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

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

Attacks in Cloud Networking

της Γεωργίας Γρηγοριάδου – mis1313

Θεσσαλονίκη 2014

Επιθέσεις στο Cloud Networking

Περίληψη

Το cloud networking, μια από τις πιο δημοφιλείς αρχιτεκτονικές τα τελευταία χρόνια, είναι μια τεχνολογία η οποία αναπτύχθηκε μετά την εμφάνιση του Διαδικτύου, για να αντιμετωπίσει τις συνεχώς αυξανόμενες απαιτήσεις για επεξεργασίας και αποθήκευσης. Σε συνδυασμός με την μείωση του κόστους των ηλεκτρονικών υπολογιστών, οι προσφερόμενες υπηρεσίες του cloud computing διατίθενται όλο και περισσότερο. Το cloud computing ή όπως θα λέγαμε στα ελληνικά «υπολογιστική νέφους», παρέχει ή νοικιάζει υπηρεσίες πληροφορικής, γνωστές ως «on-demand computing» σε επιχειρήσεις, οι οποίες χρεώνονται ανάλογα με τις υπηρεσίες που χρησιμοποιούν και με τις ανάγκες και τις απαιτήσεις τους.

Ωστόσο, παρά τα σημαντικά οφέλη, που προσφέρουν αυτές οι τεχνολογίες παρουσιάζονται ζητήματα που αφορούν την ασφάλεια του δικτύου, συμπεριλαμβανομένων τον μικρότερο έλεγχο ή και την έλλειψη ασφάλειας. Στην παρούσα εργασία, παρουσιάζονται τα θέματα ασφάλειας, οι απειλές που προκύπτουν από επιθέσεις και οι πιθανοί τρόποι αντιμετώπισης σε ένα Cloud networking.

Abstract

The cloud networking, one of the most popular architectures in recent years, is a technology that was developed after the advent of the internet, to meet the increasing demands for computer processes. Due to the reduction of technologies cost, cloud computing services are becoming increasingly available. Cloud providers offer services, known as «on-demand computing», and the charge is depending on the services users use and need.

However, despite the significant benefits offered by these technologies it has some security issues, including the less control or insecurity of the data. In this paper, we present security issues, threats arising from attacks and potential countermeasures to a Cloud networking.

Εισαγωγή

Το cloud networking, μια από τις πιο δημοφιλείς αρχιτεκτονικές τα τελευταία χρόνια, αναπτύσσετε ταχέως προσφέροντας μια νέα αναδυόμενη πλατφόρμα πληροφόρησης παροχής υπηρεσιών διαμοιραζόμενων πόρων, το οποίο δίνει μια εναλλακτική λύση στη συμβατική δικτύωση υπολογιστών. Είναι μια τεχνολογία η οποία αναπτύχθηκε μετά την εμφάνιση του Διαδικτύου, για να αντιμετωπίσει τις συνεχώς αυξανόμενες απαιτήσεις για επεξεργασίας και αποθήκευσης. [1]

Σε συνδυασμός με την μείωση του κόστους των ηλεκτρονικών υπολογιστών, οι προσφερόμενες υπηρεσίες του cloud computing διατίθενται όλο και περισσότερο. Κατά συνέπεια, οι πάροχοι υπηρεσιών πληροφορικής είναι αντιμέτωποι με τις προκλήσεις της επέκτασης των δομών και υποδομών με μικρό κόστος και σε σύντομο χρονικό διάστημα, προκειμένου να ανταποκριθούν στην συνεχώς αυξανόμενη ζήτηση των πελατών τους.

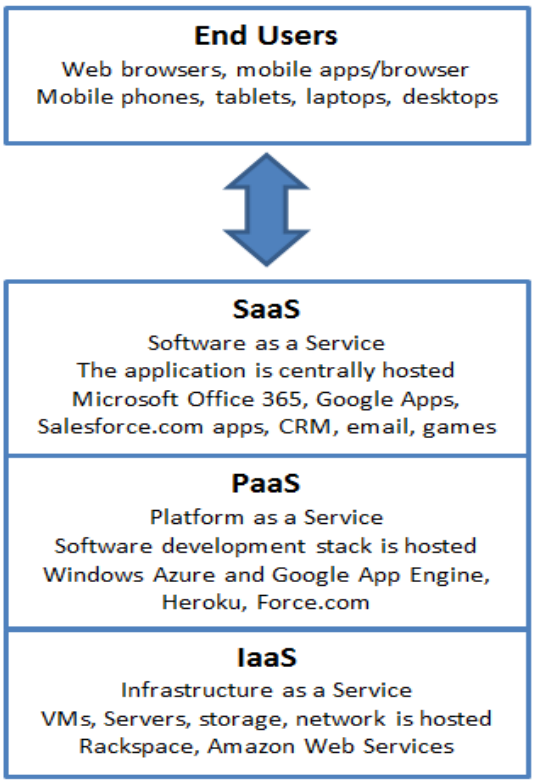
Το cloud computing ή όπως θα λέγαμε στα ελληνικά «υπολογιστική νέφους», παρέχει ή νοικιάζει υπηρεσίες πληροφορικής, γνωστές ως «on-demand computing» σε επιχειρήσεις, οι οποίες χρεώνονται ανάλογα με τις υπηρεσίες που χρησιμοποιούν και με τις ανάγκες και τις απαιτήσεις τους.

