Συμμόρφωση πλατφόρμας τηλεδιασκέψεων e:Presence με τις απαιτήσεις του ΦΕΚ (Αρ. φύλλου 433, 17 Μαρτίου 2011, Αρ. Φ.122.1/42/23076/Β2) περί τηλεδιασκέψεων συλλογικών οργάνων Πανεπιστημίων και ΑΤΕΙ

Σύνταξη κειμένου : Γεώργιος Μαμαλάκης, MSc
Επιμέλεια κειμένου : Κωνσταντίνος Βασιλάκης, PhD

Δεκέμβριος 2011

Περιεχόμενα

1. Γενικά

Το παρόν κείμενο διατίθεται για την ερμηνεία του ΦΕΚ (Αρ. φύλλου 433, 17 Μαρτίου 2011, Αρ. Φ.122.1/42/23076/Β2) περί τηλεδιασκέψεων συλλογικών οργάνων Πανεπιστημίων και Α.Τ.Ε.Ι. σε ότι αφορά τις τεχνικές προδιαγραφές που αναφέρονται σε θέματα ασφάλειας υπολογιστικών συστημάτων, καθώς και για το κατά πόσον η πλατφόρμα τηλεδιασκέψεων ePresence είναι σύμφωνη με αυτές.

Στο εν λόγω ΦΕΚ νομιμοποιείται η δυνατότητα συμμετοχής σε συνεδριάσεις συλλογικών οργάνων Πανεπιστημίων και Α.Τ.Ε.Ι. και ιδιαίτερα σε συνεδριάσεις των εκλεκτορικών σωμάτων μέσω τηλεδιάσκεψης, εφόσον πληρούνται κάποιες προϋποθέσεις. Οι προϋποθέσεις που τίθενται στην παράγραφο 2 αναφέρουν επ' ακριβώς: «…με την προϋπόθεση ότι εξασφαλίζεται η ***μυστικότητα*** και ***εμπιστευτικότητα των συνεδριάσεων***, η ***πιστοποίηση ταυτότητας των μελών***, η ***ασφάλεια της ηλεκτρονικής διακίνησης φωνής***, ***δεδομένων και εικόνας*** και ***η ακεραιότητα της πληροφορίας***.».

2. Στοιχεία θεωρίας ασφάλειας υπολογιστικών συστημάτων

2.1 Αγαθά (assets)

Οι έννοιες που χρησιμοποιούνται στο κείμενο και προέρχονται από το χώρο της ασφάλειας δεδομένων και πληροφοριακών συστημάτων είναι: η *μυστικότητα*, η *εμπιστευτικότητα*, η *πιστοποίηση ταυτότητας* και η *ακεραιότητα*. Θα αναφέρουμε τους ορισμούς αρχικά και έπειτα θα τους αναλύσουμε σε σχέση με το κείμενο και τα συμφραζόμενά του. Σύμφωνα με το [1]:

- ***Εμπιστευτικότητα*** (***confidentiality***) είναι η ιδιότητα της Πληροφορίας να είναι προσπελάσιμη μόνο από οντότητες που είναι ***εξουσιοδοτημένες*** (***authorized***) προς τούτο.

- ***Ακεραιότητα*** **(*integrity*)** είναι η ιδιότητα της Πληροφορίας να τροποποιείται μόνο από ***εξουσιοδοτημένες*** προς τούτο οντότητες.

Η έννοια της **εξουσιοδότησης (authorization)** που εμπερικλείεται στους παραπάνω ορισμούς ορίζεται ως η λειτουργία εφαρμογής πολιτικής ελέγχου πρόσβασης (***Access Control***) στην Πληροφορία, εξασφαλίζοντας ότι κάποιος πιστοποιημένος χρήστης θα έχει εκείνο το επίπεδο πρόσβασης στην Πληροφορία όπως αυτή ορίζεται και ελέγχεται από το σύστημα.

