρίσης, διαφορετικά μετά το τέλος της ο διακομιστής επανέρχεται σε κανονική κατάσταση. Η εξυπηρέτηση αιτημάτων συνεχίζεται κανονικά κατά την διάρκεια της επίθεσης, εκτός αν διακοπεί προληπτικά από το ανάχωμα ασφαλείας.
3. Κατάσταση κρίσης: ο επιτηρούμενος διακομιστής παύει να εξυπηρετεί τα εισερχόμενα αιτήματα. Κανένα στοιχείο σε σχέση με την κατάστασή του δεν είναι διαθέσιμο, αφού έχει σταματήσει πλέον να αποκρίνεται και κάθε επικοινωνία μαζί του έχει διακοπεί. Ο διαχειριστής πρέπει να επαναφέρει το σύστημα χειροκίνητα.

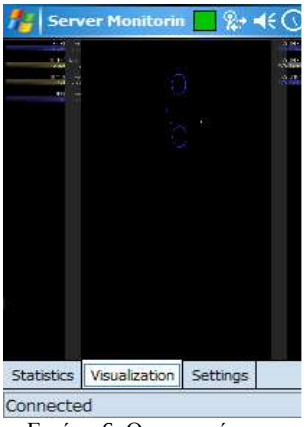
3.3 Κινητή συσκευή

Η κινητή συσκευή αποτελεί τον τελικό αποδέκτη των πληροφοριών, οπτικοποιημένων και μη. Μπορεί να είναι ένα οποιοδήποτε κινητό τηλέφωνο τύπου smartphone, που διαθέτει λογισμικό Windows Mobile και .Net Framework Compact 3.5 (Wigley & Sutton, 2002).

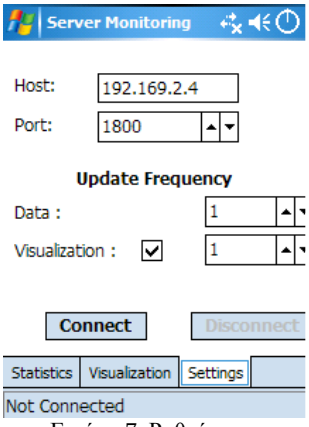
Για την υλοποίηση του προτεινόμενου συστήματος αναπτύξαμε την εφαρμογή ΚΑΣΣΙΟΠΕΙΑ με χρήση της γλώσσας Visual C# .Net (Williams 2002). Η εφαρμογή λογισμικού ΚΑΣΣΙΟΠΕΙΑ ως σκοπό έχει την παρουσίαση στην οθόνη της κινητής συσκευής των δεδομένων που λαμβάνονται από τον διακομιστή οπτικοποίησης και διαθέτει τρεις (3) καρτέλες στις οποίες παρουσιάζονται αλφαριθμητικά στατιστικά στοιχεία και οπτικοποιημένες πληροφορίες για την δραστηριότητα του επιτηρούμενου διακομιστή και ρυθμίσεις της εφαρμογής ΚΑΣΣΙΟΠΕΙΑ.



Εικόνα 5. Στατιστικά στοιχεία



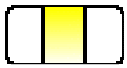
Εικόνα 6. Οπτικοποίηση



Εικόνα 7. Ρυθμίσεις

Πιο συγκεκριμένα, στην πρώτη καρτέλα (Εικόνα 5) παρουσιάζονται: το όνομα του επιτηρούμενου διακομιστή, ο ρυθμός εξυπηρετούμενων αιτημάτων, οι καταστάσεις που επιστρέφει ο επιτηρούμενος διακομιστής ως απαντήσεις στα αιτήματα που δέχεται, καθώς και η τρίχρωμη ένδειξη της τρέχουσας κατάστασης (status) του επιτηρούμενου διακομιστή. Η τρίχρωμη ένδειξη status διαμορφώνεται με βάση τον κωδικό κατάστασης που λαμβάνεται από τη συμβολοσειρά που αποστέλλει ο δοακομιστής οπτικοποίησης (Εικόνα 4) και επιπλέον όταν είναι ελαχιστοποιημένη η εφαρμογή ΚΑΣΣΙΟΠΕΙΑ εμφανίζεται στην μπάρα εργασίας.


