Πρόταση διδασκαλίας Εννοιών και Τεχνικών Ασφαλείας στη Δικτυακή Επικοινωνία. Εφαρμογή στο ΕΠΑ.Λ.

Τάσος Χατζηπαπαδόπουλος[1], Δρ. Β. Σ. Μπελεσιώτης[2]

[1]Καθηγητής Πληροφορικής 6ο ΕΠΑ.Λ. Αθήνας/1ο ΕΚ Αθήνας
chatzipap@gmail.com
[2]Σχολικός Σύμβουλος Πληροφορικής
vbelesiotis@sch.gr

Περίληψη

Στο άρθρο αυτό κατατίθεται μια διδακτική πρόταση σχετικά με τη διδασκαλία εννοιών και τεχνικών ασφάλειας στη δικτυακή επικοινωνία, με σκοπό την αξιοποίησή της στην εκπαιδευτική διαδικασία για την ενίσχυση των μαθησιακών αποτελεσμάτων. Το προτεινόμενο διδακτικό σενάριο στοχεύει στο να συνδράμει τόσο στην υποστήριξη της διδασκαλίας όσο και στην εποικοδομητική, μαθησιακά, εμπλοκή των μαθητών με μια πληθώρα σχετικών εννοιών που συναντώνται σε πολλά μαθήματα Πληροφορικής και σε όλους τους τύπους σχολείων. Το παρόν άρθρο εστιάζεται στον Τομέα Πληροφορικής των ΕΠΑ.Λ. και στο μάθημα Δικτύων, χωρίς να περιορίζεται μόνο σε αυτό. Οι δραστηριότητες που το συνοδεύουν αποσκοπούν στην επίτευξη υψηλού γνωσιακά επιπέδου μάθησης των σχετικών εννοιών, καθώς και στην ανάπτυξη δεξιοτήτων και στάσεων. Αυτό επιχειρείται και με τη σύνδεση των εννοιών με την καθημερινότητα του σύγχρονου μαθητή-πολίτη κατά την επικοινωνία του είτε γενικά ή σε θέματα συναλλαγών του με τρίτους.

Λέξεις κλειδιά: Διδακτική Πληροφορικής, ασφάλεια, κωδικοποίηση, ψηφιακή υπογραφή, διδακτικό σενάριο.

1. Εισαγωγή

Η διδασκαλία εννοιών σχετικά με την ασφάλεια κατά τη δικτυακή επικοινωνία συναντάται σε μαθήματα Πληροφορικής σε όλες τις βαθμίδες και τύπους σχολείων, σε ανάλογη έκταση και εμβάθυνση. Ειδικά στον Τομέα Πληροφορικής των ΕΠΑ.Λ. και στην Κατεύθυνση «Υποστήριξη συστημάτων, Εφαρμογών Δικτύων Η/Υ» της Γ΄ τάξης του Επαγγελματικού Λυκείου περιέχεται στη διδακτέα-εξεταστέα ύλη (ΦΕΚ 2420/τΒ΄/2014, 2014) και σε σχετική ενότητα που υποστηρίζεται από αντίστοιχο βιβλίο (Τεχνολογία Δικτύων Επικοινωνιών, ΚΕΦ. 8, Αρβανίτης κ.ά. 2014).

Αν και η επικοινωνία μέσω δικτύων και ιδιαίτερα του Διαδικτύου αποτελεί ένα σχετικά κλασσικό διδακτικό αντικείμενο, αυτό έχει ιδιαίτερες διδακτικές απαιτήσεις,

μια και εμπλουτίζεται συνεχώς με νέες τεχνικές και μεθοδολογίες ασφάλειας. Παρατηρούμε ότι την τελευταία δεκαετία, αυτές ολοένα αυξάνονται, μια και περισσότεροι χρήστες χρησιμοποιούν για τις συναλλαγές τους διαδικτυακές υπηρεσίες, σε τομείς όπως, η συναλλαγή με τη δημόσια διοίκηση και τις τράπεζες, το ηλεκτρονικό εμπόριο, η κράτηση θέσης σε εκδήλωση κ.ά. Στο παραπάνω σκεπτικό εντάσσονται και τα θέματα της ηλεκτρονικής διακυβέρνησης των κρατών, αλλά και των εταιριών, με τη θέσπιση της χρήσης των ηλεκτρονικών επικοινωνιών ως κύριου πλέον μέσου ανταλλαγής δημοσίων και ιδιωτικών εγγράφων. Η καθιέρωση του μέσου αυτού είναι επιβεβλημένη ως κυρίαρχος τρόπος επικοινωνίας, λόγω των πολλών πλεονεκτημάτων που παρουσιάζει σε σχέση με παραδοσιακούς τρόπους διακίνησης πληροφορίας. Πλεονεκτήματα όπως είναι η μείωση τους κόστους, η αύξηση της ταχύτητας και η ασφάλεια υπό τις κατάλληλες προϋποθέσεις.