Σύμφωνα με τον [1] η **πιστοποίηση ταυτότητας** αποτελείται από δύο στάδια, την ***ταυτοποίηση (identification)*** και την ***αυθεντικοποίηση (authentication)***. Η *ταυτοποίηση* στα σύγχρονα υπολογιστικά συστήματα ταυτίζεται σχεδόν πάντα με το όνομα χρήστη (***username***). Για την *αυθεντικοποίηση*, αναφέρει ο [1] τέσσερις μεθόδους με την οποία μπορεί να αποδείξει κάποιος την ταυτότητά του: 1) με κάτι που ξέρει, 2) με κάτι που έχει, 3) με κάτι που αποτελεί μοναδικό ατομικό χαρακτηριστικό του ή 4) με το πού βρίσκεται σε σχέση με το πού αναμένεται να βρίσκεται. Ο συνήθης τρόπος εξασφάλισης της αυθεντικοποίησης είναι η χρήση ενός συνθηματικού (***password***) που καλύπτει το 1. Άλλοι συγγραφείς [2] εμπερικλείουν στην έννοια της αυθεντικοποίησης και την ταυτοποίηση και πιο συγκεκριμένα στο [2] αναφέρεται στην υπηρεσία αυθεντικοποίησης ως:

- Η ***υπηρεσία αυθεντικοποίησης*** [4] διασφαλίζει ότι η επικοινωνία είναι *αυθεντική*. Στην περίπτωση επικοινωνίας με ένα μόνο μήνυμα, όπως μία προειδοποίηση, ένας συναγερμός ή ένα σήμα, η υποχρέωση της υπηρεσίας αυθεντικοποίησης είναι να διασφαλίσει στον παραλήπτη του μηνύματος

ότι το μήνυμα προέρχεται όντως από την πηγή που ισχυρίζεται ότι προέρχεται. Στην περίπτωση αλληλεπίδρασης πολλών *μελών*, όπως η σύνδεση με ένα τερματικό σε κάποιο μηχάνημα, δύο έννοιες εμπλέκονται. Πρώτον, τη στιγμή της εκκίνησης της σύνδεσης, η υπηρεσία διασφαλίζει ότι και οι δύο οντότητες είναι αυθεντικές, ήτοι ότι κάθε οντότητα είναι πράγματι αυτή που ισχυρίζεται ότι είναι. Δεύτερον, η υπηρεσία διασφαλίζει ότι δεν μπορεί να παρεμβληθεί με τρόπο τέτοιο η επικοινωνία, ώστε ένα τρίτο μέλος να μασκαρευτεί ως κάποιο από τα δύο άλλα νόμιμα μέλη με σκοπό τη μη εξουσιοδοτημένη λήψη ή αποστολή μηνυμάτων.

Η έννοια της ***μυστικότητας*** δεν ορίζεται συγκεκριμένα για την ασφάλεια υπολογιστικών συστημάτων, αλλά νοείται ως η διαδικασία διατήρησης κάποιου αγαθού (*asset*) ως κρυφό. Συνεπώς καλύπτεται πλήρως από την απαίτηση για εμπιστευτικότητα.

Τέλος, υπάρχει στο κείμενο και το σημείο που αναφέρεται στην «…*ασφάλεια της ηλεκτρονικής διακίνησης φωνής*, *δεδομένων και εικόνας…*», όπου η έννοια της ασφάλειας χρησιμοποιείται με τη γενικότερη έννοιά της, δηλαδή εμπεριέχει τη συνύπαρξη των αγαθών *εμπιστευτικότητα*, *ακεραιότητα* και *διαθεσιμότητα* κατά τη διαδικασία ανταλλαγής πληροφορίας. Η ***διαθεσιμότητα*** ενός συστήματος ή ενός πόρου κάποιου συστήματος ορίζεται [2] ως η ιδιότητα του να είναι διαθέσιμο σε εξουσιοδοτημένες οντότητες κατόπιν αίτησής και εφ’ όσον το ορίζουν οι προδιαγραφές του συστήματος. Κατ’ επέκταση η ***υπηρεσία διαθεσιμότητας*** είναι η υπηρεσία που προστατεύει ένα σύστημα με σκοπό τη διασφάλιση της διαθεσιμότητάς του. Μία τέτοια υπηρεσία διευθετεί τις ανησυχίες που προκύπτουν από ενδεχόμενες ***επιθέσεις άρνησης εξυπηρέτησης,*** που αναφέρουμε σε επόμενη παράγραφο.

Η έννοια της *ασφάλειας* στο σημείο αυτό του εγγράφου, υπερκαλύπτεται από τις υπόλοιπες έννοιες που αναφέρονται στην ίδια παράγραφο αν εντάξουμε σε αυτές και την έννοια της διαθεσιμότητας.

Για να μπορεί, λοιπόν, μία εφαρμογή τηλεδιασκέψεων να πληροί τις απαραίτητες προϋποθέσεις, θα πρέπει να διασφαλίζει την εμπιστευτικότητα των συνεδριάσεων, την ακεραιότητα της ανταλλασσόμενης πληροφορίας την αυθεντικοποίηση των χρηστών και τη διαθεσιμότητα της συνολικής υπηρεσίας. Σκοπός ύπαρξης των εννοιών αυτών είναι η προστασία του συστήματος από ενδεχόμενες δικτυακές επιθέσεις.