Κανονική λειτουργία


Επείγουσα κατάσταση


Κατάσταση κρίσης

Εικόνα 4. Ένδειξη της τρέχουσας κατάστασης (status) του επιτηρούμενου διακομιστή.

Στη δεύτερη καρτέλα, παρουσιάζεται η οπτικοποιημένη δραστηριότητα του επιτηρούμενου διακομιστή, όπως αυτή διαμορφώνεται από την εφαρμογή modified gl_tail και λαμβάνεται μέσω της σύνδεσης ssh από το διακομιστή οπτικοποίησης σε τακτά χρονικά διαστήματα.

Στην τρίτη καρτέλα παρέχεται η δυνατότητα διαμόρφωσης των ρυθμίσεων της εφαρμογής ΚΑΣΣΙΟΠΕΙΑ. Συγκεκριμένα, στις ρυθμίσεις περιλαμβάνεται η παραμετροποίηση της:

- διεύθυνσης (ip address) και της θύρας σύνδεσης (port number) του διακομιστή οπτικοποίησης
- συχνότητας λήψης των στατιστικών στοιχείων δραστηριότητας του επιτηρούμενου διακομιστή
- λήψης ή όχι της εικόνας οπτικοποίησης και της συχνότητας λήψης της

Επίσης, υπάρχουν κουμπιά σύνδεσης (connect) με και αποσύνδεσης (disconnect) από τον application server του διακομιστή οπτικοποίησης.

4. ΛΕΙΤΟΥΡΓΙΑ ΣΥΣΤΗΜΑΤΟΣ

Η επικοινωνία της εφαρμογής ΚΑΣΣΙΟΠΕΙΑ (της κινητής συσκευής) με την εφαρμογή modified gl_tail (του διακομιστή οπτικοποίησης) γίνεται με τη χρήση ενός socket client. Αφού επιτευχθεί η σύνδεση, ο client ξεκινά να ζητά δεδομένα από τον application server και αφού τα λάβει τα εμφανίζει στα πλαίσια κειμένου (textbox) της πρώτης καρτέλας. Μόλις ολοκληρωθεί η αποστολή των δεδομένων, μεταφέρεται ως εικόνα η οπτικοποιημένη δραστηριότητα του επιτηρούμενου διακομιστή και εμφανίζεται στην δεύτερη καρτέλα της εφαρμογής ΚΑΣΣΙΟΠΕΙΑ. Η παραπάνω διαδικασία επαναλαμβάνεται περιοδικά (όπως αναφέρεται προηγουμένως, η συχνότητα ανανέωσης είναι παραμετροποιήσιμη μέσω των ρυθμίσεων της εφαρμογής) και τα εμφανιζόμενα στοιχεία ανανεώνονται ανάλογα. Σε κάθε παραλαβή δεδομένων από τη κινητή συσκευή, αποστέλλεται στο διακομιστή οπτικοποίσης μια επιβεβαίωση λήψης.

Λόγω της συνεχούς αποστολής και λήψης στοιχείων, γίνεται χρήση νημάτων (threads) με σκοπό τη διαφύλαξη της δυνατότητας ανάδρασης του χρήστη (διαχειριστή του επιτηρούμενου διακομιστή), ακόμα και όταν κάποια απαιτητική επεξεργαστικά εργασία βρίσκεται σε εξέλιξη. Επίσης, ο χρήστης έχει την δυνατότητα να προσαρμόσει την συχνότητα λήψης των

αλφαριθμητικών και οπτικών δεδομένων ανάλογα με την ποιότητα της σύνδεσης που διατίθεται τη συγκεκριμένη χρονική περίοδο.