Ωστόσο, ένα σημαντικό θέμα ασφάλειας που προκύπτει από την διαχείριση των δεδομένων που τοποθετούνται στο Cloud, είναι επιθέσεις που μπορεί να απειλήσουν την ακεραιότητά τους. Σε μεγάλες υπολογιστικές μονάδες, όπως τα δίκτυα και το cloud, h έγκαιρη ανίχνευση των επιθέσεων είναι πολύ σημαντική. Λόγω του διαμοιρασμού του δικτύου από πολλούς χρήστες σε παγκόσμιο επίπεδο, αυτές οι επιθέσεις, οι οποίες ανιχνεύονται ακόμα και με μια μικρή καθυστέρηση μπορεί να προκαλέσουν πολύ σοβαρές συνέπειες στους χρήστες. Γνωρίζοντας ότι οι χρήστες από διαφορετικούς οργανισμούς μπορεί να έχουν πρόσβαση σε διαφορετικά cloud δίκτυα, είναι πολύ πιθανό σε ορισμένα

από αυτά, οι υπηρεσίες τους να μην είναι πολύ ασφαλείς στο δίκτυο. Αυτό μπορεί να συμβεί διότι μπορεί τα μηχανήματά τους να μην είναι ασφαλή, ή λόγω έλλειψης anti-virus και firewalls του δικτύου, ή γιατί δεν έχουν καθόλου ή έχουν τεθεί κακές πολιτικές ασφάλειας στο τοπικό τους δίκτυο. Αυτοί οι χρήστες είναι ευάλωτοι στις επιθέσεις και μπορεί να αποτελέσουν την κύρια αιτία διανομής επιθέσεων σε ασφαλείς χρήστες. [17]

Υπηρεσίες Cloud

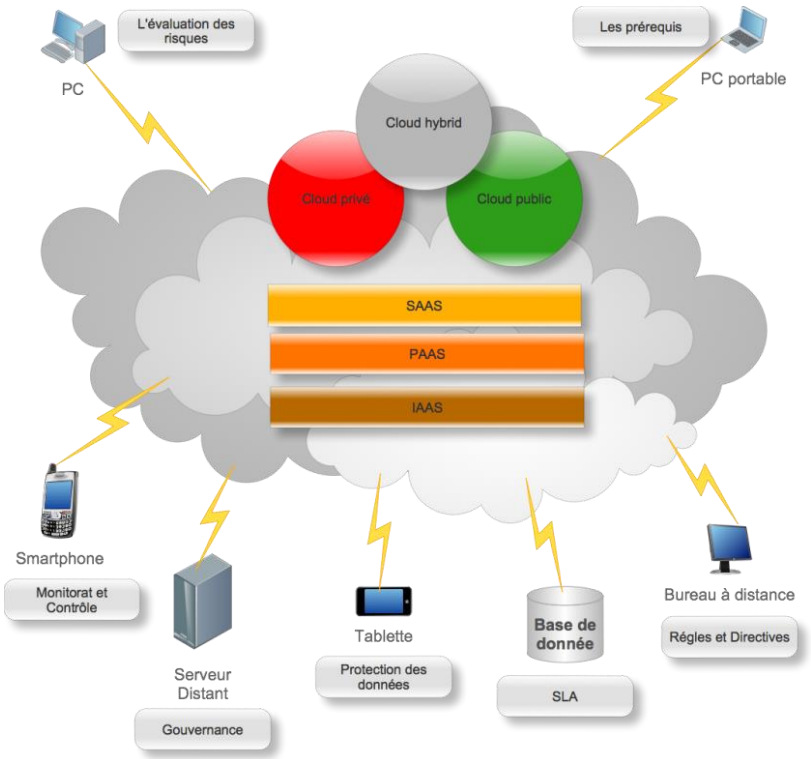
Οι υπηρεσίες που προσφέρει το Cloud computing αφορούν σε επίπεδο υπολογιστικής υποδομής (Infrastructure as a Service - IaaS), σε επίπεδο πλατφόρμας (Platform as a Service - PaaS), σε επίπεδο λογισμικού (Software as a Service - SaaS). [2]



Πηγή: http://tritoneco.com/wp-content/uploads/2012/07/Cloud-Stack-Diagram.png

Ενώ τα μοντέλα ανάπτυξης είναι: ***Private cloud***, ***Community cloud***, ***Public cloud***, ***Hybrid cloud***.