2.2 Είδη επιθέσεων

Οι επιθέσεις στην ασφάλεια των υπολογιστικών συστημάτων και δικτύων μπορούν να διαχωριστούν σε δύο γενικές κατηγορίες, στις ***παθητικές*** και στις ***ενεργητικές*** [2]. Σύμφωνα με το [2] οι *παθητικές επιθέσεις* αποσκοπούν στη μη εξουσιοδοτημένη απόκτηση μεταδιδόμενης πληροφορίας και χωρίζονται σε δύο υποκατηγορίες, την *εμφάνιση περιεχομένου του μηνύματος* και στην *ανάλυση κίνησης*. Στην πρώτη υποκατηγορία κατατάσσονται επιθέσεις όπως οι τηλεφωνικές υποκλοπές και η μη εξουσιοδοτημένη ανάγνωση μηνυμάτων ταχυδρομείου, κλπ. Οι επιθέσεις *ανάλυσης κίνησης* είναι πιο περίπλοκες και ευρείς. Θα μπορούσε, λ.χ., ένας κακόβουλος χρήστης να παρατηρεί κωδικοποιημένη κίνηση που ανταλλάσσεται μεταξύ δύο δικτυακών πόρων και να αρκείται μόνο στη στατιστική της ανταλλασσόμενης πληροφορίας για να εξάγει τα συμπεράσματά του. Ο πλέον δημοφιλής τρόπος αποφυγής τέτοιου είδους επιθέσεων είναι η χρήση κρυπτογραφίας [2].

Οι *ενεργητικές επιθέσεις* μπορούν να αναλυθούν σε τέσσερεις μεγάλες υποκατηγορίες εκ των οποίων σε όλες υπάρχει ενεργή δράση του επιτιθέμενου είτε μέσω της μεταβολής του ανταλλασσόμενου μηνύματος είτε με τη δημιουργία ψεύτικων μηνυμάτων. Οι κατηγορίες αυτές είναι [2] το *μασκάρεμα* (***masquerading***), η *αναμετάδοση* (***replay***), η *μεταβολή μηνυμάτων* (***modification of messages***) και η *άρνηση εξυπηρέτησης*

(***denial of service***). Η επίθεση μασκαρέματος μπορεί να αποφευχθεί με την ύπαρξη μεθόδων αυθεντικοποίησης χρηστών και την παράλληλη κρυπτογράφηση των ανταλλασσόμενων μηνυμάτων. Η επίθεση αναμετάδοσης μπορεί να αποφευχθεί αν ο κρυπτογραφικός αλγόριθμος χρησιμοποιεί κάποιου είδους πληροφορία (***nonce***) που να υποδηλώνει το πόσο «φρέσκο» είναι το μήνυμα. Τέτοια πληροφορία μπορεί να είναι ένας τυχαίος αριθμός που συνοδεύει το πρώτο μήνυμα και ο οποίος αυξάνεται κατά κάποιο βήμα σε κάθε επόμενη ανταλλαγή μηνύματος της ίδιας συνεδρίας (***session***) ή κάποια πληροφορία που αφορά την ώρα που ξεκίνησε η επικοινωνία (***timestamp)***. Τέτοιες μέθοδοι εφαρμόζονται από όλους τους γνωστούς αλγορίθμους κρυπτογράφησης που χρησιμοποιούνται ευρέως, όπως λ.χ. το ***SSL***. Η επίθεση μεταβολής μηνυμάτων σε συστήματα τηλεδιασκέψεων μπορεί πάλι να αποφευχθεί με την κρυπτογράφηση του μεταδιδόμενου καναλιού, μιας και όλες οι συχνά χρησιμοποιούμενες σουίτες κρυπτογράφησης διαθέτουν μεθόδους αναγνώρισης σφάλματος κατά τη μετάδοση που αποτρέπουν τέτοιες επιθέσεις. Τέλος, οι *επιθέσεις άρνησης εξυπηρέτησης* είναι πολύ δύσκολο να αποφευχθούν και συνήθως είναι πέραν των δυνατοτήτων του συστήματος που δέχεται την επίθεση το να τις αποτρέψει. Στην πραγματικότητα μόνο οι πάροχοι υπηρεσιών Internet που μεσολαβούν μεταξύ του θύματος και των επιτιθέμενων συστημάτων μπορούν να ενεργήσουν σε τέτοιες περιπτώσεις μέσω των τειχών προστασίας τους ή την ύπαρξη ανεξάντλητων πόρων από πλευράς συστήματος. Αυτό δε σημαίνει ότι δεν μπορεί να διασφαλιστεί ως ένα βαθμό η διαθεσιμότητα και από το ίδιο το σύστημα μέσω χρήσης εφεδρικών μηχανημάτων ή/και δρομολογητών.