4.1 Ασφαλής μετάδοση δεδομένων

Κατά την λειτουργία του συστήματος ΚΑΣΣΙΟΠΕΙΑ, τα δεδομένα μεταδίδονται μεταξύ των υπολογιστών μέσα από δύο κανάλια επικοινωνίας. Το καθένα από αυτά παρουσιάζει κάποιες ιδιαιτερότητες ανάλογα με τον ρόλο του στο σύστημα. Παρόλο που το ΚΑΣΣΙΟΠΕΙΑ είναι ένα σύστημα επιθεώρησης ασφαλείας, θα πρέπει και τα κανάλια μετάδοσης δεδομένων που χρησιμοποιεί να είναι προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες και υπολογιστές.

4.1.1 Κανάλι επικοινωνίας επιτηρούμενου διακομιστή με διακομιστή οπτικοποίησης

Η μετάδοση δεδομένων ανάμεσα στον επιτηρούμενο και το διακομιστή οπτικοποίησης γίνεται μέσα από μια σύνδεση τύπου Ethernet. Η παρουσία ενός δρομολογητή (router), που θα παίζει τον ρόλο του DHCP server και θα διαμοιράζει τα πακέτα, βοηθά αρκετά στην αξιόπιστη επικοινωνία, χωρίς όμως να είναι και απαραίτητη. Η Ethernet σύνδεση των δύο υπολογιστών από μόνη της παρέχει ένα βασικό επίπεδο ασφαλείας αφού για να παρεμβληθεί κάποιος τρίτος θα πρέπει να έχει φυσική πρόσβαση στο καλώδιο. Λόγω όμως της σημαντικότητας των διακινούμενων δεδομένων, αλλά και της πιθανότητας η σύνδεση να υλοποιηθεί για κάποιο λόγο μέσω ασύρματης ζεύξης, έχει προστεθεί ένα ακόμα επίπεδο ασφαλείας (Khoussainov & Patel, 2000), που χρησιμοποιεί το πρωτόκολλο SSH, όπου οι υπολογιστές έχουν την δική τους ψηφιακή υπογραφή (DSA), ώστε το σύστημα να μην είναι ευάλωτο σε επίθεση πλαστοπροσωπίας (impersonation).

Τα δεδομένα διακινούνται μονόδρομα, από τον επιτηρούμενο διακομιστή προς το διακομιστή οπτικοποίησης, αν εξαιρέσουμε την αποστολή του DSA δημόσιου κλειδιού του διακομιστή οπτικοποίησης κατά την έναρξη (initialization) της επικοινωνίας. Στη συνέχεια, ο διακομιστής οπτικοποίησης αποκτά πρόσβαση σε πραγματικό χρόνο στα αρχεία καταγραφών (log files) του επιτηρούμενου διακομιστή.

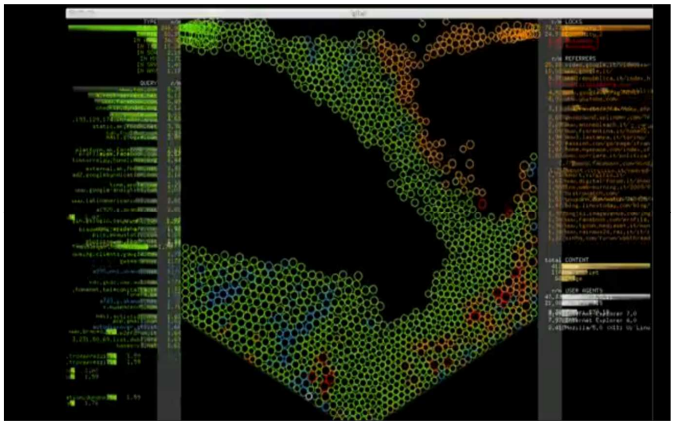
4.1.2 Κανάλι επικοινωνίας διακομιστή οπτικοποίησης με κινητή συσκευή

