ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΧΡΗΣΤΙΚΟΤΗΤΑ ΜΕΘΟΔΩΝ ΕΛΕΓΧΟΥ ΤΑΥΤΟΤΗΤΑΣ ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ: Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΑΣΦΑΛΟΥΣ ΓΡΗΓΟΡΗΣ ΑΞΙΟΠΙΣΤΗΣ ΣΥΝΔΕΣΗΣ (SQRL).

Η Διπλωματική Εργασία
παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του
Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση
των Απαιτήσεων για το Δίπλωμα του
Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

Κουλουκτσή Αρίσταρχο (ΑΜ:16109)
Μαρνέρα Φώτιο (ΑΜ:16114)
ΣΑΜΟΣ 2018

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ
ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΩΝ : Αριστάρχου Κουλουκτσή, Φώτιου Μαρνέρα

Καρύδα Μαρία, Επιβλέπων, Ημερομηνία : 19 Ιουνίου 2018
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Καμπουράκης Γ. Αναπληρωτής Καθηγητής, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Κοκολάκης Σ., Αναπληρωτής Καθηγητής , Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2018

Περίληψη της Εργασίας

Στη σημερινή σύγχρονη κοινωνία, η ψηφιοποίηση εισχωρεί αποφασιστικά σε όλες τις πλευρές της σύγχρονης κοινωνίας. Ένας από τους βασικούς παράγοντες για τη διατήρηση της ασφάλειας στον σύγχρονο ψηφιακό κόσμο είναι η αυθεντικοποίηση. Με την αυθεντικοποίηση καλύπτονται πολλές και διαφορετικές πτυχές του σύγχρονου ρυθμού ζωής, συμπεριλαμβανομένων των ηλεκτρονικών πληρωμών, επικοινωνιών, κλπ. Αυτή η εργασία αναφέρει την εξέλιξη του τρόπου αυθεντικοποίησης ενός χρήστη, ξεκινώντας από τον έλεγχο ταυτότητας ενός παράγοντα (SFA) και μέσω του ελέγχου ταυτότητας δύο παραγόντων (2FA) καταλήγει στον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA). Συγκεκριμένα, τα MFA αναμένεται να χρησιμοποιηθούν για αλληλεπιδράσεις ανθρώπου με οτιδήποτε, επιτρέποντας ταχεία, εύχρηστη και αξιόπιστη αυθεντικοποίηση κατά την πρόσβαση σε μια υπηρεσία.

Αυτή η εργασία εξετάζει, αναλύει, μελετά και εφαρμόζει την μέθοδο της Ασφαλούς Γρήγορης Αξιόπιστης Σύνδεσης (SQRL) και την εξέλιξη που φέρει όσον αφορά στη σύνδεση και στον έλεγχο ταυτότητας μέσω ενός ιστότοπου, ενώ ταυτόχρονα εξαλείφει πολλά προβλήματα εγγενή στις παραδοσιακές τεχνικές σύνδεσης. Διαπιστώθηκε πως η τεχνολογία του SQRL, κάνοντας χρήση σύγχρονων συσκευών όπως τα Smartphones, παρέχει αρκετά πλεονεκτήματα σε σχέση με τα παραδοσιακά μέσα ελέγχου ταυτότητας. Η ανάλυση αφορούσε την ασφάλεια της αυθεντικότητας, την αλληλεπίδραση με το χρήστη και την προοπτική βελτίωσης του εργαλείου, με κυριότερη αδυναμία τον ανθρώπινο παράγοντα.

Abstract in English

In today's modern society, digitalization decisively penetrates all the sides of the modern society. One of the key enablers to maintain this process secure is authentication. It covers many different areas of a hyper-connected world, including online payments, communications, etc. This work sheds light on the evolution of authentication systems, starting from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA) concludes to Multi-Factor Authentication (MFA). Particularly, MFA is expected to be utilized for human-to-everything interactions by enabling fast, user-friendly, and reliable authentication when accessing a service.

This thesis surveys, analyzes, studies and applies the case of Secure Quick Reliable Login (SQRL) and how it revolutionizes Web site login and authentication, eliminates many problems inherent in traditional login techniques. It has been found that SQRL technology, using modern devices such as Smartphones, offers several advantages over traditional authentication tools. The analysis focused on the security of authentication, the interaction with the user and the prospect of improving the tool, with the human factor being the main weakness.

