# Εφαρμογή ενός ασφαλούς και ευέλικτου συστήματος πιστοποίησης σε ασύρματα δίκτυα

**Βασίλειος Βασιλάκης**
Εκπαιδευτικός ΠΕ86 Πληροφορικής, 3ο Ημερήσιο ΕΠΑΛ Ταύρου
vdvass@gmail.com

## Περίληψη

Οι Τεχνολογίες Πληροφορίας και Επικοινωνιών παίζουν σημαντικό ρόλο στην σύγχρονη εκπαίδευση. Οι φορητές συσκευές χρησιμοποιούνται ολοένα και περισσότερο για το σκοπό αυτό, αποδεσμεύοντας μαθητές και εκπαιδευτικούς από τα στενά όρια της αίθουσας πληροφορικής. Ενισχύοντας αυτή την τάση πολλά σχολεία καλούν τους μαθητές να φέρνουν και να χρησιμοποιούν τις δικές τους συσκευές (Bring Your Own Device). Η αξιοποίηση αυτού του εξοπλισμού προϋποθέτει την σύνδεσή του σε ασύρματο τοπικό δίκτυο και αυτό με τη σειρά του εγείρει ζητήματα ασφάλειας, που οι συνηθισμένες πρακτικές δεν μπορούν να αντιμετωπίσουν. Στην εργασία αυτή προτείνεται μία ασφαλής, ευέλικτη και εύκολα διαχειρίσιμη μέθοδος πιστοποίησης χρηστών σε ασύρματα δίκτυα, με χρήση του προτύπου IEEE 802.1x σε συνδυασμό με διακομιστή RADIUS.

**Λέξεις κλειδιά:** Ασύρματο δίκτυο, ασφάλεια, πιστοποίηση, διακομιστής RADIUS.

## *1. Εισαγωγή*

Η παιδαγωγική αξιοποίηση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) μπορεί να συμβάλλει στην αύξηση της κινητοποίησης και της συμμετοχής των μαθητών, στην διευκόλυνση του διαμοιρασμού πληροφοριών, στην δημιουργία συνεργατικών περιβαλλόντων εργασίας, και στην προαγωγή της αυτοκαθοδηγούμενης μάθησης (Suryani, 2010).

Η πρόσφατη διάδοση των φορητών ψηφιακών συσκευών έχει οδηγήσει σε προσπάθειες ένταξής τους στην εκπαιδευτική διαδικασία, συχνά με καλύτερα αποτελέσματα από αυτά που επιτυγχάνονται με τη χρήση σταθερών υπολογιστών (Sung, Chang, & Liu, 2016), επεκτείνοντας την αξιοποίηση των ΤΠΕ πέρα από την «επικράτεια» του εργαστηρίου πληροφορικής. Δεν είναι λίγες οι σχολικές μονάδες που υιοθετούν πρακτικές «Φέρτε τη δική σας συσκευή» (Bring Your Own Device – BOYD) και προτρέπουν τους μαθητές να προσκομίζουν και να χρησιμοποιούν τις δικές τους συσκευές (laptop, tablet, κινητά τηλέφωνα) κατά τη διάρκεια του μαθήματος (Rae, Dabner, & Mackey, 2017).

Απαραίτητη προϋπόθεση για τα ανωτέρω είναι η δυνατότητα σύνδεσης των συσκευών σε ασύρματο δίκτυο, η σχεδίαση και η υλοποίηση του οποίου μπορεί να αποδειχθεί πρόκληση, δεδομένων των ζητημάτων που πρέπει να ληφθούν υπόψη και

ISBN: 978-960-578-084-5

αφορούν θέματα επιφάνειας κάλυψης, διαθεσιμότητας, ταχύτητας, εύρους ζώνης, παρεχόμενων υπηρεσιών και τελευταίο, αλλά εξίσου σημαντικό, ασφάλειας (Consortium for School Networking, 2015).