Η σύνδεση ανάμεσα στο διακομιστή οπτικοποίησης και την κινητή συσκευή πρέπει να χαρακτηρίζεται (πέρα από ασφάλεια) και από ευελιξία, αφού ο διαχειριστής επιθυμεί να έχει άμεση ενημέρωση για την κατάσταση και τη δραστηριότητα του επιτηρούμενου διακομιστή. Για τον λόγο αυτό, η επικοινωνία των δύο υπολογιστών συνήθως υλοποιείται με μια ασύρματη σύνδεση είτε τοπικής εμβέλειας (WiFi), είτε ευρύτερης έκτασης μέσω ενός δικτύου κινητής τηλεφωνίας (GPRS/3G). Στην υλοποίησή μας επιλέξαμε την ασύρματη σύνδεση τοπικής εμβέλειας, καθώς, πέρα από το αισθητά χαμηλότερο κόστος, παρέχει ικανοποιητικά επίπεδα ασφάλειας (με κατάλληλη υλοποίηση του προτύπου IEEE 802.11.i) και λειτουργικότητας. Συνεπώς, παρέχεται ισχυρή αυθεντικοποίηση των συμμετεχόντων μερών και κρυπτογράφηση των διακινούμενων δεδομένων, ώστε να καθιστά αδύνατες επιθέσεις πλαστοπροσωπίας (impersonation), ενδιάμεσου (man-in-the-middle) και υποκλοπής πακέτων (packet sniffing) (Lehr & McKnight, 2003).

Συγκεκριμένα, ο διακομιστής οπτικοποίησης (server) περιμένει μέχρι κάποιος client (κινητή συσκευή) να του στείλει την ειδοποίηση έναρξης σύνδεσης, οπότε και ξεκινάει η ροή δεδομένων. Για κάθε ένα πακέτο που στέλνει ο server, πρέπει να λαμβάνει μέσα σε συγκεκριμένο χρονικό διάστημα μία απάντηση παραλαβής από τον συνδεδεμένο client. Σε περίπτωση που ο client δεν απαντήσει έγκαιρα, η σύνδεση διακόπτεται και ο server αναμένει αίτημα επανασύνδεσης. Τα αλφαριθμητικά δεδομένα αποστέλλονται όλα μαζί με μια συμβολοσειρά (string) όπου χρησιμοποιούνται ως διαχωριστικό οι προκαθορισμένοι χαρακτήρες “|@|”, ενώ η εικόνα της οπτικοποίησης αποστέλλεται ξεχωριστά, αν ζητηθεί από τον client. Η σύνδεση μπορεί να τερματιστεί είτε λόγω διακοπής της επικοινωνίας από φυσικά αίτια, είτε με την αποστολή ενός μηνύματος “exit” από τον client προς τον server.

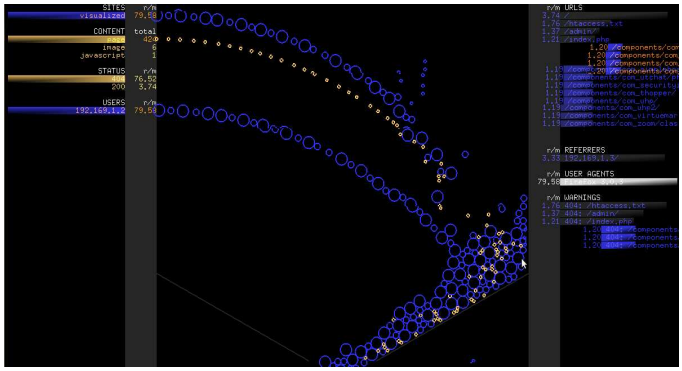
4.2 Μελέτες περιπτώσεων

Αντλώντας από τη βιβλιογραφία αλλά και από τις εμπειρίες δικών μας προσομοιώσεων επιθέσεων, αναφέρουμε στη συνέχεια ορισμένες περιπτώσεις επιθέσεων σε διάφορα είδη διαδικτυακών διακομιστών και παραθέτουμε στιγμιότυπα από τις σχετικές οπτικοποιήσεις δεδομένων καταγραφής που δημιουργούνται από την εφαρμογή gl_tail.