- *Private cloud:* οι πόροι του χρησιμοποιούνται από έναν οργανισμό και μόνο, προκειμένου να εξασφαλίζεται η ασφάλεια των δεδομένων και ο απόλυτος έλεγχος των πόρων του cloud.
- *Community cloud:* χρησιμοποιούνται από πολλούς οργανισμούς οι οποίοι εργάζονται στο ίδιο αντικείμενο ή έχουν τους ίδιου στόχους και κοινούς σκοπούς.
- *Public cloud:* χαρακτηρίζεται ως το πιο κοινό, όπου ο χρήστης μπορεί να χρησιμοποιήσει τις υπηρεσίες του είτε δωρεάν είτε με χρέωση ανάλογα με τη χρήση.
- *Hybrid cloud:* είναι ο συνδυασμό ***Community cloud*** ή ***Public cloud***. Οι χρήστες του επωφελούνται από ποικιλία παρεχόμενων υπηρεσιών οι οποίες είναι είτε ελεγχόμενες είτε διαθέσιμες για δημόσια χρήση. [3]



Πηγή: http://commons.wikimedia.org/wiki/File:Cloud_computing_map.png

Ασφάλεια

Ένας από τους κύριους ανασταλτικούς παράγοντες που προβληματίζουν τους διευθυντές πληροφορικής, για την μετάβαση στο cloud computing είναι ζητήματα που αφορούν το θέμα της ασφάλειας των δεδομένων, της απώλειας του ελέγχου ουσιαστικά, τοποθετώντας τα δεδομένα στο δίκτυο του παροχέα υπηρεσιών. Υπάρχουν 3 είδη δεδομένων στο cloud computing. Το πρώτο αφορά τα δεδομένα που μεταφέρονται (transmission data), το δεύτερο τα δεδομένα που αποθηκεύονται (storage data) και το τρίτο τα δεδομένα προς επεξεργασία (processing data).[5]

Τα στοιχεία που τοποθετούνται στο cloud μπορεί να καταχραστούν ή κινδυνεύουν από μη εξουσιοδοτημένους χρήστες και χωρίς ο χρήστης ή ο ιδιοκτήτης τους να το αντιληφθούν. [4]

Για να μειώσουν τις αμφιβολίες αυτές, οι πάροχοι υπηρεσιών cloud πρέπει να αναπτύσσουν συστήματα ασφαλείας και ελέγχου ώστε να εξασφαλίζεται μεγαλύτερη ασφάλεια από αυτήν που ήδη οι χρήστες έχουν όταν δεν χρησιμοποιούν το cloud. [5]

Γι’ αυτό είναι απαραίτητο, για την επιλογή του κατάλληλου παροχέα υπηρεσιών cloud, να εξετάζονται μερικά από τα παρακάτω θέματα ασφαλείας:

- Οι διαδικασίες ασφάλειας του παρόχου υπηρεσιών cloud θα πρέπει να είναι το ίδιο καλές ή καλύτερες από τις διαδικασίες που χρησιμοποιεί η επιχείρηση. Ο έλεγχος των διαδικασιών του πάροχου, θα πρέπει να γίνεται περιοδικά, συμπεριλαμβανομένων ενδεχομένως των επιδιορθώσεων και των ενημερώσεων ασφάλειας (updates) για τα μεμονωμένα συστατικά που χρησιμοποιούνται.
- Ο πάροχος θα πρέπει να εξασφαλίζεται την απομόνωση των υποδομών και των δεδομένων από τους υπόλοιπους χρήστες. Η απαίτηση αυτή είναι περίπλοκη, διότι είναι στενά συνυφασμένη με το επιχειρηματικό μοντέλο που χρησιμοποιείται

από τον πάροχο. Για παράδειγμα, ένας πάροχος IaaS [μπορεί να παρέχει πολλαπλές ενοικιάσεις με εικονικές μηχανές που τρέχουν στην ίδια φυσική μηχανή. Ανάλογα με το είδος της εργασίας που ζητείται να εκτελεστεί στο cloud, αυτή η ρύθμιση μπορεί ή δεν μπορεί να γίνει αποδεκτή από έναν χρήστη cloud. Σε τέτοιες περιπτώσεις, ο πάροχος υπηρεσιών cloud θα πρέπει να έχει τη δυνατότητα να παρέχει χωριστούς φυσικούς servers για συγκεκριμένους πελάτες.

- Οι λειτουργίες ασφαλείας μπορεί να τρέξουν ως εικονικές συσκευές από τους host σε περιβάλλον cloud. Έτσι, είναι δυνατό για τους χρήστες cloud σε ένα περιβάλλον IaaS να φορτώσουν και να διαμορφώσουν το δικό τους τείχος προστασίας ή άλλης ασφαλούς εικονική συσκευή για να τρέξει μέσα στο cloud. Οι εικόνες λογισμικού που χρησιμοποιούνται για αυτές τις εικονικές συσκευές πρέπει να διαχειρίζονται και να επιδιορθώνουν όπως, με τον τρόπο που το λειτουργικό σύστημα, host, και άλλες εφαρμογές λειτουργούν.

- Καταγραφή και ιστορικό ελέγχων για τις αιτήσεις που είναι σημαντικές για τις επιχειρήσεις να κατανοήσουν τόσο την απόδοση των εφαρμογών καθώς και τα κενά ασφαλείας. Cloud πάροχοι υπηρεσιών θα πρέπει να επιτρέψουν την πρόσβαση στην παρακολούθηση της εφαρμογής και των χαρακτηριστικών εργαλείων τους, ανάλογα με την περίπτωση.

- Οι μηχανισμοί ελέγχου ταυτότητας («Είστε αυτός που λες ότι είσαι») και στα δύο άκρα των επιπέδων παροχής σύνδεσης - στο χρήστη σύννεφο και των υπηρεσιών cloud. Ο χρήστης και ο διαχειριστής πρέπει να συμφωνήσουν σε προγράμματα όπως ο έλεγχος ταυτότητας με τα ψηφιακά πιστοποιητικά και αρχές έκδοσης πιστοποιητικών.