Με το τελευταίο αυτό ζήτημα θα ασχοληθεί η παρούσα εργασία, προτείνοντας έναν εναλλακτικό τρόπο εξατομικευμένης πιστοποίησης και σύνδεσης χρηστών σε ασύρματα δίκτυα, χρησιμοποιώντας το πρότυπο 802.1x με χρήση RADIUS Server.

## *2. Ζητήματα ασφάλειας*

Το πλέον σύνηθες σχήμα ασφαλείας για σύνδεση σε ασύρματα δίκτυα πραγματοποιείται με χρήση των πρωτοκόλλων Wi-Fi Protected Access (WPA και WPA2). Σύμφωνα με αυτές τις υλοποιήσεις (Khasawneh, Kajman, Alkhudaidy, & Althubyani, 2014) στα σημεία πρόσβασης (Access points – AP) του ασύρματου δικτύου καταχωρείται ένα μυστικό κλειδί υπό τη μορφή μιας φράσης μεγέθους 8-63 χαρακτήρων. Για να συνδεθεί μία συσκευή στο AP θα πρέπει και σε αυτή να καταχωρηθεί το ίδιο κλειδί. Λόγω της κοινής χρήσης του κλειδιού από AP και συσκευές, αυτό ονομάζεται διαμοιραζόμενο κλειδί (Pre Shared Key, PSK).

Παρά το γεγονός ότι το WPA2-PSK είναι η συνιστώμενη μέθοδος πιστοποίησης ασφάλειας για οικιακά δίκτυα και δίκτυα μικρών επιχειρήσεων, η χρήση του στο σχολικό περιβάλλον εγκυμονεί τους ακόλουθους κινδύνους:

- Η γνωστοποίηση του κλειδιού σε μεγάλο πλήθος χρηστών αυξάνει την πιθανότητα αυτό να διαρρεύσει και να διαδοθεί σε όλη τη μαθητική κοινότητα, προκαλώντας υπερφόρτωση και ενδεχομένως κατάρρευση του δικτύου, ενώ ακόμη και η απευθείας εισαγωγή του κλειδιού στις συσκευές δεν μπορεί να εξασφαλίσει ότι αυτό θα παραμείνει μυστικό, καθώς αφενός υπάρχουν λογισμικά που μπορούν να το «ανασύρουν» από την συσκευή, αφετέρου οι σύγχρονες φορητές συσκευές παρέχουν εγγενώς τη δυνατότητα κοινοποίησής του μέσω κώδικα QR.
- Το πρόβλημα οξύνεται όταν η σχολική μονάδα εφαρμόζει πρακτικές BOYD, οπότε οι συσκευές των μαθητών θα πρέπει να συνδέονται στο ασύρματο δίκτυο κατά την έναρξη του μαθήματος και να αποσυνδέονται αμέσως μετά.
- Τυχόν αλλαγή του μυστικού κλειδιού θα πρέπει να γίνει σε όλα τα AP της σχολικής μονάδας και σε όλες τις συσκευές των εξουσιοδοτημένων χρηστών, διαδικασία ιδιαίτερα χρονοβόρα ειδικά αν στο δίκτυο συνδέονται πολλές συσκευές.

Προκύπτει λοιπόν η ανάγκη για ένα σύστημα πιστοποίησης που να έχει τα ακόλουθα χαρακτηριστικά:

- Να παρέχει τη δυνατότητα εξατομικευμένης ταυτοποίησης των χρηστών, χρησιμοποιώντας όνομα χρήστη και κωδικό πρόσβασης. Με τον τρόπο αυτό,

ISBN: 978-960-578-084-5

αν ένας από τους κωδικούς διαρρεύσει θα χρειαστεί αλλαγή μόνο για το συγκεκριμένο χρήστη και όχι για όλους. Επιπλέον θα μπορούν να απενεργοποιούνται λογαριασμοί μαθητών, όταν δεν χρησιμοποιούνται.