Εικόνα 8. Οπτικοποίηση πραγματικού χρόνου ενός DNS server.

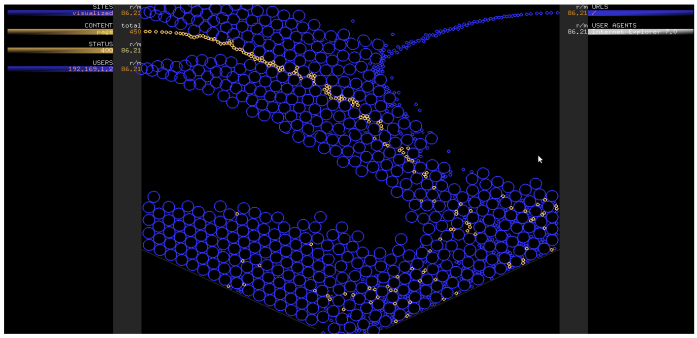
Ένας DNS server δέχεται πολυάριθμα αιτήματα κάθε στιγμή. Παρόλα αυτά, όπως φαίνεται στην εικόνα 8, η οπτικοποίηση σε πραγματικό χρόνο των καταγεγραμμένων κινήσεών του, δημιουργεί ένα σκηνικό που μπορεί να ερμηνευτεί αρκετά εύκολα. Ας υποθέσουμε ότι ο διακομιστής είναι ένας fooldns server (FoolDNS, 2010) που εξυπηρετεί 1300 αιτήματα το λεπτό. Από τα χαρακτηριστικά (μέγεθος, χρώμα) των φυσαλίδων μπορούμε να καταλάβουμε τα είδη των αιτημάτων και των πελατών (client) που εξυπηρετεί. Πιο συγκεκριμένα με πράσινο χρώμα αναπαρίστανται οι πελάτες που βρίσκονται εντός του δικτύου, με μπλέ οι εταιρικοί και με πορτοκαλί και κόκκινο τα αιτήματα που ο fooldns server έχει απορρίψει ως διαφημιστικό περιεχόμενο ή κακόβουλες ιστοσελίδες. Από τα στατιστικά στοιχεία που εμφανίζονται μας δίνεται μια ακριβή εικόνα του συστήματος μέσα από αριθμητικές τιμές, π.χ. ρυθμοί εισερχόμενων αιτημάτων, απόλυτοι αριθμοί πελατών και σελίδων κ.α. (The Fool s.r.l,. 2009).



Εικόνα 9: Οπτικοποίηση επίθεσης στο CMS Joomla.

Με το είδος οπτικοποίησης που χρησιμοποιεί το σύστημα ΚΑΣΣΙΟΠΕΙΑ διακρίνεται άμεσα το slashdot effect (Baryshnikov, Coffman, Pierre, Rubenstein, Squillante & Yimwadsana 2005), καθώς ο διαχειριστής έχει μια συνολική εικόνα των αιτημάτων που δέχεται την τρέχουσα στιγμή ο επιτηρούμενος διακομιστής. Ανάμεσα στα στατιστικά στοιχεία που εμφανίζει η εφαρμογή ΚΑΣΣΙΟΠΕΙΑ βρίσκεται και η αναφέρουσα ιστοσελίδα (referrer) μαζί με τον ρυθμό επισκεπτών που έρχονται από αυτή μέσω κάποιου υπερσυνδέσμου (hyperlink). Κατά την διάρκεια του slashdot effect ο ρυθμός επισκεπτών από μία οι περισσότερες αναφέρουσες ιστοσελίδες είναι ιδιαίτερα αυξημένος (Simonsen 2008).

Στην εικόνα 9 παρουσιάζεται μια επίθεση σε ένα σύστημα διαχείρισης περιεχομένου (CMS), συγκεκριμένα το Joomla.



Εικόνα 10: Οπτικοποίηση επίθεσης DOS.