- Επειδή, οι υπηρεσίες cloud είναι εκτεθειμένες στον έξω κόσμο, οι πόροι του cloud θα πρέπει να υποστηρίζουν λειτουργίες ασφάλειας, όπως η ανίχνευση εισβολής

και πρόληψης, firewal για την πρόληψη της μη επιτρεπόμενης κυκλοφορίας, καθώς και Denial of Service (DoS) πρόληψη. Οι υπηρεσίες cloud είναι ευάλωτες σε Distributed Denial of Service (DDoS), που μπορεί να πνίξει αποτελεσματικά τις γραμμές πρόσβασής του, με αποτέλεσμα οι χρήστες να μην έχουν πρόσβαση στις υπηρεσίες Cloud. Η πρόληψη DDoS που βασίζεται στο διαδίκτυο είναι μια πιθανή λύση, με μία από τις τεχνικές που περιλαμβάνουν τη διανομή των πόρων cloud σε συγκεκριμένες γεωγραφικές περιοχές και τη δυνατότητα να ανακατευθύνει τους χρήστες σύννεφο σε περίπτωση DDoS συμφόρησης. [6]

Επιθέσεις

Η ασφάλεια στο cloud networking μπορεί να χαρακτηριστεί ως ένας πολύ σημαντικός παράγοντας ποιότητας των υπηρεσιών. Χωρίς μέτρα και ελέγχους ασφαλείας, τα δεδομένα είναι εκτίθενται σε μια πιθανή επίθεση. Μερικές επιθέσεις μπορεί να χαρακτηριστούν ως παθητικές, που σημαίνει ότι οι πληροφορίες απλώς παρακολουθούνται. Ενώ άλλες είναι ενεργές, που σημαίνει ότι οι πληροφορίες μπορεί να μεταβληθούν με μια προσθήκη, να αλλοιωθούν ή να καταστραφούν δεδομένα ακόμα και στο ίδιο το διαδίκτυο. Το διαδίκτυο και τα δεδομένα είναι ευάλωτα σε οποιαδήποτε από τους παρακάτω τύπους επιθέσεων, εάν δεν εξασφαλίζεται η ασφάλειά τους. Ορισμένες κατηγορίες επιθέσεων είναι και οι ακόλουθες:

- ***Eavesdropping*:** Σε γενικές γραμμές, η πλειοψηφία των επικοινωνιών δικτύου πραγματοποιούνται σε ένα ακάλυπτο ή σε «απλό κείμενο», οι οποίες επιτρέπουν σε έναν εισβολέα που έχει αποκτήσεις πρόσβαση στα δεδομένα, υποκλέπτοντας τις επικοινωνίες τους χρήστη. Αυτό αναφέρεται ως sniffing ή κατασκοπεία. Η ικανότητα ενός ωτακουστή (sniffer) να παρακολουθεί το διαδίκτυο

είναι γενικά το μεγαλύτερο πρόβλημα της ασφάλειας που αντιμετωπίζουν οι διαχειριστές σε μια επιχείρηση. Χωρίς ισχυρές υπηρεσίες κρυπτογράφησης, τα δεδομένα μπορεί να διαβαστούν από τους άλλους, καθώς διασχίζουν το διαδίκτυο.

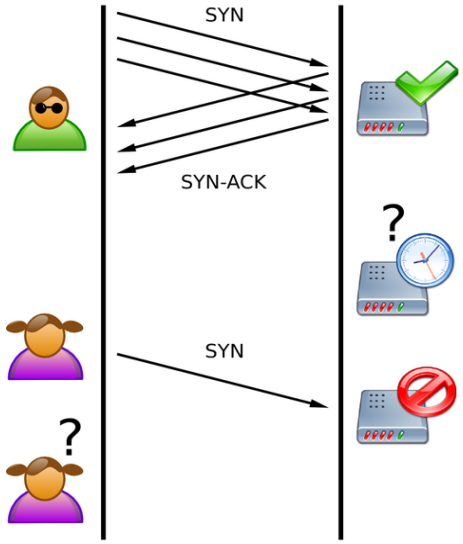
- ***Data Modification*:** Μετά ένας εισβολέας έχει διαβάσει τα δεδομένα ενός χρήστη, το επόμενο που μπορεί να κάνει είναι να τα αλλάξει. Αυτό γίνεται χωρίς τη γνώση του αποστολέα ή του παραλήπτη. Ακόμα κι αν ο χρήστης δεν έχει ζητήσει την εμπιστευτικότητα για όλες τις επικοινωνίες, δεν επιθυμεί την τροποποίηση κάποιου από τα εξερχόμενα μηνύματά του να τροποποιηθεί κατά την μεταφορά.
- ***Identity Spoofing (IP Address Spoofing):*** Τα περισσότερα δίκτυα και λειτουργικά συστήματα χρησιμοποιούν τη διεύθυνση IP ενός υπολογιστή για να εντοπίσουν μια έγκυρη διεύθυνση. Σε ορισμένες περιπτώσεις, είναι δυνατόν ο επιτιθέμενος να προσποιηθεί κάποιον άλλον, έχοντας την ίδια IP διεύθυνση με του πραγματικού κατόχου. Έτσι μπορεί να έχει πρόσβαση στα δεδομένα του, να τα τροποποιήσει, δρομολογήσει ή και να τα διαγράψει. [8], [18]
- ***Password-Based Attacks:*** Ένα κοινό χαρακτηριστικό του σχεδιασμού των περισσότερων λειτουργικών συστημάτων και συστημάτων ασφάλειας του διαδικτύου, αποτελεί ο κωδικός πρόσβασης. Αυτό σημαίνει ότι τα δικαιώματα πρόσβασης σε έναν υπολογιστή και τους πόρους του δικτύου καθορίζεται από το «ποιος είσαι», δηλαδή, το όνομα χρήστη και τον κωδικό πρόσβαση. Παλαιότερες εφαρμογές δεν προστάτευαν πάντα τα στοιχεία ταυτότητας καθώς αυτά διαπερνούσαν το διαδίκτυο για την επικύρωση. Αυτό μπορεί να επιτρέψει σε ένας ωτακουστή να αποκτήσουν πρόσβαση στο δίκτυο θέτοντάς τον έγκυρο χρήστη. [8],[18]