- Η διαχείριση του συστήματος, τουλάχιστον μετά το στάδιο της αρχικής παραμετροποίησης, θα πρέπει να είναι απλή έτσι ώστε να μην ξοδεύεται πολύς χρόνος σε αυτήν και να μην απαιτεί εξειδικευμένες γνώσεις.

Η πιστοποίηση με το πλαίσιο 802.1x και τη χρήση RADIUS Server μπορεί να ανταποκριθεί στην πρώτη από αυτές τις απαιτήσεις, παρέχοντας την δυνατότητα εξατομικευμένης ταυτοποίησης χρηστών. Η υλοποίηση χρησιμοποιώντας το Zeroshell, μια εξειδικευμένη διανομή Linux που, μεταξύ άλλων, υλοποιεί έναν RADIUS Server και επιτρέπει την διαχείριση χρηστών μέσω ενός απλού γραφικού περιβάλλοντος, μπορεί να καλύψει και την δεύτερη απαίτηση.

## *3. Ταυτοποίηση 802.1x*

Το πλαίσιο 802.1x (Chen & WANG, 2005) στηρίζεται στη χρήση του EAP (Extensible Authentication Protocol), ενός πρωτοκόλλου που αρχικά χρησιμοποιήθηκε για την πιστοποίηση χρηστών σε συνδέσεις σημείου προς σημείο (point to point). Μία από τις μεθόδους πιστοποίησης που χρησιμοποιεί είναι και η χρήση Radius Server που θα χρησιμοποιηθεί και στην παρούσα υλοποίηση. Για την περιγραφή του τρόπου με τον οποίο επιτυγχάνεται η πιστοποίηση χρηστών με το πρωτόκολλο 802.1x και την χρήση του Radius Server θα πρέπει να αποσαφηνιστούν οι παρακάτω έννοιες/ρόλοι των συμμετεχόντων στη διαδικασία.

*Αιτούμενος (supplicant):* Κάθε χρήστης/συσκευή που ζητά να συνδεθεί στο δίκτυο. Συνήθως φορητός υπολογιστής, tablet ή κινητό τηλέφωνο.

*Πιστοποιητής ταυτότητας (authenticator):* Η συσκευή που ελέγχει την πρόσβαση στο δίκτυο και διαμεσολαβεί στην διαδικασία ταυτοποίησης. Συνήθως πρόκειται για τα σημεία πρόσβασης (AP) που συνδέουν τις συσκευές στο ασύρματο δίκτυο.

*Διακομιστής πιστοποίησης (authentication server):* Η συσκευή που θα αποφανθεί αν ένας χρήστης/συσκευή είναι εξουσιοδοτημένος για σύνδεση στο ασύρματο δίκτυο. Στην προτεινόμενη υλοποίηση το ρόλο αυτό θα έχει ο RADIUS Server που θα υλοποιήσει το Zeroshell.

Ο RADIUS Server του Zeroshell χρησιμοποιεί δύο μεθόδους πιστοποίησης, τις EAP-TLS και PEAP (Authentication on Wireless networks, n.d.). Στην πρώτη απαιτείται η εγκατάσταση ενός ψηφιακού πιστοποιητικού στον αιτούμενο (δημιουργείται από το Zeroshell), ενώ στη δεύτερη χρησιμοποιείται το πρωτόκολλο MS-CHAPv2 και ο αιτούμενος ταυτοποιείται παρέχοντας ως διαπιστευτήρια όνομα χρήστη (user name) και συνθηματική λέξη (password).