Ο αναγνώστης που επιθυμεί να εντρυφήσει περισσότερο στις έννοιες που αναφέρονται σε αυτό το έγγραφο, παραπέμπεται στη βιβλιογραφία. Επίσης, μία εκτενής συγκεντρωτική λίστα ορισμών που αφορούν την ασφάλεια επικοινωνιών και τους οποίους χρησιμοποιούμε σε αυτό το κείμενο, παρέχεται από την ITU-T στο [4].

3. Προϋποθέσεις, όπως προκύπτουν, για επίτευξη συμμόρφωσης με το ΦΕΚ (Αρ. φύλλου 433, 17 Μαρτίου 2011, Αρ. Φ.122.1/42/23076/Β2)

Με βάση την παραπάνω ανάλυση, για να μπορέσει μια εφαρμογή τηλεδιασκέψεων να πληροί τις προϋποθέσεις ασφάλειας που αναφέρονται στο ΦΕΚ, θα πρέπει να διαθέτει μηχανισμό αυθεντικοποίησης των συμμετεχόντων ενώ παράλληλα να υποστηρίζει κρυπτογράφηση των ανταλλασσόμενων μηνυμάτων ώστε να διασφαλίζει αφενός την πιστοποίηση ταυτότητας των μελών και αφετέρου να αποτρέπει επιθέσεις μασκαρέματος κατά την είσοδο στην τηλεδιάσκεψη.

Επιπλέον, θα πρέπει να υποστηρίζει έλεγχο πρόσβασης στην υπηρεσία και ταυτόχρονα την κρυπτογραφημένη ανταλλαγή πληροφορίας των εμπλεκόμενων μελών σε όλα τα στάδια που προηγούνται μέχρι την τηλεδιάσκεψη αλλά και καθ' όλη τη διάρκεια της τηλεδιάσκεψης. Με αυτόν τον τρόπο διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα της ανταλλασσόμενης πληροφορίας (προστασία τόσο από παθητικές επιθέσεις, όσο και από απόπειρες μεταβολής μηνύματος, αναμετάδοσης και μασκαρέματος κατά τη διάρκεια της τηλεδιάσκεψης).

Τέλος, σε ό,τι αφορά τη διαθεσιμότητα της υπηρεσίας, η υιοθέτηση μηχανισμών εφεδρείας μπορεί να φανεί ιδιαίτερα χρήσιμη σε συνήθεις επιθέσεις άρνησης εξυπηρέτησης.

4. *ePresence και ΦΕΚ (Αρ. φύλλου 433, 17 Μαρτίου 2011, Αρ. Φ.122.1/42/23076/Β2)*

Η εφαρμογή ePresence χρησιμοποιεί τη μέθοδο αυθεντικοποίησης που παρέχεται από την πλατφόρμα single-sign-on (***SSO***) ***shibboleth 2*** *[3]* η οποία εγγυάται την ασφαλή πιστοποίηση χρηστών σε επίπεδο ομοσπονδίας, κατά την οποία η πληροφορία ανταλλάσσεται πάνω από κρυπτογραφημένο κανάλι *δημοσίου κλειδιού* (***PKI***) με κλειδί *SSL* μεγέθους 2048 bit. Προκειμένου να συνδεθεί ένας χρήστης σε μία τηλεδιάσκεψη στο ePresence, πρέπει να περάσει από μία διαδικασία δύο βημάτων: α) πρέπει να ακολουθήσει το σύνδεσμο που του παρέχεται μέσα στο email-πρόσκληση που λαμβάνει από το συντονιστή τηλεδιασκέψεων, και β) προτού συνδεθεί στην τηλεδιάσκεψη πρέπει να πιστοποιηθεί από το μηχανισμό shibboleth 2 δίνοντας το όνομα χρήστη και το συνθηματικό που διατηρεί στο ίδρυμα στο οποίο ανήκει. Επιπλέον, ο σύνδεσμος που ακολουθεί ο χρήστης για να συνδεθεί στην τηλεδιάσκεψη περιέχει μία μοναδική ακολουθία αλφαριθμητικών χαρακτήρων που χαρακτηρίζει ένα συγκεκριμένο χρήστη για μία συγκεκριμένη τηλεδιάσκεψη. Η εφαρμογή ePresence συνδυάζει τη μοναδική αυτή πληροφορία με τα στοιχεία που της επιστρέφονται από τον ***Identity Provider*** (***IdP***) μέσω του μηχανισμού shibboleth2 ώστε να προωθήσει το χρήστη στην σωστή τηλεδιάσκεψη. Με την παραπάνω μέθοδο, η πλατφόρμα ePresence επιτυγχάνει τον έλεγχο πρόσβασης.