Πίνακας Περιεχομένων

Κεφάλαιο 1

Ασφάλεια και Αυθεντικοποίηση

1.1 Εισαγωγή - Βασικές Έννοιες

Στη σημερινή σύγχρονη κοινωνία, οι χρήστες θέλουν να έχουν πρόσβαση σε συστήματα (όπως είναι οι πλατφόρμες μέσων δικτύωσης, email, e-banking) και να εκτελούν εργασίες ανεξάρτητα από το χρόνο και την τοποθεσία. Το πρόβλημα που τίθεται είναι πώς μπορεί κανείς να είναι σίγουρος ότι ένα άτομο είναι αυτός που ισχυρίζεται ότι είναι. Καθώς ολοένα και περισσότερες σημαντικές και προσωπικού χαρακτήρα πληροφορίες, διαχειρίζονται ηλεκτρονικά από κατανεμημένα πληροφοριακά συστήματα, οι προσπάθειες για την απόκτηση μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες αυτές καθίστανται πιο διαδεδομένες. Παραδοσιακοί μηχανισμοί ελέγχου ταυτότητας, όπως οι κωδικοί πρόσβασης και τα PIN, είναι αρκετά αδύναμοι μηχανισμοί για τον έλεγχο της πρόσβασης και την αυθεντικοποίηση σε κρίσιμους πόρους, καθώς και τον αποκλεισμό ή μη εξουσιοδοτημένων χρηστών. Αυτό οφείλεται στο γεγονός ότι οι μηχανισμοί που χρησιμοποιούν μόνο ένα παράγοντα, όπως ένας κωδικός πρόσβασης ή ένας κωδικός PIN, είναι όλο και πιο εύκολο να παραβιαστεί. Έχει καταστεί εξαιρετικής σημασίας να εξετάσουμε τη χρήση πολλαπλών μηχανισμών για την ενίσχυση της ασφάλειας. Για παράδειγμα, μια προσπάθεια ελέγχου ταυτότητας που απαιτεί την εισαγωγή ενός κωδικού πρόσβασης μπορεί να απαιτεί και την επαλήθευση μέσω της εισαγωγής κωδικού πρόσβασης μιας χρήσης, που θα αποστέλλεται στο χρήστη στο κινητό του τηλέφωνο. Σκοπός της παρούσας εργασίας η ανάλυση της εξέλιξης των μεθόδων ελέγχου ταυτότητας, από

απλούστερους σε πιο σύνθετους, τα πλεονεκτήματα και τα μειονεκτήματά τους, τις ιδιότητές και τα χαρακτηριστικά τους σε ότι αφορά τους τομείς της ασφάλειας (security) και της χρηστικότητας τους (usability) και το κατά πόσο τελικά καθίσταται εύκολο για τους χρήστες να τα αποδεχτούν και να τα χρησιμοποιήσουν. Τέλος, σε αυτή την εργασία περιγράφεται και αναλύεται και παρουσιάζεται η μέθοδος Ασφαλούς Γρήγορης Αξιόπιστης Σύνδεσης (SQRL) και την εξέλιξη που φέρει όσον αφορά στη σύνδεση και στον έλεγχο ταυτότητας μέσω ενός ιστότοπου, ενώ ταυτόχρονα εξαλείφει πολλά προβλήματα εγγενή στις παραδοσιακές τεχνικές σύνδεσης.

Η φιλοσοφία της ασφάλειας (security) επεκτείνεται σε διάφορα επίπεδα. Με τον ορισμό ασφάλεια αναφερόμαστε τόσο στη φυσική ασφάλεια των μέσων και των χρηστών, όσο και στην ασφάλεια των πληροφοριών, των εφαρμογών, του δικτύου. Οι εταιρείες και τα άτομα επιθυμούν τα δεδομένα και οι προσωπικές τους πληροφορίες να είναι ασφαλή και προσβάσιμα μόνο από εκείνους ή όσους πρέπει να έχουν πρόσβαση σε αυτά. Αναφερόμενοι στην ασφάλεια προσωπικών δεδομένων στο διαδίκτυο και την προστασία της ιδιωτικής ζωής, είναι σημαντικό να καθορίσουμε αν ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Η ασφάλεια στην τεχνολογία της πληροφορικής / Information Technology (IT) ορίζεται ως η υπεράσπιση των ψηφιακών πληροφοριών και των τεχνολογιών πληροφορικής κατά διάφορων εσωτερικών και εξωτερικών, κακόβουλων απειλών. Αυτή η υπεράσπιση περιλαμβάνει την ανίχνευση, την πρόληψη και την αντιμετώπιση απειλών μέσω της χρήσης πολιτικών ασφάλειας, εργαλείων λογισμικού και υπηρεσιών πληροφορικής. Η ασφάλεια αποτελεί κρίσιμο παράγοντα για επιχειρήσεις και οργανισμούς οποιουδήποτε μεγέθους και σε όλων των ειδών τις βιομηχανίες. Μια παρωχημένη πολιτική ασφάλειας μπορεί να οδηγήσει σε παραβίαση συστημάτων και πρόσβαση σε δεδομένα, είτε από έναν κακόβουλο φορέα απειλής είτε από μια ακούσια εσωτερική απειλή. Η μη τήρηση των προτύπων ασφαλείας που ρυθμίζονται από ξεχωριστό οργανισμό ή νόμο, μπορεί επίσης να οδηγήσει σε οικονομικές κυρώσεις.