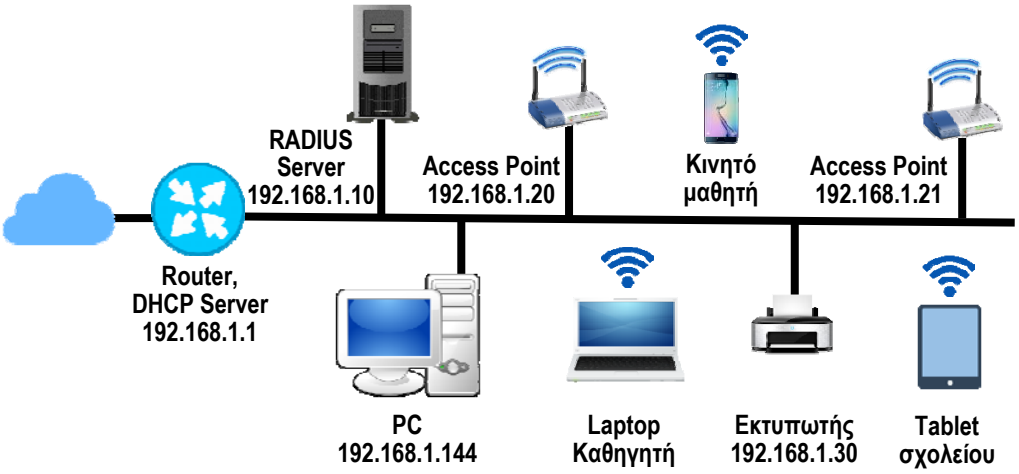
ISBN: 978-960-578-084-5

Μετά τη σύνδεση στο δίκτυο, οι πληροφορίες που διακινούνται κρυπτογραφούνται με κλειδιά που αλλάζουν ανά τακτά χρονικά διαστήματα. Επιπλέον οι πιστοποιητές ταυτότητας και ο διακομιστής πιστοποίησης συνδέονται με σχέση εμπιστοσύνης, αφού μοιράζονται μία κοινή μυστική φράση, όπως περίπου στο WPA2, που όμως δεν κοινοποιείται σε κανέναν. Συνοπτικά, η διαδικασία ελέγχου ταυτότητας γίνεται ως εξής:

- Ο αιτούμενος συνδέεται σε ένα πιστοποιητή ταυτότητας (AP) και ζητά σύνδεση στο δίκτυο. Το AP ζητά τα διαπιστευτήρια του αιτούμενου.
- Ο αιτούμενος παρέχει τα διαπιστευτήρια, τα οποία μεταδίδονται (κρυπτογραφημένα) στον διακομιστή πιστοποίησης.
- Ο διακομιστής πιστοποίησης αποφαίνεται σχετικά με την ταυτοποίηση του αιτούμενου. Αν αυτή είναι επιτυχής ο αιτούμενος συνδέεται στο ασύρματο δίκτυο και μπορεί να χρησιμοποιήσει τις υπηρεσίες του.

## *4. Υλοποίηση*

Ως παράδειγμα για την υλοποίηση θα χρησιμοποιηθεί ένα τυπικό δίκτυο Σχολικής μονάδας, όπως αυτό που φαίνεται στην Εικόνα 1. Οι αναγραφόμενες διευθύνσεις (εδώ σε δίκτυο 192.168.1.0/24) θα πρέπει να προσαρμοστούν στο σχήμα διευθυνσιοδότησης που υλοποιεί ο DHCP Server κάθε Σχολικής μονάδας.




***Εικόνα 1.*** *Ενδεικτική απεικόνιση δικτύου Σχολικής μονάδας*

### *4.1 Απαιτήσεις σε υλικό*

Οι απαιτήσεις σε υλικό του Zeroshell είναι πολύ μικρές. Μπορεί να εγκατασταθεί σε ένα παλαιό και παροπλισμένο υπολογιστή ή ακόμη και σε μία εικονική μηχανή, που θα πρέπει να βρίσκεται σε μόνιμη λειτουργία. Μπορεί επίσης να εγκατασταθεί και σε

ISBN: 978-960-578-084-5

συσκευές αρχιτεκτονικής ARM, (π.χ. Raspberry Pi, και να τοποθετηθεί μέσα στην ντουλάπα εξοπλισμού (rack), καθώς η διαχείρισή του, μετά την αρχική παραμετροποίηση, γίνεται απομακρυσμένα μέσω Web Server.