Επιπλέον, η είσοδος συντονιστών στην εφαρμογή διαχείρισης τηλεδιασκέψεων πραγματοποιείται με χρήση *ονόματος χρήστη* και *συνθηματικού* (***username***, ***password***) πάνω από κρυπτογραφημένο κανάλι (https) το οποίο χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού μεγέθους 2048 bit επίσης. Τα στοιχεία των χρηστών είναι αποθηκευμένα στη βάση δεδομένων του συστήματος και τα συνθηματικά τους είναι αποθηκευμένα με μορφή ***SHA1 digest*** και επιπλέον χρήση ***salt*** για ελαχιστοποίηση της δυνατότητας αποκρυπτογράφησης των κωδικών μέσα από ***rainbow tables***. Ως εκ τούτου, υπερκαλύπτεται η προϋπόθεση ύπαρξης μηχανισμού αυθεντικοποίησης πάνω από κρυπτογραφημένο κανάλι. Επιπλέον, στην εφαρμογή τηλεδιασκέψεων τα κανάλια σημάτων είναι κρυπτογραφημένα με ***TLS*** και όλες οι οπτικοακουστικές ροές (audio/video streams) διασφαλίζονται μέσω της χρήσης του πρωτοκόλλου ***SRTP*** ενώ η πληροφορία είναι κρυπτογραφημένη με χρήση συμμετρικού κλειδιού ***AES 128*** καθ' όλη τη διάρκεια των κλήσεων. Με αυτόν τον τρόπο υπερκαλύπτεται και η απαίτηση που αφορά την κρυπτογραφημένη ανταλλαγή πληροφορίας κατά τη διάρκεια της τηλεδιάσκεψης. Επιπλέον, για ελαχιστοποίηση των κινδύνων που προκύπτουν από επιθέσεις άρνησης εξυπηρέτησης η πλατφόρμα τηλεδιασκέψεων ePresence χρησιμοποιεί μηχανισμούς εφεδρείας τόσο σε επίπεδο υλικού (σε εξυπηρετητές και δρομολογητές δικτύου) όσο και σε επίπεδο λογισμικού (εναλλακτικές δρομολογήσεις, δυναμική επιλογή χρήσης εφεδρικού εξοπλισμού). Τέλος, συμπληρωματικά στα πλαίσια πληρότητας της αντιμετώπισης των ζητημάτων που σχετίζονται με την ασφάλεια της υπηρεσίας, πραγματοποιήθηκε αξιολόγηση ασφάλειας λογισμικού (***software security assessment***) σε επίπεδο ανάλυσης κώδικα (***code auditing***) και σε επίπεδο ελέγχου παρείσδυσης (***penetration testing***) στα επιμέρους υποσυστήματα της πλατφόρμας ePresence και ελήφθησαν οι προβλεπόμενες ενέργειες.

Ως εκ τούτου, η πλατφόρμα τηλεδιασκέψεων ePresence πληροί και τις τρεις προϋποθέσεις ασφάλειας όπως προκύπτουν από την ερμηνεία του ΦΕΚ (Αρ. φύλλου 433, 17 Μαρτίου 2011, Αρ. Φ.122.1/42/23076/Β2) περί τηλεδιασκέψεων συλλογικών οργάνων και άρα μπορεί να χρησιμοποιηθεί με ασφάλεια ως πλατφόρμα τηλεδιασκέψεων για συλλογικά όργανα Πανεπιστημίων και Α.Τ.Ε.Ι.

5. Αναφορές

[1] Σ. Κάτσικας, “Προστασία και Ασφάλεια Συστημάτων Υπολογιστών”, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2000.

[2] W. Stallings, “Cryptography and Network Security, Principles and Practices” fourth edition, Prentice Hall, 2005.

[3] ITU-T, “X.800, *Security Architecture for OSI*”.

[4] ITU-T, “Compendium of approved ITU-T Security Definitions (edition 2003 February)”, http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-E&type=items