Όταν ένας εισβολέας βρίσκει έναν έγκυρο λογαριασμό χρήστη, αποκτά αυτόματα τα ίδια δικαιώματα με τον πραγματικό χρήστη. Ως εκ τούτου, εάν ο χρήστης διαθέτει δικαιώματα επιπέδου διαχειριστή, ο εισβολέας μπορεί επίσης να δημιουργήσει

λογαριασμούς για την επόμενη πρόσβαση σε μεταγενέστερο χρόνο.

Μετά την απόκτηση πρόσβασης στο δίκτυο του χρήστη, με ένα έγκυρο λογαριασμό, ο εισβολέας μπορεί να κάνει οποιοδήποτε από τα ακόλουθα: να αποκτήσει τους καταλόγους των έγκυρων ονομάτων χρηστών ηλεκτρονικών υπολογιστών και πληροφορίες δικτύου, να τροποποιήσει τον server και δικτύου, συμπεριλαμβανομένων των ελέγχων πρόσβασης και των πινάκων δρομολόγησης. Να τροποποιήσει, να αναδρομολογήσει, ή να διαγράψει τα δεδομένα του χρήστη.[8],[18]

- ***Denial-of-Service Attack (DoS):*** είναι μια από τις επιθέσεις η οποία εμποδίζει ολοκληρωτικά την παροχή υπηρεσιών από το cloud στους χρήστες του. Μετά την απόκτηση πρόσβασης στο δίκτυο του χρήστη, ο εισβολέας γεμίζει με υπερβολικό αριθμό αιτήσεων για εξυπηρέτηση τον server υπερφορτώνοντας το δικτύου με κίνηση μέχρι να διακοπεί η λειτουργία του. Ένα είδος επίθεσης DoS είναι



Πηγή:
http://upload.wikimedia.org/wikipedia/co

η επίθεση SYN flood κατά την οποία ο εισβολέας στέλνει πολλά πακέτα TCP SYN προς στον θύμα για να πραγματοποιήσει σύνδεση, εκμεταλλευόμενος το TCP 3-way handshake. [7]. Για να πετύχει η επίθεση, βασική προϋπόθεση είναι ο διακομιστής να δεσμεύσει πόρους του συστήματος αμέσως μόλις δεχτεί το πρώτο ACK πακέτο και

όχι μετά το πέρας της χειραψίας. Ο διακομιστής θεωρεί ότι τα πακέτα αυτά προέρχονται από τον κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει. Επειδή για κάθε ημιτελή σύνδεση TCP ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όριά του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρήστες. Αυτή η κατάσταση ονομάζεται άρνηση υπηρεσιών (DOS - Denial of Service). Αυτή η επίθεση μπορεί να προληφθεί με την έγκριση αυστηρής πρόσβασης στο cloud και τη χρησιμοποίηση πρωτόκολλων κρυπτογράφησης έτσι ώστε αν εξασφαλίζεται η ασφαλής πρόσβαση από τον κατάλληλο χρήστη.[8], [18]

Μια ακόμα αποτελεσματική μέθοδος αντιμετώπισης αυτής της επίθεσης είναι η καταγραφή του αριθμού των συνδέσεων που έχει ξεκινήσει κάθε χρήστης και η απαγόρευση δημιουργίας νέων συνδέσεων όταν ο αριθμός αυτός ξεπεράσει κάποιο προκαθορισμένο όριο.[8], [18]