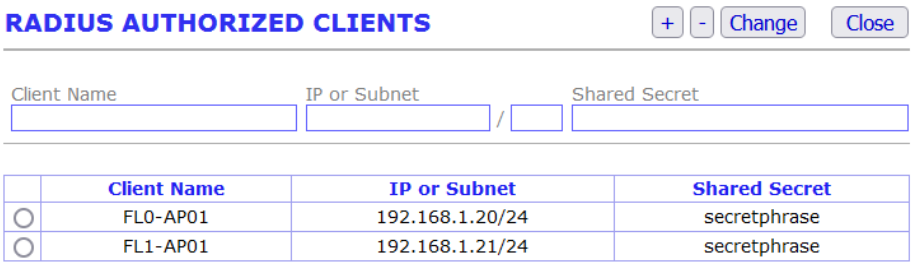
Απαραίτητο πάντως είναι τα AP της Σχολικής μονάδας να υποστηρίζουν τη μέθοδο ασφαλείας WPA/WPA2 Enterprise έτσι ώστε να μπορούν να συνδεθούν με τον RADIUS Server μέσω του κοινού κλειδιού.

### *4.2 Εγκατάσταση*

Τα αρχεία εγκατάστασης του βρίσκονται στον επίσημο δικτυακό τόπο της διανομής https://zeroshell.org/download/, υπάρχουν όμως διαθέσιμα και στον ftp server του Πανεπιστημίου Κρήτης στη διεύθυνση http://ftp.cc.uoc.gr/mirrors/linux/zeroshell/. Η εγκατάσταση του Zeroshell γίνεται μέσω περιβάλλοντος γραμμής εντολών χωρίς να παρουσιάζει ιδιαίτερη δυσκολία. Κατά τη διάρκειά της θα ζητηθεί το password του διαχειριστή, το Domain Name του σχολείου (μπορεί να δοθεί αυτό του ΠΣΔ ή να παραμείνει το προεπιλεγμένο example.com), το τρέχον προφίλ εργασίας και οι ρυθμίσεις για την IP διεύθυνση, την μάσκα υποδικτύου και την προεπιλεγμένη πύλη του δικτύου. Θα πρέπει να δοθεί μία στατική IP διεύθυνση, σε χώρο διευθύνσεων που να μην αποδίδεται από τον DHCP Server. Όλες αυτές οι ρυθμίσεις μπορούν να αλλάξουν από το μενού που εμφανίζεται μετά την εγκατάσταση, αλλά και απομακρυσμένα, μετά την εισαγωγή των δικτυακών ρυθμίσεων.

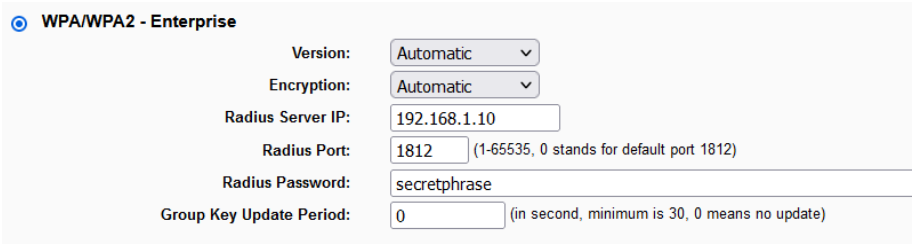
### *4.3 Διαμόρφωση*

Από το μενού USERS επιλέγουμε RADIUS και τσεκάρουμε το Enabled για να ενεργοποιηθεί ο RADIUS Server. Στη συνέχεια πατάμε στην καρτέλα Authorized Clients και για κάθε AP της σχολικής μονάδας καταχωρούμε ένα όνομα, την IP διεύθυνσή του και την μυστική φράση, (Εικόνα 2). Η ίδια φράση θα καταχωρηθεί και στις ρυθμίσεις των AP (Εικόνα 3), ώστε να δημιουργηθεί η σχέση εμπιστοσύνης με τον RADIUS Server. Όταν ολοκληρωθεί η καταχώρηση πατάμε το +.