Η αυθεντικοποίηση (authentication) είναι η διαδικασία δημιουργίας ενός επιπέδου εμπιστοσύνης στην ορθότητα ενός ισχυρισμού [1]. Υπάρχουν δύο είδη αυθεντικοποίησης με βάση τη φύση τους: Η εξακρίβωση της ταυτότητας και η εξακρίβωση της προέλευσης δεδομένων. Η διαδικασία εξακρίβωσης της ταυτότητας ενός χρήστη αποκαλείται αυθεντικοποίηση ταυτότητας. Ενώ η αυθεντικοποίηση της προέλευσης των δεδομένων παρέχει τη διασφάλιση ότι η πηγή ενός μηνύματος είναι αυτή που ισχυρίζεται ότι είναι. Σε γενικές γραμμές, οι τύποι ταυτοποίησης μπορούν να ταξινομηθούν σε:

- κάτι που ο χρήστης γνωρίζει
- κάτι που έχει ο χρήστης
- κάτι που προσδιορίζει ποιος είναι ο χρήστης.
- την τοποθεσία που βρίσκεται χρήστης

Προκειμένου να ελεγχθεί η ασφάλεια της καταχώρησης / αποθήκευσης των προσωπικών δεδομένων σε ένα πληροφοριακό σύστημα (ΠΣ), η αυθεντικοποίηση είναι κρίσιμη. Πολλοί άνθρωποι έχουν πληγεί από άλλους που εισέρχονται στα προσωπικά τους δεδομένα, τις περισσότερες φορές λόγω κακών διαδικασιών αυθεντικοποίησης. Η χρήση της αυθεντικοποίησης γίνεται, όχι μόνο για πρόσβαση στο τηλέφωνό, αλλά για πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου, στα κοινωνικά μέσα, στον υπολογιστή και ακόμη και για τη μεταφορά χρημάτων από τους τραπεζικούς λογαριασμούς. Αυτός είναι ο λόγος για τον οποίο η αυθεντικοποίηση είναι ένα τόσο σημαντικό μέρος της ασφάλειας, έλλειψη της οποίας, οποιοσδήποτε θα έχει πρόσβαση σε οποιοδήποτε τύπο δεδομένων, ανεξάρτητα από το πόσο κρίσιμα ή ευαίσθητα είναι τα δεδομένα.

Με τον όρο αυθεντικοποίηση, αναφερόμαστε στη διαδικασία θετικής επαλήθευσης ταυτότητας χρήστης, είτε αυτός πρόκειται για άτομο, είτε για συσκευή είτε για σύστημα υπολογιστή, που είναι συχνά προαπαιτούμενη, προκειμένου να επιτραπεί η πρόσβαση σε διαθέσιμους πόρους ή υπηρεσίες. Ο μηχανισμός ελέγχου ταυτότητας πραγματοποιεί θετική επαλήθευση, συνδυάζοντας κάποιο κοινό δείκτη ταυτότητας μικρής μορφής που έχει προκαθοριστεί κατά την εγγραφή ή την εγγραφή από το χρήστη. Αυτό γίνεται

με σκοπό την δημιουργία αξιόπιστου δίαυλου επικοινωνίας για εφαρμογές πληροφορικής και τηλεπικοινωνιών.

Η αυθεντικοποίηση, είναι μια διαδικασία όπου ένας χρήστης αναγνωρίζει τον εαυτό του αποστέλλοντας την τιμή x στο σύστημα. το σύστημα επαληθεύει την ταυτότητά του υπολογίζοντας το F(x) και ελέγχοντας ότι ισούται με την αποθηκευμένη τιμή y. Αυτός ο ορισμός δεν έχει αλλάξει σημαντικά με την πάροδο του χρόνου παρά το γεγονός ότι ένας απλός κωδικός πρόσβασης δεν είναι πλέον ο μόνος παράγοντας για την επικύρωση του χρήστη από την άποψη της τεχνολογίας των πληροφοριών

Με τον όρο χρηστικότητα (usability) [2] ενός συστήματος αυθεντικοποίησης, αναφερόμαστε στο βαθμό στον οποίο ένα σύστημα, προϊόν ή υπηρεσία μπορεί να χρησιμοποιηθεί από συγκεκριμένους χρήστες για την επίτευξη συγκεκριμένων στόχων, με αποτελεσματικότητα και ικανοποίηση σε συγκεκριμένο πλαίσιο χρήσης. Η χρηστικότητα αποτελεί στρατηγικό ζήτημα για τη δημιουργία των μεθόδων ελέγχου ταυτότητας χρήστη και αφορά στη μελέτη του τρόπου που θα έπρεπε να υπάρχουν οι πληροφορίες ασφαλείας και να διεκπεραιώνονται στο περιβάλλον χρήστη (user interface) [2] και ταυτόχρονα τον τρόπο με τον οποίο οι μηχανισμοί ασφάλειας και συστημάτων ταυτοποίησης θα πρέπει να είναι εύκολοι στη χρήση.