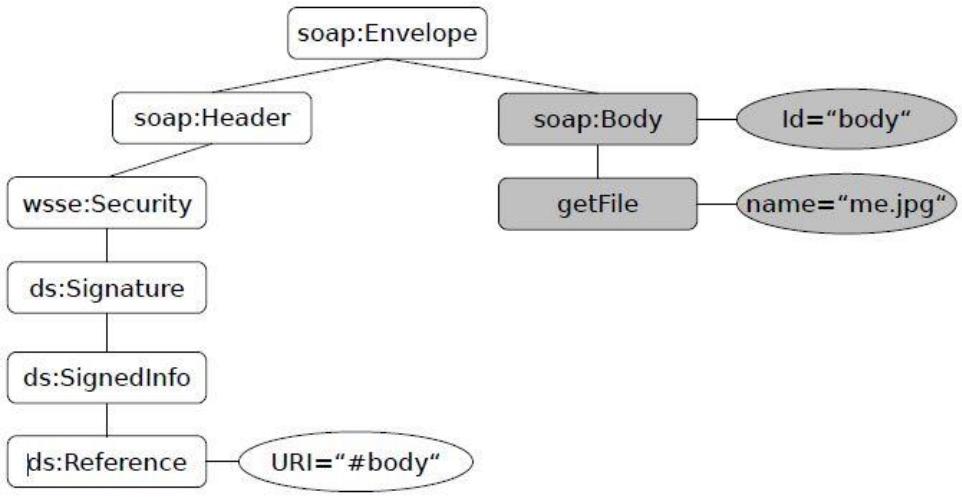
- ***Man-in-the-Middle επίθεση:*** Όπως αναφέρει το όνομα, εμφανίζεται μια επίθεση man-in-the-middle όταν κάποιος ανάμεσα στον χρήστη και το άτομο με το οποίο επικοινωνεί, παρακολουθείται ενεργά από τον εισβολέα, ο οποίος καταγράφει και ελέγχει της επικοινωνία του χρήστη [10] . Όταν δηλαδή το SSL (secure socket layer) δεν λειτουργεί σωστά. Για παράδειγμα όταν δυο χρήστες επικοινωνούν μεταξύ τους και το SSL δεν είναι σωστά εγκατεστημένο, τότε όλη η μεταξύ τους επικοινωνία μπορεί να υποκλαπεί από έναν ενδιάμεσο χρήστη. Για την αντιμετώπιση αυτής της επίθεσης θα πρέπει να εγκατασταθεί σωστά το SSL και να ελεγχθεί πριν την επικοινωνία μεταξύ εξουσιοδοτημένων χρηστών. [8] [10]

- ***XML signature element:*** Η XML υπογραφή στοιχείου, περιγράφει τον

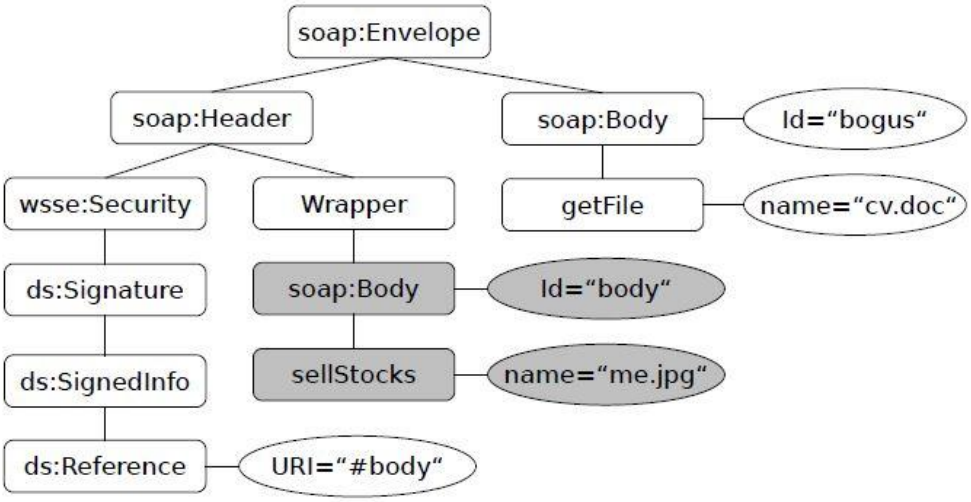
τρόπο δημιουργίας και αναπαράστασης των κρυπτογραφημένων δεδομένων XML, καθώς και του τρόπου αποκρυπτογράφησης ενώ παράλληλα μπορεί να υποστηρίξει την κρυπτογράφηση ενός ολόκληρου κειμένου XML ή μόνο επιλεγμένων κομματιών του [11]. Επειδή οι χρήστες είναι συνήθως σε θέση να συνδεθεί με το cloud computing μέσω ενός web browser ή μιας υπηρεσίας web, οι επιθέσεις των υπηρεσιών web επηρεάζουν επίσης το cloud computing. Η XML signature element wrapping είναι μια γνωστή επίθεση των υπηρεσιών web η οποία περιλαμβάνει κακόβουλο λογισμικό. Παρόλο που η ασφάλεια Cloud χρησιμοποιεί την XML υπογραφή, προκειμένου να προστατεύσει το όνομα, τα χαρακτηριστικά και την αξία ενός στοιχείου από μη εξουσιοδοτημένα πρόσωπα, δεν είναι σε θέση να προστατεύσει τα στοιχεία του εγγράφου. Ένας εισβολέας είναι σε θέση να χειριστεί ένα μήνυμα SOAP (Simple Object Access Protocol) αντιγράφοντας το στοιχείο στόχου και εισάγοντας οτιδήποτε θεωρεί ότι χρειάζεται και το αρχικό στοιχείο οπουδήποτε αλλού στο μήνυμα SOAP (το SOAP είναι ένα πρωτόκολλο βασισμένο στην XML το οποίο επιτρέπει στις εφαρμογές να ανταλλάσουν πληροφορία πάνω από κοινώς χρησιμοποιούμενα πρωτόκολλα του διαδικτύου [12]. Αυτή η τεχνική μπορεί να εξαπατήσει την υπηρεσία δικτύου για να επεξεργαστεί το κακόβουλο μήνυμα που δημιουργείται από την επίθεση. Τα παρακάτω σχήματα απεικονίζουν ένα παράδειγμα επίθεσης XML signature element wrapping. [8][13][18]