***Εικόνα 2.*** *Καταχώρηση AP στον RADIUS Server*

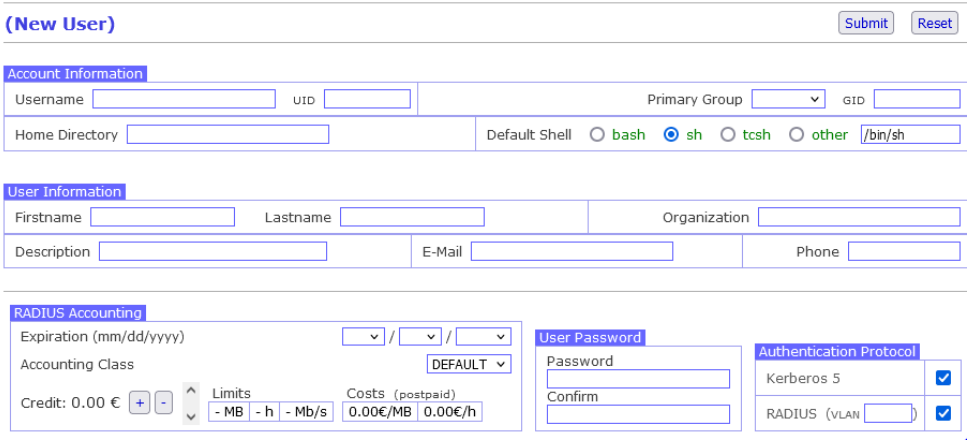
ISBN: 978-960-578-084-5




***Εικόνα 3.*** *Ρύθμιση ασφαλείας σε AP (TP-LINK TL-WA701ND)*

### *4.4 Δημιουργία/Διαχείριση χρηστών*

Από το μενού USERS επιλέγουμε Users και στην συνέχεια την καρτέλα Add. Εμφανίζεται η οθόνη της Εικόνας 4 στην οποία εισάγουμε τα στοιχεία του χρήστη. Απαιτείται η εισαγωγή ονόματος χρήστη (Username), ονόματος (Firstname), επώνυμου (Lastname) και Password. Σε περίπτωση που τα AP υποστηρίζουν την δημιουργία εικονικών δικτύων (VLAN) μπορούμε να αντιστοιχίσουμε το χρήστη σε κάποιο από αυτά, απομονώνοντας έτσι ομάδες χρηστών, π.χ. μαθητές ή επισκέπτες, από το υπόλοιπο δίκτυο ή/και ρυθμίζοντας το διαθέσιμο για κάθε κατηγορία χρηστών εύρος ζώνης. Πατάμε Submit και στη συνέχεια εμφανίζεται το ψηφιακό πιστοποιητικό του χρήστη που μπορούμε να το εξάγουμε για καταχώρηση στη φορητή συσκευή. Αυτό μπορεί να γίνει και αργότερα, επιλέγοντας από τη λίστα το όνομα του χρήστη και πατώντας στην καρτέλα X509. Όταν σε μια ασύρματη συσκευή εγκατασταθεί το πιστοποιητικό η σύνδεση γίνεται απευθείας χωρίς να χρειάζεται εισαγωγή username και password (π.χ. για φορητές συσκευές που ανήκουν στη σχολική μονάδα). Οι υπόλοιπες καρτέλες αφορούν στη διαχείριση των χρηστών απ' όπου μπορεί να γίνει διαγραφή ενός χρήστη και τροποποίηση των στοιχείων του, συμπεριλαμβανομένης της αλλαγής password.