Η χρηστικότητα και το επίπεδο προστασίας των συστημάτων ασφάλειας των χρηστών αποτελεί ένα σημαντικό θέμα στην έρευνα που αφορά την αποδοτικότητα και την αποδοχή τους από τους ίδιους τους χρήστες. Οι διαδικασίες ελέγχου ταυτότητας πολλαπλών παραγόντων / Multi Factor Authentication (MFA) θεωρούνται πλέον αναγκαίες και απαραίτητες για τον έλεγχο της πρόσβασης σε διάφορους πόρους, υπηρεσίες και εγκαταστάσεις.

Η χρηστικότητα λοιπόν, είναι το μέτρο της δυνατότητας ενός προϊόντος να επιτύχει τους στόχους που θέτει ένας χρήστης. Στην τεχνολογία της πληροφορίας δηλαδή, ο όρος χρησιμοποιείται συχνά σε σχέση με εφαρμογές λογισμικού, τοποθεσίες Web, και υπηρεσίες μέσω δικτύου.

Γενικότερα όμως, μπορεί να χρησιμοποιηθεί σε σχέση με οποιοδήποτε προϊόν που χρησιμοποιείται για την εκτέλεση μιας εργασίας. Η χρηστικότητα είναι μία από τις πτυχές ενός συστήματος, που αφορούν την ποιότητα και αποτελείται από τα ακόλουθα κριτήρια: ικανότητα μάθησης, αποδοτικότητα, αξιοπιστία, λάθη και ικανοποίηση χρήστη και μπορεί να εξεταστεί σε διαφορετικούς τύπους λειτουργίες, από εμπορικές ιστοσελίδες έως συστήματα ηλεκτρονικής μάθησης.

1.2 Είδη / Τύποι Αυθεντικοποίησης

Οι συνήθεις μέθοδοι ελέγχου ταυτότητας έχουν μελετηθεί εκτενώς ανά τα χρόνια προκειμένου να εκτιμηθεί το επίπεδο ασφάλειας που μπορεί να επιτευχθεί μαζί τους.

Διαφορετικές μέθοδοι αυθεντικοποίησης, έχουν πολλές φορές μελετηθεί και αναλυθεί [3], καθώς επίσης και τα πλεονεκτήματα και τα μειονεκτήματα αυτών των μεθόδων. Αρκετές μελέτες έχουν ασχοληθεί με την αποτελεσματικότητα των κωδικών πρόσβασης, την χρήση καρτών ψηφιακής υπογραφής, και η πιθανότητα εφαρμογής της επαλήθευσης ταυτότητας με χρήση βιομετρικών στοιχείων του χρήστη.

Οι έξυπνες κάρτες (smartcards) [4] είναι αρκετά ασφαλείς, όμως εντοπίζονται κάποιες γνωστές ευπάθειες. Ωστόσο, αυτές οι ευπάθειες απαιτούν εκτεταμένη τεχνική εμπειρογνωμοσύνη και πολύ δαπανηρό εξοπλισμό για να αξιοποιηθούν. Οι έξυπνες κάρτες μπορούν να παρέχουν ένα επιπλέον επίπεδο ασφάλειας και να συμβάλλουν στη μείωση των κινδύνων στα υπάρχοντα συστήματα. Έχουν περιγραφεί οι υπάρχουσες απειλές [4] για τις έξυπνες κάρτες και ένα μοντέλο ασφαλείας ενός συστήματος έξυπνων καρτών συζητείται ανεξάρτητα από την εφαρμογή του. Σχεδιάζεται ένα περιβάλλον εμπιστοσύνης καθώς και όλα τα πιθανά μέρη που εμπλέκονται σε οποιοδήποτε σύστημα έξυπνων καρτών: ο κάτοχος κάρτας, ο τερματικός σταθμός, ο κάτοχος δεδομένων, ο εκδότης της κάρτας, ο κατασκευαστής της κάρτας και ο κατασκευαστής του λογισμικού.

Σημαντικά ζητήματα [6] που σχετίζονται με τα ερευνητικά ερωτήματα πάνω στις έξυπνες κάρτες βρίσκονται ακόμα υπο συζήτηση. Αυτά περιλαμβάνουν για παράδειγμα: την ευκολία χρήσης, τη δυνατότητα εφαρμογής, ταχύτητα επαλήθευσης, την ευπάθεια σε απάτες, το μέγεθος αποθήκευσης και πολλαπλές τεχνολογίες επαλήθευσης ταυτότητας. Εξηγώντας με τον τρόπο αυτό, τις βασικές έννοιες της βιομετρικής και των βιομετρικών τεχνολογιών, καθώς και τις εφαρμογές τους στον ηλεκτρονικό κόσμο.