Σε κάθε διαδικτυακή επικοινωνία, όταν αυτή εξελίσσεται μέσω "ασφαλών" δικτύων, τα θέματα υπονόμευσης της ασφάλειας των συναλλαγών είναι μειωμένα, πράγμα που δεν συμβαίνει όταν γίνεται μέσω ανοιχτών δημόσιων δικτύων, όπως για παράδειγμα συχνά συναντάμε σε πολλές υπηρεσίες στο Διαδίκτυο. Οι βασικές έννοιες καθώς και τεχνικές του τομέα αυτού της ασφάλειας δικτύων και επικοινωνιών, όπως είναι η ασυμμετρική κρυπτογράφηση, η ψηφιακή υπογραφή, η χρήση αλγορίθμων κατατεμαχισμού, αποτελούν, όπως αναφέρθηκε, αντικείμενα μελέτης του τομέα Πληροφορικής των ΕΠΑ.Λ., με τους μαθητές στο μάθημα των Δικτύων της Γ΄ Τάξης των ημερησίων και Δ΄ Τάξης των εσπερινών ΕΠΑ.Λ. να διδάσκονται επαρκώς σχετικές βασικές έννοιες και διαδικασίες. Οι στόχοι τέτοιων ενοτήτων πρέπει να αποσκοπούν τόσο στην εξειδίκευση του μαθητή ως αυριανού ειδικού Πληροφορικής όσο και στη χρήση του Διαδικτύου χρησιμοποιώντας διαδικασίες ασφάλειας. Η απλή και θεωρητική αναφορά των τεχνικών όρων και των μηχανισμών λειτουργίας τους δεν επαρκεί για την σε βάθος κατανόηση των λεπτών αυτών εννοιών ασφάλειας παρόλο που ως λέξεις (κρυπτογράφηση, ψηφιακή υπογραφή κ.λπ.) είναι γνωστές κατ' αρχάς στους μαθητές. Για να επιτευχθεί μια σε βάθος επιτυχής γνωσιακή εμπλοκή του μαθητή με τις έννοιες και τις τεχνολογίες αυτές, γνώση που να εκτείνεται σε όλες τις μαθησιακές κλίμακες (Anderson et al, 2001), απαιτείται υποστήριξη της διδασκαλίας από ποικίλα μέσα σε λογισμικό και εξοπλισμό, αλλά και με σχετικά διδακτικά σενάρια. Σε αυτό έρχεται να συνεισφέρει το άρθρο αυτό, όπου επιχειρείται να περιγραφεί μια ολοκληρωμένη διδακτική πρόταση με σκοπό την επίτευξη υψηλού μαθησιακού επιπέδου, διευκολύνοντας παράλληλα την διδασκαλία του αντικειμένου.

Το υπόλοιπο του άρθρου εξελίσσεται ως εξής: Στην ενότητα 2 "Θεωρητικό Υπόβαθρο" αναλύονται συνοπτικά θεωρητικά ζητήματα άμεσα συνδεόμενα με το θέμα τόσο στην θεματική περιοχή της Διδακτικής Πληροφορικής όσο και σε αυτήν της ασφάλειας και δικτύωσης. Στην ενότητα 3 παρουσιάζεται το Διδακτικό σενάριο, ενώ στην ενότητα 4 κατατίθενται παρατηρήσεις μας από την εφαρμογή του στην τάξη και χρήσιμα συμπεράσματα και προτάσεις για πιθανή αξιοποίησή του. Το άρθρο κλείνει με αναφορές οι οποίες αναφέρθηκαν στο κείμενο.

2. Θεωρητικό υπόβαθρο

Ένα διδακτικό σενάριο απαιτείται να ενσωματώνει κατάλληλα τόσο θεωρήσεις και μεθοδολογίες της Διδακτικής Πληροφορικής όσο και την ορθή αναφορά και χρήση των εννοιών και τεχνικών της επιστημονικής περιοχής που διαπραγματεύεται, με την κατάλληλη προσαρμογή της επιστημονικής γνώσης στο γνωσιακό επίπεδο των μαθητών.

Οι προς διαπραγμάτευση έννοιες και μεθοδολογίες που εμπλέκονται εδώ είναι πολλές, με πιο βασικές την κρυπτογράφηση με τη χρήση δημόσιου κλειδιού, τις συναρτήσεις κατατεμαχισμού, την ψηφιακή υπογραφή. Διαδικαστικά, η χρήση αλγορίθμων κατατεμαχισμού και κρυπτογράφησης γίνεται με τη χρήση OnLine εργαλείων για την υλοποίηση των παραπάνω αλγορίθμων, όπως και η ακολουθούμενη μεθοδολογία της ψηφιακής υπογραφής.

Πιο αναλυτικά, η ασυμμετρική κρυπτογράφηση, ή κρυπτογράφηση δημόσιου κλειδιού, βασίζεται στη χρήση δύο κλειδιών, ενός δημοσίου και ενός ιδιωτικού, όπως επίσης στη ψηφιακή υπογραφή χρησιμοποιούνται δύο ζεύγη τέτοιων κλειδιών ένα ζεύγος για τον αποστολέα και ένα για τον παραλήπτη, με τα δημόσια κλειδιά να ανταλλάσσονται κατά την έναρξη της επικοινωνίας. Ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για την κρυπτογράφηση της σύνοψης του αποστελλόμενου μηνύματος (ψηφιακή υπογραφή) και ο παραλήπτης το δημόσιο του αποστολέα για την επαλήθευσή της. Η μεθοδολογία αυτή εξασφαλίζει, εκτός από την αυθεντικότητα του αποστολέα. την ακεραιότητα των δεδομένων και τη μη άρνηση ταυτότητας. Εάν δε ο αποστολέας χρησιμοποιήσει και το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση του μηνύματος εξασφαλίζει και την εμπιστευτικότητα. Αποτελεί επίσης για τις ιδιωτικές, τις δημόσιες υπηρεσίες αλλά και τους απλούς χρήστες του Διαδικτύου ένα πολύ χρήσιμο εργαλείο για την ασφάλεια στη διακίνηση εγγράφων. «*Το Π.Δ. 150/2001 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μια ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μια ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν*», (Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, ΕΕΤΤ). Η τεχνική της ψηφιακής υπογραφής διαθέτει πολλά από τα χαρακτηριστικά της ασφάλειας δικτύων τα οποία συνήθως οι εκπαιδευόμενοι αποστηθίζουν, (ακεραιότητα, αυθεντικότητα, μη άρνηση ταυτότητας, δημόσια – ιδιωτικά κλειδιά, συνάρτηση κατατεμαχισμού, σύνοψη μηνύματος, κρυπτογράφηση - αποκρυπτογράφηση) τα οποία, σε συνδυασμό με τον τρόπο λειτουργίας της, δυσχεραίνουν ιδιαίτερα τους μαθητές στις αρχικές διδακτικές προσεγγίσεις καθιστώντας τις τεχνικές ασφαλείας ένα από τα δύσκολα σημεία διδασκαλίας των δικτύων. Οι μαθητές παρόλο που έχουν έρθει σε επαφή με πλήθος εννοιών ασφάλειας στις προηγούμενες ενότητες, έχουν συνήθως αδυναμία να τις