Σύμφωνα με το *σχήμα 1*, ο χρήστης ζητά μια εικόνα που ονομάζεται "me.jpg". Ωστόσο, εάν ο εισβολέας παρακολουθεί και αλλοιώνει το μήνυμα SOAP εισάγοντας το ίδιο στοιχείο με τον χρήστη, αλλά υποθέτουμε ότι ζητά ένα αρχείο με το όνομα "CV.doc". Τότε αντί της εικόνας εμφανίζεται το *σχήμα 2*. Αφού η υπηρεσία δικτύου λάβει το μήνυμα, θα στείλει στον χρήστη το αρχείο με το όνομα "CV.doc". Το 2008, η υπηρεσία EC2 της Amazon, το δημόσιο σύστημα το cloud computing της Amazon,

ανακάλυψε ότι ήταν ευάλωτη στις επιθέσεις κρυπτογράφησης στοιχείων XML. Η πιθανή αντιμετώπιση του προβλήματος είναι να χρησιμοποιείται ένας συνδυασμός WSSecurity με κρυπτογράφηση XML για την υπογραφή συγκεκριμένων στοιχείων και ψηφιακή πιστοποιημένη αυτών όπως το X.509 [14] που εκδίδονται από αξιόπιστες αρχές έκδοσης πιστοποιητικών [15]). Επιπλέον, ο διακομιστής του web server θα πρέπει να δημιουργήσει μια λίστα των στοιχείων που χρησιμοποιούνται στο σύστημα και να απορρίψει κάθε μήνυμα που περιέχει μη αναμενόμενα μηνύματα από τους χρήστες.[8][18]



Σχήμα 1. SOAP μήνυμα πριν την επίθεση



Σχήμα 2. SOAP μήνυμα μετά την επίθεση

(πηγή: http://www.narensportal.com/papers/exploitation-vulnerabilities-cloud-storage.aspx) [8][18]

- *Cloud malware injection attack:* Cloud malware ένεση είναι η επίθεση που επιχειρεί να προδώσει μια κακόβουλη υπηρεσία, εφαρμογή ή ακόμη και εικονική μηχανή στο σύστημα ανάλογα με το μοντέλο cloud υπηρεσίας (SaaS, PaaS ή IaaS). Στην επίθεση αυτή, ο εισβολέας πρέπει να δημιουργήσει τη δική του κακόβουλη εφαρμογή, υπηρεσία ή εικονική μηχανή και θα πρέπει να την προσθέσει στο σύστημα cloud. Εφόσον έχει προστεθεί το κακόβουλο λογισμικό, ο εισβολέας πρέπει να ξεγελάσει το cloud system έτσι ώστε αυτό να το αναγνωρίσει ως έγκυρη εφαρμογή. Αν εγκατασταθεί με επιτυχία, οι κανονικοί χρήστες είναι σε θέση να ζητήσουν την υπηρεσία του κακόβουλου λογισμικού, και στη συνέχεια αυτή να εκτελεστεί. Μια άλλη περίπτωση επίθεσης μπορεί να είναι μια προσπάθεια να φορτωθεί ένας ιός ή ένα πρόγραμμα trojan στο cloud system. Μόλις το αναγνωρίσει ως έγκυρη εφαρμογή ή υπηρεσία, το πρόγραμμα του ιού εκτελείται αυτόματα και το cloud system μολύνετε με τον ιό και μπορεί να του προκαλέσει βλάβη. Σε αυτή την περίπτωση ο ιός μπορεί να καταστρέψει τους πόρους του cloud system και να επηρεάσει άλλα συστήματα που

μοιράζονται τους ίδιους πόρους. Επιπλέον, ο εισβολέας μπορεί να στοχεύει στη χρήση ενός προγράμματος προστασίας από ιούς για να επιτεθεί σε άλλους χρήστες του cloud. Μόλις ένας χρήστης ζητά το κακόβουλο πρόγραμμα για παράδειγμα, το cloud system στέλνει τον ιό στο διαδίκτυο για τον χρήστη, και στη συνέχεια αυτό εκτελείτε στον υπολογιστή του χρήστη, μολύνοντάς τον. [8] [16]