Έχουν επίσης μελετηθεί [7] τα μειονεκτήματα της χρήσης αναγνώρισης προσώπου στα ηλεκτρικά διαβατήρια. Σκοπός των βιομετρικών διαβατηρίων είναι να αποφευχθεί η παράνομη είσοδος ταξιδιωτών σε μια συγκεκριμένη χώρα και να περιοριστεί η χρήση παραποιημένων εγγράφων με ακριβέστερη αναγνώριση ενός ατόμου. Αναφέρεται επίσης ότι υπάρχει μεγάλος κίνδυνος για την κλοπή ταυτότητας όταν γίνεται χρήση μόνο ενός βιομετρικού ελέγχου ταυτότητας σε ένα διαβατήριο. Εξετάζονται [8] πολλές από τις διαθέσιμες μεθόδους ελέγχου της βιομετρικής ταυτότητας και συζητείται η χρηστικότητα και η ασφάλεια τους σύμφωνα με τα δυνατά σημεία, τις αδυναμίες και τις πολιτιστικές ανησυχίες, καταλήγοντας στο συμπέρασμα ότι: "Η βιομετρία προσφέρει τουλάχιστον εν μέρει έναν τρόπο να υπερασπιστεί την τρομοκρατία στον κυβερνοχώρο και να αυξήσει την ασφάλεια του δικτύου".

Τα προβλήματα ταυτοποίησης [9] ερευνήθηκαν με έμφαση στην αβεβαιότητα που σχετίζεται με τις αποφάσεις αυθεντικότητας, καθώς και ότι η εμπειρία είναι απαραίτητη για να προσδιοριστεί με ακρίβεια πώς να υλοποιηθεί καλύτερα η εμπιστευτικότητα της αυθεντικότητας στην πράξη.

Δεδομένου ότι με τους συνηθισμένους τρόπους αυθεντικοποίησης δεν προσφέρεται ικανοποιητική ασφάλεια, έχουν γίνει διάφορες προσπάθειες για τη μελέτη μεθόδων πολλαπλών ελέγχων ταυτότητας. Σε παρελθοντικές μελέτες, αναλύθηκαν και παρουσιάστηκαν, τα πλεονεκτήματα και μειονεκτήματα του συνδυασμού δύο ή περισσότερων μεθόδων αυθεντικοποίησης.

Η ασφάλεια επίσης επηρεάζεται [10] από τον τρόπο με τον οποίο γίνεται ο συνδυάσμός της έξυπνη κάρτας και της βιομετρικής επαλήθευσης, π.χ. δακτυλικών αποτυπωμάτων. Γίνεται σύγκριση επίσης του επιπέδου ασφάλειας που επιτυγχάνεται σε ένα τέτοιο σύστημα με το παραδοσιακό σύστημα ελέγχου ταυτότητας PIN.

Ακόμα, ο συνδυασμός διαφόρων μεθόδων βιομετρικής πιστοποίησης [11] βελτιώνει την ακρίβεια και μειώνει τα ψευδώς θετικά και τα ψευδώς αρνητικά στο επίπεδο που δεν μπορεί να επιτευχθεί με μια βιομετρική λύση ενός μοντέλου. Αναφέρεται ότι μπορούν να χρησιμοποιηθούν δύο τεχνικές για την αύξηση της αξιοπιστίας της βιομετρικής πιστοποίησης: χρησιμοποιώντας πολλαπλά δείγματα και πολλαπλές βιομετρικές πηγές.

Έχει πραγματοποιηθεί ήδη [12] μελέτη και σύγκριση της χρηστικότητας μεταξύ της μεθόδου ελέγχου ταυτότητας με κωδικό πρόσβασης και άλλων μεθόδων ελέγχου ταυτότητας, για παράδειγμα, το Passfaces. Λαμβάνει επίσης υπόψη ότι οι βιομετρικές και άλλες μέθοδοι ελέγχου ταυτότητας που βασίζονται σε συμβολισμούς απαιτούν συχνά ειδικό και ακριβό υλικό.

Η αυθεντικοποίηση με τη χρήση βιομετρικών στοιχείων αξιολογήθηκε [13] και έχει προταθεί μια ταξινόμηση των βιομετρικών συστημάτων ελέγχου ταυτότητας. Αυτή η ταξινόμηση συμβάλλει στη σύγκριση διαφορετικών συστημάτων βιομετρικής πιστοποίησης. Αν αφαιρεθούν τα βιομετρικά χαρακτηριστικά, αυτή η ταξινόμηση θα μπορούσε επίσης να χρησιμοποιηθεί για την αξιολόγηση άλλων συστημάτων πιστοποίησης ταυτότητας. Γίνεται ανάλυση επίσης των πλεονεκτημάτων και των μειονεκτημάτων της βιομετρίας. Συμπεραίνεται ότι ένα σύστημα που περιέχει κρυπτογραφικές λειτουργίες, βιομετρική αντιστοίχιση, εξαγωγή χαρακτηριστικών και βιομετρικό αισθητήρα σε μια συσκευή Tamper Resistant θα ήταν ιδανική. Τα βιομετρικά στοιχεία είναι μια καλή μέθοδος επαλήθευσης ταυτότητας, αλλά όχι βασική. Ακόμη και οι φτηνές και απλές βιομετρικές λύσεις μπορεί να αυξήσουν τη συνολική ασφάλεια του συστήματος όταν συνδυάζονται με μια υπάρχουσα μέθοδο επαλήθευσης ταυτότητας.