συσχετίσουν με τις κατάλληλες ενέργειες, τη σειρά εκτέλεσης και με τα αντίστοιχα αποτελέσματά τους. Μπορούν για παράδειγμα να απαντήσουν στην ερώτηση τι μας προσφέρει η αυθεντικότητα ή η εμπιστευτικότητα, αλλά δυσκολεύονται να απαντήσουν με ποιο κλειδί συνδέεται η αντίστοιχη έννοια. Και όταν το κάνουν αυτό είναι περισσότερο προϊόν αποστήθισης παρά λογικής συσχέτισης της λειτουργίας του κάθε κλειδιού.

Στα θέματα Διδακτικής Πληροφορικής και Μέσων υποστήριξης της διδασκαλίας, το παρόν σενάριο, ως προς τα θέματα αξιοποίησης των θεωρήσεων της Διδακτικής, βασίζεται και αντλεί τις διδακτικές πρακτικές του από τις σύγχρονες θεωρίες μάθησης, όπως είναι ο κοινωνικός εποικοδομισμός και οι θωρήσεις για την επεξεργασία των πληροφοριών στον εγκέφαλο. Επίσης ενσωματώνει αυτές σχετικά με την κοινωνική οργάνωση της τάξης, αξιοποιώντας το Ομαδοσυνεργατικό σχήμα και λαμβάνει υπόψη του τα θέματα γνωστικών ταξινομιών (Anderson et al., 2001) και νοημοσύνης (Gardner, 1993). Επίσης, θεωρήσεις της γνωστικής επιστήμης όπως αυτή που αναφέρει ότι η σκέψη μπορεί να κατανοηθεί καλύτερα με δομές αναπαράστασης και υπολογιστικές διαδικασίες χειρισμού των δομών αυτών, γνωστή ως υπολογιστική αναπαραστατική κατανόησης του νου (Computational - Representational Understanding of the Mind,, CRUM) (Thagard, 1996). Ως προς τα Μέσα υποστήριξης της διδασκαλίας, χρησιμοποιούνται διαδικτυακά εργαλεία, και λογισμικό, όπως αυτό της εννοιολογικής χαρτογράφησης (Cmap Tools, 2015) το οποίο χρησιμοποιείται για τη διαγραμματική αναπαράσταση της ανθρώπινης γνώσης για μια θεματική περιοχή. Η γνώση αποτελείται από μια σύνθεση μεταξύ των εννοιών της θεματικής περιοχής και των σχέσεων μεταξύ τους, σχηματίζοντας προτάσεις και δημιουργώντας ένα συνεκτικό σύστημα που διαφοροποιείται ανάλογα με την προϋπάρχουσα γνώση του ατόμου (Novak & Canas, 2006). Η ένταξη της εννοιολογικής χαρτογράφησης στην εκπαιδευτική διαδικασία παρέχει γνωστικό εργαλείο που βοηθά τους μαθητές να οργανώσουν, να συνδέσουν και να αναδομήσουν τις γνώσεις που ήδη κατέχουν, να συσχετίσουν τις νέες έννοιες που δεν έχουν οικοδομηθεί πλήρως ή έχουν οικοδομηθεί εσφαλμένα (Γουλή Ε. κ.ά., 2006). Μπορεί να χρησιμοποιηθεί σε πολλές φάσεις του σεναρίου διδασκαλίας, όπως στην εναρκτήρια φάση και τη φάση αυτοαξιολόγησης. Μια πιο προχωρημένη δυναμική αναπαράσταση γνώσης μπορεί να γίνει μέσω των Οντολογιών (Belesiotis V., Alexandris N., 2009).

Όλα τα παραπάνω μπορούν να βοηθήσουν από τη μια μεριά τον εκπαιδευτικό να τα προσαρμόσει σύμφωνα με την οργάνωση της τάξης, του διαθέσιμου εξοπλισμού αλλά και τη σύνθεση του μαθητικού δυναμικού και από την άλλη τους μαθητές να διαφωνήσουν, να συνεργαστούν μεταξύ τους, να αναπτύξουν πρωτοβουλία, κριτική αλλά και δημιουργική σκέψη, οικοδομώντας σταδιακά τη ατομική και συλλογική γνώση αναβαθμίζοντας τις γνωστικές τους ικανότητες.