Τα πολυάριθμα requests από μόνο ένα χρήστη αμέσως φανερώνουν το σοβαρό ενδεχόμενο μιας επίθεσης. Τα ζητούμενα “URLS” και “WARNINGS”, που αναγράφονται στα δεξιά, παρέχουν πολλές πληροφορίες για τον τύπο της επίθεσης. Εκτός από τα αριθμητικά στοιχεία που φανερώνουν την ύπαρξη επίθεσης, η εικόνα που παρέχεται μέσω της οπτικοποίησής τους είναι εντελώς διαφορετική από αυτή που θα παράγονταν σε περίπτωση που ο διακομιστής βρισκόταν σε κατάσταση φυσιολογικής κίνησης. Πιο συγκεκριμένα, ο ρυθμός δημιουργίας των φυσαλίδων, δηλαδή τα εισερχόμενα στον διακομιστή αιτήματα ανά μονάδα χρόνου, είναι πολύ μεγαλύτερος από αυτόν που μπορεί να δημιουργήσει ένας χρήστης που περιηγείται σε κάποια ιστοσελίδα με τον φυλλομετρητή του. Η προσομοίωση της επίθεσης έγινε με τα εργαλεία Joomscan (OWASP, 2009a) και Perl Interpreter (OWASP, 2009b).

Η επίθεση που εμφανίζεται στην εικόνα 10 είναι τύπου άρνησης εξυπηρέτησης (Denial of Service – DOS) για HTTP αιτήματα (Mirkovic & Reiher, 2004) και υλοποιήθηκε με το εργαλείο Slowloris (Rsnake, 2009). Λόγω του τρόπου λειτουργίας της δεν εντοπίζεται εύκολα, αφού δεν ακολουθεί την μεθοδολογία των υπολοίπων επιθέσεων τύπου πλημμύρας (flood attacks) (Chang, 2002). Παρόλα αυτά, μέσω της οπτικοποίησης γίνεται εύκολα αντιληπτή, λόγω των τεράστιου αριθμού των αιτημάτων που εμφανίζονται σχεδόν ταυτόχρονα ως φυσαλίδες στην οθόνη, όπως φαίνεται και στην εικόνα 10. Η συγκεκριμένη επίθεση έχει ως σκοπό να κάνει τον επιτηρούμενο διακομιστή αργό στην απόκρισή του, διατηρώντας ενεργές για μεγάλο χρονικό διάστημα πολλαπλές συνδέσεις TCP.

5. ΤΕΧΝΟΛΟΓΙΚΑ ΖΗΤΗΜΑΤΑ

Κατά την υλοποίηση και λειτουργία του συστήματος, προέκυψαν ορισμένα τεχνολογικά ζητήματα που αξίζει να τα συζητήσουμε σε αυτό το σημείο.

Στο κανάλι επικοινωνίας μεταξύ διακομιστή οπτικοποίησης και κινητής συσκευής, η μετάδοση των δεδομένων γίνεται ασύρματα, οπότε μια επίθεση υποκλοπής δεδομένων μπορεί να στεφθεί με επιτυχία, καθώς η πρόσβαση στο φυσικό μέσο μετάδοσης είναι εύκολη και δεν απαιτεί ιδιαίτερες γνώσεις, αν δεν έχουν γίνει οι κατάλληλες ρυθμίσεις για την ενεργοποίηση του πρωτοκόλλου WPA2 (Lashkari, 2009). Ο οργανισμός Wi-Fi ονομάζει WPA2 ή RSN (Robust Security Network) την εγκεκριμένη υλοποίηση του προτύπου 802.11i (IEEE802.11i, 2004). Το πρότυπο 802.11i κάνει εκτενή χρήση του σύγχρονου κρυπτογραφικού αλγορίθμου δέσμης Advanced Encryption Standard, γνωστού ως AES. Για την πλήρη αξιοποίηση του WPA2 είναι απαραίτητη η χρήση ενός κωδικού με μήκος χαρακτήρων ίσο η μεγαλύτερο του 10 που θα πρέπει να περιλαμβάνει αριθμούς, χαρακτήρες και σύμβολα στίξης. Σε περίπτωση που ο κωδικός δεν πληροί τις παραπάνω προϋποθέσεις, τότε το κανάλι επικοινωνίας θεωρείται ευάλωτο σε επιθέσεις.