Έχει ήδη αναπτυχθεί μία προσέγγιση [14] σε ότι αφορά την αξιολόγηση της ασφάλειας των συστημάτων πληροφορικής που χρησιμοποιούν τρωτά σημεία που εκπροσωπούνται σε ένα γράφημα πλεονεκτημάτων. Το γράφημα αυτό αποτελείται από κόμβους με τόξα, όπου οι κόμβοι είναι συστήματα ή πόροι αλλά και επιτιθέμενοι. Το βάρος κάθε τόξου αντιστοιχεί στην πιθανότητα και σοβαρότητα της επίθεσης. Μια παραβίαση της ασφάλειας μπορεί να συμβεί εάν υπάρχει μια σύγκληση μεταξύ ενός κόμβου που αντιπροσωπεύει έναν πιθανό εισβολέα και με έναν κόμβο που αντιπροσωπεύει έναν επιτιθέμενο.

Από αυτό το παράδειγμα μπορούν να εξαχθούν τρεις ιδιότητες:

1. Η ασφάλεια αυξάνεται εάν αυξάνεται το "μήκος των διαδρομών" που οδηγεί στον στόχο.

2. Η ασφάλεια μειώνεται αν αυξηθεί ο "αριθμός διαδρομών" που οδηγεί στον στόχο.

3. Η ασφάλεια επηρεάζεται κυρίως από τη συντομότερη πορεία που οδηγεί στον στόχο.

Επίσης αναφέρει ότι "η ασφάλεια είναι ανάλογη με το χρόνο που χρειάζεται ένας εισβολέας για να επιτύχει την επίθεσή του".

Η ενσωμάτωση της αναγνώριση φωνής και προσώπου [15], καθώς και το πιθανό όφελος από το συνδυασμό αυτών των τεχνικών με σκοπό τη βελτίωση της ευελιξίας της αναγνώρισης προσώπων. Συμπεραίνεται ότι ο συνδυασμός αυτών των τεχνικών είναι ικανός να ταυτοποιεί πρόσωπα με υψηλή ακρίβεια κάτω από περιορισμένες συνθήκες. Εκτός από την αναγνώριση προσώπου και ομιλίας, το [16] τα συνδυάζει με τις χαρακτηριστικές κινήσεις των χειλιών. Τα αποτελέσματα αυτής της μελέτης δείχνουν ότι η ενσωμάτωση δύο ή τριών τεχνικών οδηγεί σε υψηλότερα ποσοστά αναγνώρισης.

Στην τεχνική της απεικόνισης κατακερματισμού (Hash Visualization) [17] κατά την αυθεντικοποίηση του χρήστη, έχει γίνει περιγραφή ενός πρωτοτύπου όπου ο χρήστης έχει πιστοποιηθεί αναγνωρίζοντας ένα σύνολο εικόνων που έχει δει προηγουμένως. Κατόπιν ανάλυσης της συγκεκριμένης τεχνικής [18,19] εξάγεται το συμπέρασμα πως δεδομένου ότι τα ποσοστά

ανάκτησης σφάλματος ήταν σημαντικά υψηλότερα για τις εικόνες σε σύγκριση με τους κωδικούς πρόσβασης και τα PINS, ένα τέτοιο σύστημα μπορεί να είναι χρήσιμο σε περιβάλλοντα όπου η υψηλή διαθεσιμότητα ενός κωδικού πρόσβασης είναι πρωταρχικής σημασίας και όπου είναι δύσκολη η επικοινωνία των κωδικών πρόσβασης με άλλους.

Σε ότι έχει να κάνει με τις διάφορες μεθόδους ελέγχου ταυτότητας [20] όπως κωδικοί πρόσβασης, tokens και βιομετρική αυθεντικοποίηση, έχουν πραγματοποιηθεί συγκρίσεις όσον αφορά τις αδυναμίες και τα πλεονεκτήματα των διαφόρων στοιχείων ελέγχου ταυτότητας και τα αποτελέσματα δείχνουν πως ότι η ανθρώπινη επαλήθευση ταυτότητας αποτελεί κρίσιμο στοιχείο για την εταιρική ασφάλεια

Οι μελέτες [21] και [22] παρέχουν μια εξαιρετική επισκόπηση των μηχανισμών προσωπικού ελέγχου ταυτότητας, εξετάζοντας βιομετρικά στοιχεία και διαφορετικά χαρακτηριστικά που τα καθιστούν χρήσιμα. Χαρακτηριστικά που αναφέρονται είναι η μοναδικότητα (uniqueness), η καθολικότητα (universality), η μονιμότητα (permanence) , η φιλικότητα προς το χρήστη, το κόστος και η ακρίβεια. Αναφέρονται επίσης στα πλεονεκτήματα και τα προβλήματα της χρήσης της βιομετρικής αναγνώρισης. Ενώ παρέχεται μια επισκόπηση του ελέγχου ταυτότητας και εξετάζεται το πρόβλημα της επαλήθευσης ταυτότητας και του τρόπου με τον οποίο μπορεί να λειτουργήσει σωστά. Αναφέρονται τόσο οι μέθοδοι ελέγχου ταυτότητας όσο και οι ευπάθειες και οι τύποι επιθέσεων.