3. Διδακτικό σενάριο

3.1 Γενικά στοιχεία

Η διδακτική πρόταση αφορά κύρια στη Γ΄ Τάξη του ημερησίου και στη Δ΄ Τάξη του εσπερινού ΕΠΑ.Λ. του τομέα Πληροφορικής - Δικτύων υπολογιστών και στο κεφάλαιο 8, Διαχείριση και Ασφάλεια Δικτύου, του διδακτικού εγχειριδίου (Τεχνολογία Δικτύων Επικοινωνιών, Αρβανίτης κ.ά. 2014).

Σκοπός του σεναρίου είναι να ευαισθητοποιήσει τους μαθητές στο γεγονός ότι όταν χρησιμοποιούμε το χώρο του Διαδικτύου για την επικοινωνία σημαντικών θεμάτων, είμαστε ευάλωτοι χωρίς τα κατάλληλα μέτρα σε θέματα ασφάλειας. Να τους εξηγήσει ότι η τεχνική της κρυπτογράφησης αποτελεί έναν από τους θεμέλιους λίθους της δικτυακής ασφάλειας, ο άλλος είναι το τείχος προστασίας και ότι η ψηφιακή υπογραφή μπορεί να δώσει λύση σε πολλά από αυτά. Επίσης να διευκολύνει στη κατανόηση των χαρακτηριστικών και της λειτουργίας του μηχανισμού της ασυμμετρικής κρυπτογράφησης και της ψηφιακής υπογραφής. Οι στόχοι του είναι, οι μαθητές να:

- Αναγνωρίζουν ότι το Διαδίκτυο είναι ένας χώρος με προβλήματα ασφάλειας.
- Ανακαλούν τους διδαχθέντες όρους ασφάλειας και να συσχετίζουν τα χαρακτηριστικά τους.
- Διακρίνουν τα αποτελέσματα ανάμεσα στη χρήση δημοσίου και του ιδιωτικού κλειδιού.
- Εξηγούν την έννοια αλλά και την αναγκαιότητα του αλγόριθμου κατατεμαχισμού.
- Ερμηνεύουν τις έννοιες Αυθεντικότητας, Ακεραιότητας, Μη άρνησης Ταυτότητας, Εμπιστευτικότητας.
- Αξιολογούν τους κινδύνους που προκύπτουν από τη μη χρήση της ψηφιακής υπογραφής και να αναγνωρίζουν τις συνθήκες κάτω από τις οποίες είναι απαραίτητη.
- Διακρίνουν τα πλεονεκτήματα της ψηφιακής υπογραφής και να στοιχειοθετούν τη χρησιμότητά της.
- Αναπαριστούν και να συντάσσουν τα βήματα δημιουργίας της ψηφιακής υπογραφής από την πλευρά του αποστολέα και του παραλήπτη.

Οργάνωση Τάξης: Το σενάριο πραγματοποιείται στο εργαστήριο Πληροφορικής, όπου και εφαρμόζεται κύρια το ομαδοσυνεργατικό σχήμα. Οι μαθητές χωρίζονται σε ομάδες των τριών ατόμων και έχουν στη διάθεσή τους έναν σταθμό εργασίας. Οι ρόλοι της ομάδας είναι: ο 1ος μαθητής, όταν είναι απαραίτητο, ανατρέχει σε αντίστοιχα σημεία του σχολικού βιβλίου, ο 2ος χειρίζεται τον υπολογιστή και ο 3ος μαθητής συμπληρώνει, όπου απαιτείται, τις δραστηριότητες των φύλλων εργασίας (ΦΕ), στο χαρτί ή αν υπάρχει η δυνατότητα χρόνου και μέσων σε wiki. Οι ερωτήσεις

των δραστηριοτήτων συμπληρώνονται μετά από συζήτηση και συμφωνία των μελών της ομάδας, με τους ρόλους να εναλλάσσονται σε κάθε ΦΕ.

Ρόλος εκπαιδευτικού: Στη κοινωνική οργάνωση της τάξης με την ομαδοσυνεργατική προσέγγιση, ο εκπαιδευτικός, λειτουργεί υποστηρικτικά ως διευκολυντής - εμψυχωτής και συμβάλλει για τη δημιουργία εποικοδομητικού κλίματος, αναζήτησης και δημιουργίας.

Δραστηριότητες υποστήριξης της διδασκαλίας: Η διδακτική πρόταση υποστηρίζεται από μια σειρά δραστηριοτήτων και ΦΕ που περιλαμβάνουν: συμπλήρωση ερωτηματολογίων, αναζητήσεις στο Διαδίκτυο για ανεύρεση υλικού, ερωτήσεις συμπλήρωσης και αντιστοίχισης, χρήσης OnLine εργαλείων κρυπτογράφησης και κατατεμαχισμού, όπως επίσης συμπλήρωσης, τροποποίησης και επέκτασης ΕΧ οι οποίες υλοποιούνται στο περιβάλλον του εργαστηρίου Πληροφορικής.

Μέσα και υποστηρικτικό υλικό: Για την εφαρμογή του σεναρίου θα χρειαστεί εργαστήριο Πληροφορικής με πρόσβαση στο Διαδίκτυο, βιντεοπροβολέας και πιθανά διαδραστικός πίνακας για την παρουσίαση του υλικού. Επίσης εγκατεστημένο το λογισμικό δημιουργίας και επεξεργασίας εννοιολογικών χαρτών (Cmap Tools, 2015).