Συμπεράσματα

Στην εργασία αυτή γίνεται μια παρουσίαση για το τι είναι το Cloud. Αναφέρεται το θέμα της ασφάλειας των δεδομένων που διαχειρίζονται οι πάροχοι των υπηρεσιών Cloud, όπως είναι οι DoS επιθέσεις, οι XML Signature Element Wrapping, οι Cloud Malware Injection επιθέσεις, και παρουσιάζονται ορισμένες λύσεις. Στις επιθέσεις αυτές, ο εισβολέας έχει την δυνατότητα να πλημυρίσει το δίκτυο με μηνύματα, το οποίο έχει ως αποτέλεσμα την άρνηση εξυπηρέτησης του χρήστη. Σε άλλη περίπτωση, μπορεί ο εισβολέας αλλοιώνοντας ένα μήνυμα SOAP να υποκλέψει τα προσωπικά στοιχεία του χρήστη και να μεταβάλει τις πληροφορίες του. Επίσης, μπορεί να εγκαταστήσει ένα κακόβουλο λογισμικό ή ένα πρόγραμμα στο cloud, το οποίο μπορεί να προκαλέσει μεγάλη ζημιά στο Cloud και να υποκλέψει πολλές πληροφορίες και δεδομένα από τον πάροχο. Η ασφάλεια στο Cloud αποτελείτε από τις δυνατότητες ασφάλειας των web browser και τις δομές των web server, ενώ αναπτύσσονται νέα μοντέλα προστασίας των δεδομένων των χρηστών.[10]

Αναφορές

[1] Bing Luo, Liu, W. (2011). The Sustainability and Survivabiltiy Network Design for Next Generation Cloud Networking. *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, Sydney, NSW, 12-14 Ιανουαρίου 2011. Sydney, NSW, 12525984, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6119073&queryText%3Dcloud+networking

[2] France Bélanger and Craig Van Slyke, *Information Systems for Business: an Experiential Approach* (Hoboken, NJ: Wiley, 2012), pageNr. 130

[3] (National Institute of Science and Technology. Retrieved 24 July 2011.)

[4] (http://www.sersc.org/journals/IJAST/vol34/8.pdf)

[5] Mohamed, E. (2012). Data Security Model for Cloud computing. *The Twelfth International Conference on Networks*, Egypt, 14-16 Μαΐου 2012. Egypt, 12864203, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6236556&queryText%3DData+Security+Model+for+Cloud+computing.

[6] Sridhar, T. (2009, 1 Δεκεμβρίου). Cloud Computing - A Primer Part 2: Infrastructure and Implementation Topics. *The Internet Protocol Journal*. volume 12, (issue 4), http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_12-4/ipj_12-4.pdf.

[7] *http://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml*. (1 Σεπτεμβρίου, 2013). Ανακτήθηκε 6 Ιανουαρίου, 2014, από http://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml.

[8] Muralidhara, P. (2013, 1 Οκτωβρίου). Security issues in cloud computing and its countermeasures. *International Journal of Scientific & Engineering Research*. Volume 4, (Issue 10), http://www.ijser.org/.

[9] Jensen, M. ; Horst Gortz Inst.; Schwenk, J. ; Gruschka, N. ; Iacono, L.L. .On Technical Security Issues in Cloud Computing. *2009 IEEE International Conference on Cloud Computing*, Bangalore, 21-25 Σεπτεμβρίου 2009. [χ.τ.], 10908783, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5284165&queryText%3DOn+Technical+Security+Issues+in+Cloud+Computing

[10] Qaisar, S. & Fiaz Khawaja, K. (2012, 1 Ιανουαρίου). Cloud Computing: Network/Security Threats and Countermesures. *Interdesciplinary journal of contemporary resarch in Business*. Vol 3, (9), http://www.journal-archieves14.webs.com/1323-1329.pdf.

[11] [http://gunet2.cs.unipi.gr/eclass/modules/document/file.php/ (Θάνος)].

[12] http://www.it.uom.gr/project/soap/Theory/SOAP.html])

[13] (Muralidhara, 2013)

[14] http://en.wikipedia.org/wiki/X.509

[15] http://en.wikipedia.org/wiki/Certification_authority

[16] http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf

[17] Hassan, S.R.; Bourgeois, J.; Sunderam, V.; Li Xiong, (2012). Detection of Distributed Attacks in Hybrid & Public Cloud Networks. *Semantics, Knowledge and Grids (SKG), 2012 Eighth International Conference on Networks*, Beijing, 22-24 Οκτωβρίου 2012. [χ.τ.], df, http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6389879.

[18] Jamil, D., & Zaki, H. (2011). Security Issues in cloud Computing and countermesures. *International Journal of Engineering Science and Technology (IJEST)*, *3*(4), 2672-2676. Retrieved from http://www.ijest.info/issue.php?file=vol03issue04

Βιβλιογραφία

Hamdi,, M. ([χ.χ.]). Security of cloud computing, storage, and networking. *Collaboration Technologies and Systems (CTS), 2012 International Conference on*, Denver, CO, 21-25 Μαΐου 2012. [χ.τ.], 12911882, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6261019&queryText%3DSecurity+of+cloud+computing%2C+storage%2C+and+networking.

Jouini, M., Mili, A., Aissa, A. B., & Rabai, L. B. A. (2012). OWARDS QUANTITATIVE MEASURES OF INFORMATION SECURITY: A CLOUD COMPUTING CASE STUDY. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *1*(3). Retrieved from http://sdiwc.net/digital-library/towards-quantitative-measures-of-information-security-a-cloud-computing-case-study.html

Biggest Security Concern with Cloud Computing? (2012). Retrieved from http://www.cloudtweaks.com/2012/01/infographic-biggest-security-concern-with-cloud-computing/