Ο ρυθμός εμφάνισης των οπτικών δεδομένων στην κινητή συσκευή, μπορεί να καθορισθεί από το διαχειριστή συστήματος μέσω τις καρτέλας ρυθμίσεων της εφαρμογής ΚΑΣΣΙΟΠΕΙΑ. Στην περίπτωση όμως που ο χρόνος ανανέωσης ρυθμιστεί σε λιγότερα από 2 δευτερόλεπτα, η νέα λήψη της εικόνας ξεκινά πριν ολοκληρωθεί η λήψη της προηγούμενης. Αυτό συμβαίνει λόγω της μεγάλης ανάλυσης και του μεγέθους του μεταδιδόμενου αρχείου εικόνας που αυτή συνεπάγεται και έχει ως αποτέλεσμα να μην προλαβαίνει ο διαχειριστής να εξετάσει προσεκτικά και να αναλύσει την πληροφορία που εμφανίζεται στην οθόνη της κινητής συσκευής. Η μεγάλη ανάλυση της εικόνας οπτικοποίησης δημιουργεί ένα ακόμα ζήτημα αφού η ανάλυση και το μέγεθος της οθόνης μίας κινητής συσκευής είναι συνήθως μικρότερο αυτού ενός προσωπικού υπολογιστή. Έτσι θα πρέπει να εμφανιστεί προσαρμοσμένη στην μικρότερου μεγέθους οθόνη και συνεπώς κάποιες λεπτομέρειες δεν θα είναι πλέον ορατές, χωρίς την εφαρμογή της λειτουργίας μεγέθυνσης/σμίκρυνσης (zoom). Ο βαθμός εφαρμογής της λειτουργίας μεγέθυνσης/σμίκρυνσης μπορεί να παίξει μεγάλο ρόλο στην παρατήρηση ύποπτης κίνησης (traffic). Όμως, η πολυπλοκότητα που εισάγεται από τις πολυάριθμες ρυθμίσεις, μπορεί να αντισταθμίσει τα οφέλη που παρέχει η οπτικοποίηση δεδομένων με σκοπό τη συνολική και γρήγορη επισκόπηση της κατάστασης του επιτηρούμενου διακομιστή.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η οπτικοποίηση των καταγεγραμμένων δεδομένων κατάστασης, ως εργαλείο για την συνεχή επιθεώρηση της ασφάλειας ενός υπολογιστικού συστήματος, μπορεί να προσφέρει σημαντικές λύσεις ειδικά για περιπτώσεις διακομιστών των οποίων η σημαντικότητα των λειτουργιών που επιτελούν απαιτεί αδιάλειπτη λειτουργία (100% uptime). Με την αξιοποίηση της φορητότητας από το προτεινόμενο σύστημα ΚΑΣΣΙΟΠΕΙΑ παρέχεται μια αποτελεσματική λύση στη βάση απεικόνισης της κατάστασης του επιτηρούμενου συστήματος. Αν και η χρήση κινητής συσκευής θέτει περιορισμούς και αστάθεια στη μετάδοση των οπτικοποιημένων δεδομένων, αφού είναι δύσκολο να εξασφαλιστεί η ύπαρξη καλής σύνδεσης παντού και πάντα, εν τούτοις εισάγει πολλά από τα πλεονεκτήματα του σύγχρονου παραδείγματος της διάχυτης υπολογιστικής (pervasive computing). Για την ενίσχυση του βασικού χαρακτηριστικού της «ελεύθερης-περισπασμού» (distraction-free) χρήσης υπολογιστών (Elliott & Phillips 2004), σχεδιάζουμε να προσθέσουμε λειτουργίες σημασιολογικής ανάλυσης των καταγεγραμμένων δεδομένων και αυτόματης ειδοποίησης του χρήστη-διαχειριστή μέσω κατάλληλων ηχητικών σημάτων, ώστε να μην χάνεται μέρος της πληροφορίας κατάστασης στα χρονικά διαστήματα κατά τα οποία ο διαχειριστής δεν έχει εστιασμένη την προσοχή του στην οθόνη της κινητής συσκευής.