Οι τεχνικές διδασκαλίας: Κατευθυνόμενη διερεύνηση - ανακάλυψη, με το διδάσκοντα σε ρόλο διευκολυντή, Καταιγισμός ιδεών, Μελέτη περίπτωσης, Προσομοίωση, Ομαδοσυνεργατική προσέγγιση.
Ο προτεινόμενος χρόνος διδασκαλίας: τρεις (3) ώρες.

Προαπαιτούμενες γνώσεις των μαθητών: Οι μαθητές πέραν των βασικών δεξιοτήτων χρήσης υπολογιστών και αναζήτησης στο Διαδίκτυο, πρέπει να έχουν γνωρίσει και εξασκηθεί στο λογισμικό εννοιολογικών χαρτών Cmap Tools.

3.2 Η διδακτική πορεία του σεναρίου. Φύλλα εργασίας

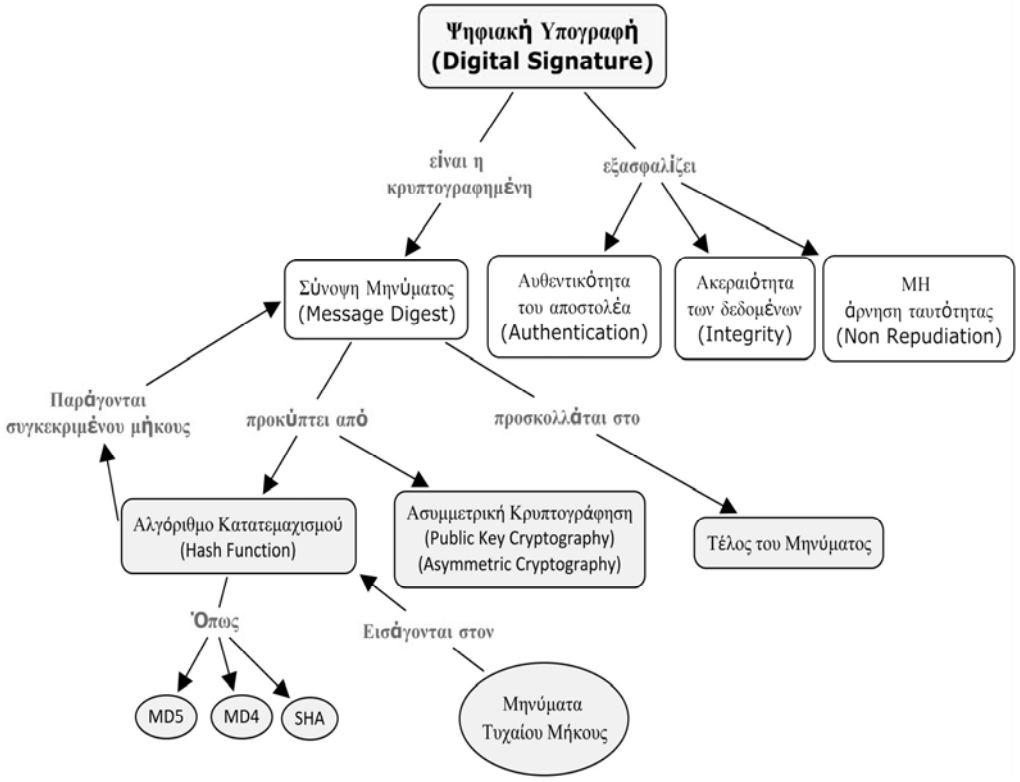
Το διδακτικό σενάριο περιλαμβάνει τρία φύλλα εργασίας (ΦΕ) καθένα εκ των οποίων έχει διάρκεια μίας (1) ώρας.

Το **ΦΕ-1** έχει σκοπό να φέρει σε επαφή τους μαθητές με πραγματικές καταστάσεις υπονόμευσης της ασφάλειας στις δικτυακές επικοινωνίες. Αυτό γίνεται για να τους ευαισθητοποιήσει στους κινδύνους που εκτίθεται ένας χρήστης, κάθε φορά που χρησιμοποιεί τον υπολογιστή του για την επικοινωνία του και να προκαλέσει το ενδιαφέρον τους σχετικά με τις έννοιες της ασφάλειας στις δικτυακές επικοινωνίες. Γι' αυτό το σκοπό χρησιμοποιούνται σχετικά και επίκαιρα άρθρα από την διαδικτυακή ειδησιογραφία. Σε αυτά δίνεται η δυνατότητα να συζητηθούν καταστάσεις επικοινωνίας μεταξύ μη ασφαλούς δικτύου, όπου μπορούν να δημιουργηθούν προβλήματα ασφάλειας. Προβλήματα όπως είναι η αποστολή ενός μηνύματος, όπου για παράδειγμα α) θα διαρρεύσουν κρίσιμες πληροφορίες (εμπιστευτικότητα), β)το μήνυμα αυτό θα τροποποιηθεί κακόβουλα από τρίτους μη