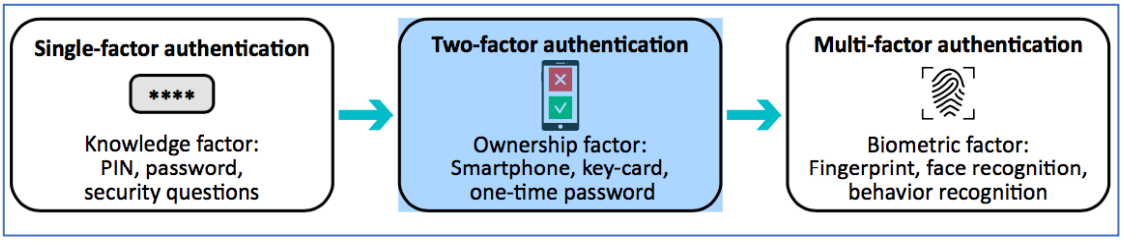
Οι δυνατότητες κάθε μεμονωμένου βιομετρικού στοιχείου εκμεταλλεύτηκαν [23], προκειμένου να ξεπεράσει τόσο την ταχύτητα όσο και τον περιορισμό της ακρίβειας μιας μοναδικής βιομετρίας στην πραγματοποίηση προσωπικής αναγνώρισης. Εξετάστηκαν ορισμένα θέματα που σχετίζονται με το σχεδιασμό ενός πολύτροπου (Multimodal) βιομετρικού συστήματος όπως ο κύριος σκοπός της χρήσης πολλαπλών βιομετρικών στοιχείων, ο τρόπος λειτουργίας, η ενσωμάτωση των βιομετρικών στοιχείων και ο επαρκής αριθμός βιομετρικών στοιχείων.

Η έξυπνη κάρτα (Smart Card) [24] διαδραματίζει σημαντικό ρόλο ως εργαλείο ασφάλειας και παρουσιάζει το πλεονέκτημα της χρήσης ενός βιομετρικού κωδικού πρόσβασης αντί του κωδικού PIN ή μιας γνώσης ως μεθόδου επαλήθευσης. Για να αποκλειστούν οι απειλές ασφάλειας, ο αλγόριθμος βιομετρικής αντιστοίχισης πρέπει να εφαρμοστεί στην έξυπνη κάρτα για να αποφευχθεί η πραγματοποίηση της αντιστοίχισης των δεδομένων σε μια ξεχωριστή συσκευή. Ακόμη και αν ένας εισβολέας κατέχει την έξυπνη κάρτα κάποιου άλλου, ένα τερματικό με τη βιομετρική μονάδα και τα δεδομένα επαλήθευσης του χρήστη, δεν θα μπορεί να παρουσιάσει με επιτυχία τα δεδομένα επαλήθευσης στην έξυπνη κάρτα.

Τέλος, σε προγενέστερες μελέτες [24] έχει αναλυθεί το γεγονός ότι είναι επιθυμητό και εφικτό να εφαρμοστούν αλγόριθμοι αντιστοίχισης σε κάρτες, επιτρέποντας την πραγματοποίηση αυθεντικοποίησης των βιομετρικών στοιχείων του χρήστη στην έξυπνη κάρτα. Εάν για παράδειγμα μια έξυπνη κάρτα παρέχει λειτουργίες όπως η δημιουργία ηλεκτρονικής υπογραφής, ηλεκτρονικό χρήμα καθώς και ιατρικά δεδομένα, τότε η έξυπνη κάρτα πρέπει να επαληθεύει ότι χρησιμοποιείται από τον νόμιμο κάτοχο κάρτας.

Η πορεία της εξέλιξης των μεθόδων αυθεντικοποίησης, υπήρξε καταιγιστική κατά τη διάρκεια των ετών καθώς η ανάγκη εύρεσης πιο περίπλοκων και ταυτόχρονα ασφαλών τρόπων προστασίας των ιδιωτικών δεδομένων γινόταν έντονα επιτακτική λόγω της εξέλιξης των μεθόδων παραβίασης και παράνομης πρόσβασης τρίτων, παρακάμπτοντας τις δικλείδες ασφαλείας των χρηστών.