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

Θεοχάρης Θ., Παπαϊωάννου Γ., Πλατής Ν. και Πατρικαλάκης Ν.Μ., 2010. *Γραφικά και Οπτικοποίηση - Αρχές και αλγόριθμοι*. Συμμετρία, Αθήνα.

Bächle M. and Kirchberg P., 2007. Ruby on Rails, IEEE Software, vol. 24, no. 6, pp. 105-108.

Barrett D. D. and Silverman R., 2003. *SSH, the Secure Shell: The Definitive Guide*. O'Reilly Media, Sebastopol.

Baryshnikov Y., Coffman E., Pierre G., Rubenstein D., Squillante M. and Yimwadsana T., 2005. Predictability of Web-server traffic congestion. *Web Content Caching and Distribution, 2005. WCW 2005. 10th International Workshop on*, French Riviera, France, pp. 97 - 103.

Canavan J., 2001. *Fundamentals of Network Security.* Artech House, Norwood.

Clark D., Shenker S. and Lixia Z., 1992. Supporting real-time applications in an Integrated Services Packet Network: architecture and mechanism. *ACM SIGCOMM Computer Communication Reviewal*, Volume 22, Issue 4, pp 14 – 26.

Chang R., 2002. Defending against flooding-based distributed denial-of-service attacks: a tutorial. *Communications Magazine, IEEE*, Volume 40, pp. 42 – 51.

Elliott G. and Phillips N., 2004. *Mobile Commerce and Wireless Computing Systems*, Pearson Education Limited, Essex, England.

FoolDNS, 2010. FoolDNS business, Fool DNS community, http://www.fooldns.com/fooldns-community/english-version/

Frisch E., 2002. *Essential System Administration, Third Edition*. O'Reilly Media, Sebastopol.

IEEE802.11i 2004, IEEE, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

Khoussainov R. and Patel A., 2000. LAN security: problems and solutions for Ethernet networks. *Computer Standard and Interfaces 2000*, pp 191-202.

Lashkari A., 2009. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *2009 2nd IEEE International Conference on Computer Science and Information Technology*. Beijing, China, pp. 48-52.

Lehr W. and McKnight L., 2003. Wireless Internet access: 3G vs. WiFi?. *Telecommunications Policy*, Volume 27, Issues 5-6, pp 351-370.

Mirkovic L. and Reiher P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, Volume 34, Issue 2, pp. 39 – 53.

Moere, E. and Andrew, V., 2004. Time-Varying Data Visualization Using Information Flocking Boids. *Proceedings of IEEE Symposium on Information Visualization*. London, England, UK, pp 409 – 414.

OWASP, 2009a. Joomla Vulnerability Scanner Project, OWASP, http://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project.

OWASP, 2009b. OWASP, owasp the free and open application security community, http://www.owasp.org/index.php/Main_Page.

RSnake, 2009. Slowloris HTTP DoS, ha.ckers, http://ha.ckers.org/slowloris/

Schweitzer D., 2003. *Incident Response: Computer Forensics Toolkit.* Wiley, Indianapolis.

Simonsen E., 2009. Fudge, github, http://github.com/Fudge/gltail.

Simonsen E., 2008. glTail - Slashdot effect, YouTube, http://www.youtube.com/watch?v=eV5-EhBXZyQ.

The Fool s.r.l., 2009. Visualizing DNS queries using glTail, thefool, http://www.thefool.it/2009/07/25/how-to-visualize-dns-queries-using-gltail/.

Wigley A. and Sutton M., 2002. *Microsoft .Net Compact Framework: Core Reference.* Microsoft Press, Redmond.

Williams M., 2002. *Microsoft Visual C# :Core Reference.* Microsoft Press, Redmond.