εξουσιοδοτημένους για δόλιους σκοπούς (ακεραιότητα), γ) κάποιος, κακόβουλα θα προσποιηθεί ότι είναι κάποιος άλλος και θα στείλει μηνύματα για λογαριασμό μας (αυθεντικότητα), δ) αυτός ο οποίος απέστειλε το μήνυμα θα αποποιηθεί της διαδικασίας αποστολής του για συγκεκριμένους λόγους αποποίησης ευθύνης (άρνηση ταυτότητας) (αναλυτικοί ορισμοί στο πρότυπο ISO 7498-2 (1989). Εδώ προτρέπουμε τους μαθητές να ανακαλέσουν και να αναφέρουν από την εμπειρία τους τυχόν παραδείγματα προσπάθειας εξαπάτησης με παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου, αναφέροντας και εμείς αντίστοιχα δικά μας. Στη συνέχεια οι μαθητές πλοηγούνται σε ιστοσελίδες της εταιρείας Akamai Technologies Inc. (2015), της εταιρείας Arbor Networks (2015) (The Active Threat Level Analysis System, ATLAS) και του κόμβου DigitalAttackMap (2015), όπου έχουν τη δυνατότητα να παρατηρήσουν την γραφική απεικόνιση διάφορων επιθέσεων ασφαλείας που συμβαίνουν σε παγκόσμιο επίπεδο και σε πραγματικό σχεδόν χρόνο. Στο τέλος καλούνται οι μαθητές να απαντήσουν σε ένα OnLine ερωτηματολόγιο με ερωτήσεις σχετικές με τις συνήθειές τους στις δικτυακές τους επικοινωνίες. Η δημιουργία του σε φόρμες google (google forms) μας δίνει τη δυνατότητα άμεσης παρουσίασης, συζήτησης και σχολιασμού των αποτελεσμάτων, με το διδάσκοντα να έχει τη δυνατότητα να αντιληφθεί παρανοήσεις και την ποικιλία αντιλήψεων.

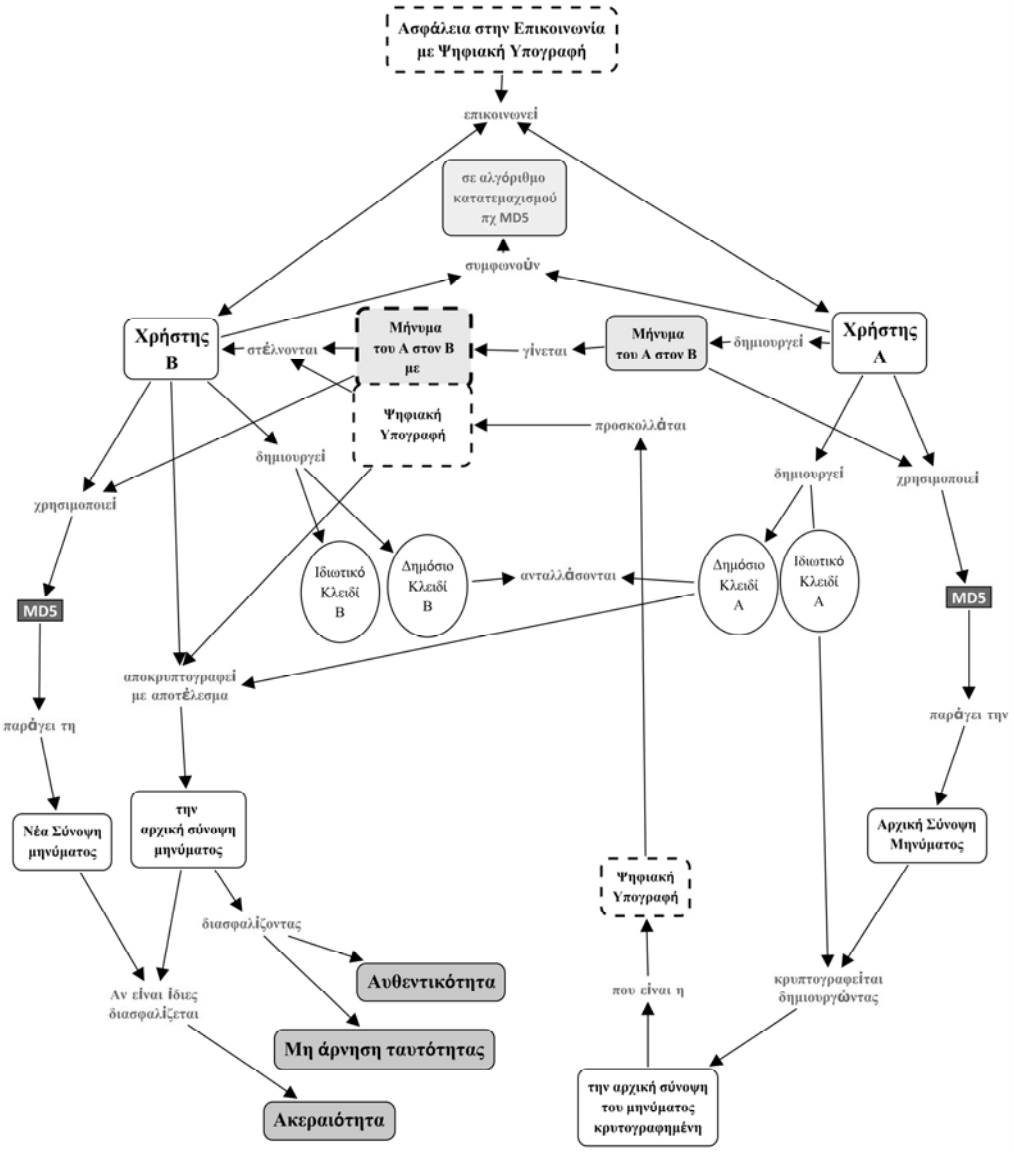
Στη συνέχεια και μετά το ΦΕ-1 ο εκπαιδευτικός προχωρά στη διδασκαλία των εννοιών και των τεχνικών της ασφάλειας δικτύων όπως καθορίζει το (ΠΣ) για 4-5 ώρες.

