Αυθεντικοποίηση για το Ασύρματο δίκτυο του Τμήματος Πληροφορικής

Σκοπός του έργου

Η παροχή υπηρεσιών ασύρματου δικτύου μόνο σε μέλη του Τμήματος, Ακαδημαϊκό, διοικητικό, ερευνητικό προσωπικό, φοιτητές και συνεργάτες που έχουν ήδη πρόσβαση στα υπόλοιπα συστήματα του Τμήματος. Επίσης θα δίνετε ελεγχόμενη προσωρινή πρόσβαση σε επισκέπτες καθηγητές/συνεργάτες του Τμήματος.

Μέθοδοι Αυθεντικοποίησης

Υπάρχουν γύρω στις 40 μεθόδοι για πρόσβαση σε ασύρματα δίκτυα. Λόγω το ότι θα θέλαμε να επιτρέπουμε τη πρόσβαση μόνο σε άτομα που έχουν ήδη πρόσβαση στα υπόλοιπα συστήματα του Τμήματος έπρεπε να διαλέξουμε μια μέθοδο αυθεντικοποίησης που να χρησιμοποιεί username/password αφού είναι και ο τρόπος πρόσβασης στα υπόλοιπα συστήματα.

Οι πιο κοινές μέθοδοι που χρησιμοποιούν τον πιο πάνω τρόπο είναι οι: EAP-TLS, EAP-TTLS. Η πρώτη μέθοδος απορρίφθηκε διότι κατά την αυθεντικοποίηση το password αποστέλλεται χωρίς κρυπτογράφηση και είναι εύκολο να υποκλαπεί. Η μέθοδος EAP-TTLS διοχετεύει την επικοινωνία μέσω ενός κρυπτογραφημένου καναλιού, αλλά σε περιβάλλον windows δεν περιλαμβάνεται στο λειτουργικό και χρειάζεται η εγκατάσταση επιπλέον λογισμικού. Η μέθοδος όπως και η EAP-TTLS διοχετεύει την επικοινωνία μέσω ενός αυθεντικοποιημένου και κρυπτογραφημένου καναλιού, και είναι ενσωματωμένη στα πλείστα λειτουργικά. Για τους πιο πάνω λόγους επέλεξα να χρησιμοποιήσω **EAP-PEAP**

Ο τρόπος που λειτουργούν οι δύο προαναφερθείσες μεθόδοι είναι παρόμοιος αφού και οι δύο χρησιμοποιούν ένα server-side PKI certificate to create για να ανοίξουν ένα secure TLS tunnel για την μετάδοση των συνθηματικών του χρήστη (user authentication), ενώ χρησιμοποιούν ένα server-side public key certificate για την αυθεντικοποίηση του server.

Υλοποίηση αυθεντικοποίησης

Για την υλοποίηση της πιο πάνω μεθόδου χρειάζονται τα ακόλουθα:

1. Radius server
2. Self signed certificate για τον Radius server
3. Samba (smbd και nmbd)
4. Server Registration to AD (join)
5. Winbind