***Εικόνα 4.*** *Η καρτέλα για την εισαγωγή νέου χρήστη*

ISBN: 978-960-578-084-5

### *4.5 Παρακολούθηση*

Το Zeroshell κρατά αναλυτικά αρχεία καταγραφής που είναι προσβάσιμα από την επιλογή SYSTEM/Logs. Αυτά που αφορούν τον RADIUS Server εμφανίζονται επιλέγοντας στον κατάλογο section το radius. Μέσω αυτών μπορούμε να δούμε, ανά ημέρα, τις αιτήσεις για σύνδεση στο ασύρματο δίκτυο. Αν διαπιστώσουμε ότι ένας χρήστης συνδέεται υπερβολικά συχνά ή με πάρα πολλές ταυτόχρονες συνδέσεις, τότε ίσως έχει διαρρεύσει το συγκεκριμένο password, το οποίο μπορεί να αλλάξει όπως περιγράφηκε προηγουμένως.

## *5. Συμπεράσματα*

Η χρήση του RADIUS Server του Zeroshell, μπορεί να αποτελέσει μία αξιόπιστη και ευέλικτη λύση για την σύνδεση χρηστών σε ασύρματο δίκτυο. Το γεγονός ότι διατίθεται δωρεάν, αλλά και οι χαμηλές του απαιτήσεις σε υλικό και υπολογιστική ισχύ σημαίνουν ότι μπορεί να εγκατασταθεί σε κάποιον παλιό υπολογιστή ή σε εικονική μηχανή, χωρίς ουσιαστικά κανένα κόστος για τη Σχολική μονάδα.

## *Αναφορές*

Authentication on Wireless networks. (n.d.). Ανακτήθηκε 20/8/2021 από το https://zeroshell.org/radius-details/

Chen, J. C., & Wang, Y. P. (2005). Extensible Authentication Protocol (EAP) and IEEE 802.1 x: Tutorial and Empirical Experience. *IEEE Communications Magazine*, *43*(12), S26-S32. doi: 10.1109/MCOM.2005.1561920

Consortium for School Networking. (2015). *Wireless best practices for schools*. Washington, DC. Ανάκτηση από το https://cosn.org/sites/default/files/pdf/Wireless Best Practices for Schools – COSN 2-18-2015_ALV.pdf

Khasawneh M., Kajman I., Alkhudaidy R., Althubyani A. (2014). A Survey on Wi-Fi Protocols: WPA and WPA2. In Pérez G. Martínez, S.M. Thampi, R. Ko, & L. Shu (Eds.) *Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2014. Communications in Computer and Information Science, Vol 420* (pp. 496-511). Springer, Berlin, Heidelberg. doi: 10.1007/978-3-642-54525-2_44

Rae, G., Dabner, N., & Mackey, J. (2017). Bring Your Own Device (BYOD) and teacher pedagogy in a New Zealand primary school. *Teachers and Curriculum*, *17*(2), 53-60. doi: 10.15663/tandc.v17i2.160

Sung, Y. T., Chang, K. E., & Liu, T. C. (2016). The effects of integrating mobile devices with teaching and learning on students' learning performance: A meta-analysis and research synthesis. *Computers & Education*, *94*, 252-275. doi: 10.1016/j.compedu.2015.11.008

ISBN: 978-960-578-084-5

Suryani, A. (2010). ICT in education: Its benefits, difficulties, and organizational development issues. *Jurnal Sosial Humaniora (JSH)*, *3*(1), 13-33. doi: 10.12962/j24433527.v3i1.651

## Abstract

ICT plays an important role in contemporary education. Mobile devices are being increasingly used to support it, releasing teachers and students from the narrow confines of the computer lab. Building on this trend, many schools implement Bring Your Own Device (BOYD) policies, aiming at using students' devices in the teaching process. Utilizing all this equipment requires connection to a wireless network, which in turn raises security issues that cannot be addressed by ordinary security practices. This paper proposes a secure, versatile and easily managed user authentication method for connection to wireless networks, using the IEEE 802.1x standard combined with a RADIUS Server.

**Keywords:** WLAN, security, authentication, RADIUS Server.

ISBN: 978-960-578-084-5