Στο **ΦΕ-2** που ακολουθεί, δίνεται βαρύτητα στην ανάκληση και κατανόηση της αποκτηθείσας γνώσης, όσον αφορά κυρίως στα χαρακτηριστικά και στις τεχνολογίες ασφάλειας των επικοινωνιών, πλήθος των οποίων χρησιμοποιεί η ψηφιακή υπογραφή. Αυτό επιτυγχάνεται με ερωτήσεις συμπλήρωσης κόμβων εννοιών και όρων σε εννοιολογικό χάρτη, καθώς και την προσθήκη σε αυτόν επιπλέον πληροφοριών από το Διαδίκτυο. Στη συνέχεια ζητείται να επεκτείνουν το δοθέντα ΕΧ με νέους κόμβους και να τοποθετήσουν κατάλληλα και την αντίστοιχη ξενόγλωσση ορολογία στους υπάρχοντες κόμβους. Ακολούθως, ζητείται να συμπληρώσουν κατάλληλα ορισμούς εννοιών και να τους τοποθετήσουν ως πληροφορίες στους κόμβους του ΕΧ κάνοντας έτσι και έλεγχο των προσληφθέντων γνώσεών τους. Το ολοκληρωμένο αποτέλεσμα του ολοκληρωμένου ΕΧ περιλαμβάνει και αναπαριστά διαγραμματικά όλες σχεδόν τις έννοιες που διδάχθηκαν, τους αντίστοιχους ορισμούς και τις σχέσεις μεταξύ τους. Στο τέλος του ΦΕ-2 έχουν τη δυνατότητα, χρησιμοποιώντας online εργαλεία κατατεμαχισμού και κρυπτογράφησης από τους δικτυακούς τόπους (Advameg Inc., 2015) και (OnLine RSA Key Generator, 2015), να δημιουργήσουν βήμα - βήμα τη δική τους ψηφιακή υπογραφή σε ένα συγκεκριμένο μήνυμα. Ο εκπαιδευτικός αξιολογεί τα συμπληρωμένα ΦΕ-2 και αποτιμά το βαθμό της προσληφθείσας γνώσης.



Εικόνα 1. *Ο ΕΧ του ΦΕ-2 ολοκληρωμένος*

Το τελευταίο **ΦΕ-3** αφορά στη λειτουργία της ψηφιακής υπογραφής, όπου απαιτείται βέβαια η εφαρμογή των όρων και εννοιών ασφάλειας που προηγήθηκαν. Δίνεται η σειρά των βημάτων λειτουργίας, με αλγοριθμικό θα λέγαμε τρόπο, ενώ απαιτείται η αναγνώριση και η συμπλήρωση των απαιτούμενων ενεργειών δημιουργώντας προτάσεις, έννοια - ενέργεια - αποτέλεσμα, καθώς και η αναπαράστασή τους στον εννοιολογικό χάρτη. Ο βαθμός δυσκολίας στα δοθέντα αλγοριθμικά βήματα μπορεί να διαφοροποιηθεί κατά την κρίση του εκπαιδευτικού και ανάλογα με τη σύνθεση της τάξης και το βαθμό των προσληφθέντων γνώσεων, αφαιρώντας λέξεις, προτάσεις ή και ολόκληρα βήματα. Ολοκληρώνοντας τον ΕΧ του ΦΕ-3, αναπαρίσταται πλήρως ο μηχανισμός λειτουργίας της ψηφιακής υπογραφής.



Εικόνα 2. *Ο ΕΧ του ΦΕ-3 ολοκληρωμένος*

3.3 Διδακτική εφαρμογή - Αποτίμηση

Το σενάριο, που η παρουσίασή του εδώ δεν είναι δυνατή σε πλήρη ανάπτυξη λόγω των περιορισμών της έκτασης του άρθρου από τις προδιαγραφές του Συνεδρίου, υλοποιήθηκε στο 6ο ΕΠΑ.Λ. Αθήνας κατά τα έτη 2013-14 και 2014-15 και παρουσιάστηκε στα πλαίσια δειγματικής διδασκαλίας το 2015.

Παρατηρήθηκε ότι το ποσοστό μαθητών που συμμετείχαν ενεργά ήταν σχεδόν καθολικό (90%), σε αντίθεση με παλαιότερα σχολικά έτη με διδασκαλία χωρίς την υποστήριξη τέτοιων μέσων, όπου η συμμετοχή των μαθητών στην εκπαιδευτική διαδικασία στην ενότητα αυτή κυμαινόταν μεταξύ 50-70% και ανάλογα τη σύνθεση του μαθητικού δυναμικού. Αυτό το γεγονός μαζί με μια ενδεικτική αύξηση του μέσου όρου των βαθμολογικών αποτελεσμάτων της τάξης στην ίδια διαδικασία γραπτής αξιολόγησης σε ποσοστό του 20-30% σε σχέση με παλαιότερα έτη, είναι ενθαρρυντικό στοιχείο για τη διδακτική αυτή πρακτική.

4. Συμπεράσματα και μελλοντικές κατευθύνσεις

Στο άρθρο αυτό κατατέθηκε μια διδακτική πρόταση σχετικά με τη διδασκαλία εννοιών και τεχνικών ασφάλειας στη δικτυακή επικοινωνία, η οποία σχετίζεται κύρια, χωρίς να περιορίζεται, στον Τομέα Πληροφορικής των ΕΠΑ.Λ. και το μάθημα των Δικτύων.

Από την εφαρμογή της στην τάξη διαπιστώθηκε ότι η διδακτική πρόταση συνέβαλε θετικά στο να κατανοήσουν οι μαθητές σύνθετες έννοιες του μαθήματος των δικτύων, όπως είναι αυτή της ασυμμετρικής κρυπτογράφησης, το ρόλο της συνάρτησης κατατεμαχισμού και της ψηφιακής υπογραφής. Πιστεύουμε ότι μέσα από τέτοιες διδακτικές προτάσεις, που εφαρμόστηκαν στην τάξη και έδειξαν θετικά μαθησιακά αποτελέσματα, μπορεί να βελτιωθεί η εκπαιδευτική διαδικασία. Στην κατεύθυνση αυτή, θεωρούμε ότι και η παραπάνω πρόταση αποτελεί μια καλή πρακτική προς εκμετάλλευση και κατάλληλη προσαρμογή της -πορεία, φύλα εργασίας- από το διδάσκοντα στο επίπεδο της τάξης του. Λόγω του πρόσθετου απαιτούμενου χρόνου που αναλώνεται για την εφαρμογή της, θεωρούμε ότι γενικά ενδείκνυται για νευραλγικά ή σύνθετα σημεία της διδακτέας ύλης και όχι για καθολική εφαρμογή σε όλο το φάσμα της διδασκαλίας του ανάλογου κεφαλαίου.

Μελλοντικά έχουμε σκοπό να ασχοληθούμε με τον εμπλουτισμό της διδακτικής πρότασης με δραστηριότητες και σε άλλα θεματικά αντικείμενα του μαθήματος και την περαιτέρω εφαρμογή τους στην τάξη.

5. Αναφορές

Advameg, Inc. (2015). http://www.unit-conversion.info/texttools/md4/#data.

Akamai Technologies Inc. (2015). http://wwwnui.akamai.com/gnet/globe/index.html Attacks/Hour from Akamai Kona network.

Arbor Networks (2015). https://atlas.arbor.net/. The Active Threat Level Analysis System, ATLAS.

Anderson L. W., Krathwohl D. R, Airasian P. W., Cruikshank K. A., Mayer R E., Pintrich P. R, Raths,J. & Wittrock M. C. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom 's taxonomy of educational objectives*, New York: Longman.

Belesiotis V., Alexandris N. (2009). A scenario for the development and use of teaching-oriented ontologies, *Int. J. Metadata, Semantics and Ontologies* 4, No. 3, 183-195 (2009), Available on. http://www.inderscience.com/browse/index.php?journalID=152&year=2009&vol=4&issue=3.

Cmap Tools. (2015). Florida institute for humans & machine cognition, (http://cmap.ihmc.us/).

Digital Attack Map. (2015). http://www.digitalattackmap.com/about/, DDoS attacks around the globe, built through a collaboration between Google Ideas and Arbor Networks.

Gardner, H. (1993), *Multiple Intelligences*. The Theory in Practice, Basic

ISO 7498-2. (1989). Information processing systems, Open Systems Interconnection, Basic Reference Model — Part 2: Security Architecture.

Novak D.J & Canas A (2006). *The Theory Underlying Concept Maps and How To Construct and Use Them, Institute for Human and Machine Cognition*. Accessed 24 Nov 2008.

Online RSA Key Generator, http://travistidwell.com/jsencrypt/demo.

Thagard Paul (1996). *Mind Introduction to Cognitive Science*. The MIT Press, London.

Γουλή, Ε., Γόγουλου, Α., & Γρηγοριάδου, Μ. (2006). Ο Εννοιολογικός Χάρτης στην Εκπαιδευτική διαδικασία του μαθήματος της Πληροφορικής: Μια Πιλοτική διερεύνηση. Θέματα στην Εκπαίδευση, Ειδικό Αφιέρωμα: Σύγχρονη έρευνα στη διδακτική της Πληροφορικής, 7:3, 351-377. Εκδόσεις Ελληνικά Γράμματα.

Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ). Ψηφιακές Υπογραφές, http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#6.

Αρβανίτης Κ., Κολυβάς Γ., Ούτσιος Σ. (2014). *Τεχνολογία Δικτύων Επικοινωνιών*, ΙΤΥΕ «Διόφαντος».

ΦΕΚ 2420/τΒ/10-09-2014, (2014). Υ.Α 138300/Γ2 Καθορισμός εξεταστέας και διδακτέας ύλης των Πανελλαδικά εξεταζόμενων μαθημάτων της Γ΄ τάξης Ημερησίων και Δ΄ τάξης Εσπερινών ΕΠΑ.Λ. για το σχολικό έτος 2014−2015 και το μάθημα «Δίκτυα Υπολογιστών ΙΙ» της Ειδικότητας «Υποστήριξη συστημάτων, Εφαρμογών Δικτύων Η/Υ».

Abstract

This article presents a didactic proposal related to the teaching of concepts and techniques in security and network communications, which has been developed to utilised in the educational process in order to enhance the learning outcome. The proposed didactic scenario aims to support the teaching process and assist the effective, in educational terms, engagement of pupils with a plethora of relevant concepts from multiple IT courses taught in different levels of the educational system. This article focuses on the IT Sector of the Technical High School level and the Computer Networking course without being exclusively limited to it. The activities that accompany the proposal are designed with the aim to contribute to the development of a high cognitive level, with respect to the relevant concepts, skills and attitudes. This is attempted by linking these concepts with the daily activities of the modern student-citizen, such as their communication, or more generally their transactions, with other parties.

Keywords: Teaching IT security, asymmetric cryptography, hash function, digital signature, teaching scenarios.