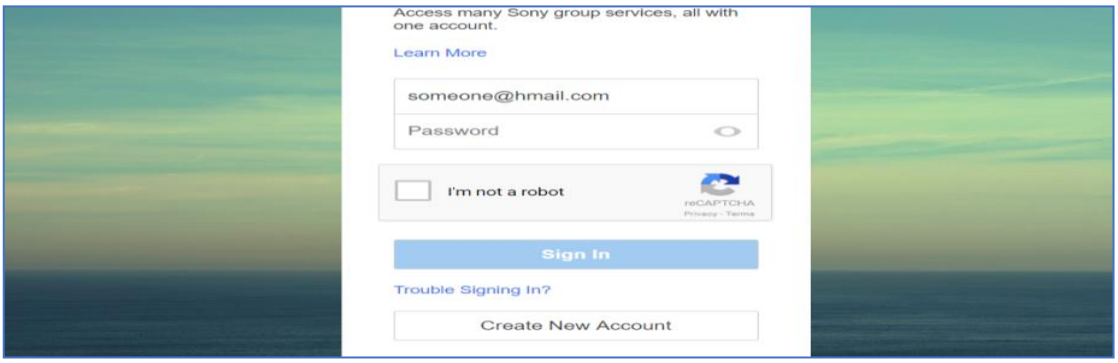
Η εξέλιξη αυτή οδήγησε στη δημιουργία διαφορετικών επιπέδων μεθόδων αυθεντικοποίησης τα οποία διακρίνονται στα ακόλουθα (1.1)



1.1 Εξέλιξη Παραγόντων Αυθεντικοποίησης

SFA (Single Factor Authentication)

Ο έλεγχος ταυτότητας μονού παράγοντα (SFA) είναι μια διαδικασία για την εξασφάλιση πρόσβασης σε ένα σύστημα, όπως ένα δίκτυο ή ένας ιστότοπος, μέσω μιας μόνο κατηγορίας διαπιστευτηρίων. Το πιο κοινό παράδειγμα του SFA είναι ο απλός έλεγχος ταυτότητας με βάση τον κωδικό πρόσβασης (1.2) . Ο οποίος εξαρτάται από τους περιορισμούς και την αυστηρότητα του διαχειριστή συστήματος ή του χρήστη που δημιουργεί το λογαριασμό.



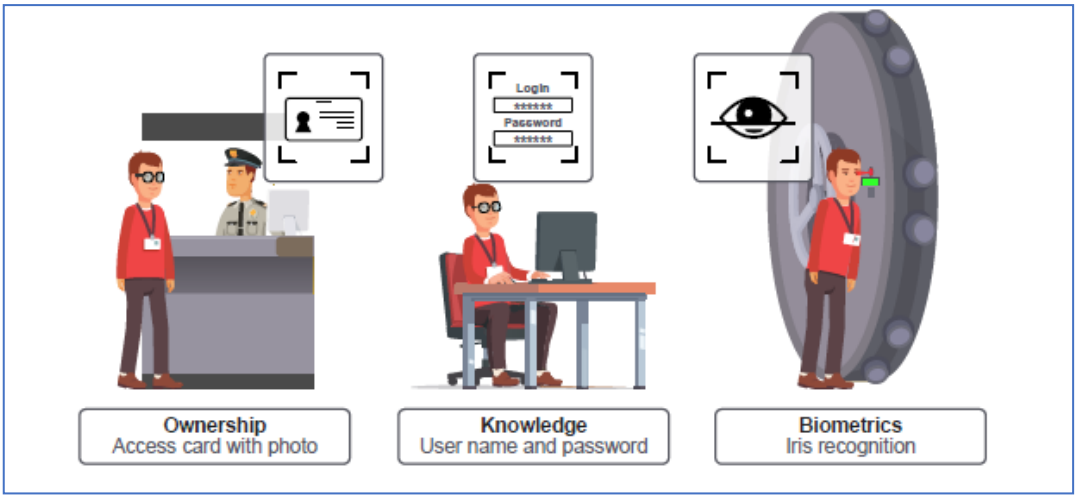
1.2 Τρόπος σύνδεσης με SFA

2FA (Two Factor Authentication)

Ο έλεγχος ταυτότητας δύο παραγόντων χρησιμοποιεί τον ίδιο συνδυασμό κωδικού πρόσβασης / ονόματος χρήστη, επιπρόσθετα όμως ζητείται από τον χρήστη να επαληθεύσει ποιος είναι, χρησιμοποιώντας κάτι μόνο του, όπως μια κινητή συσκευή. Με απλά λόγια: χρησιμοποιεί δύο παράγοντες για να επιβεβαιώσει μια ταυτότητα.

MFA (Multi Factor Authentication)

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) χρησιμοποιεί έναν συνδυασμό των ακόλουθων παραγόντων: κάτι που ο χρήστης γνωρίζει, κάτι που έχει, κάτι που είναι και που βρίσκεται (1.3) . Τα 2FA είναι ένα υποσύνολα των MFA.



1.3 Τρόποι Αυθεντικοποίησης με MFA

1.3 Περιγραφή Προβλήματος

Η ταυτόχρονη ύπαρξη διαφόρων μεθόδων και πρακτικών που συνοδεύονται από διαφορετικά εργαλεία και εφαρμογές καθιστά απαραίτητη την χρήση, την εξέταση, τον έλεγχο και τον τελικό καθορισμό από τους σχεδιαστές και τους διαχειριστές των εργαλείων, προκειμένου να επιλεγεί το φιλικότερο, το πιο εύχρηστο αλλά και το αποτελεσματικότερο για τον απλό χρήστη, με τελικό σκοπό τη μέγιστη προστασία δεδομένων του και την ασφαλή παροχή υπηρεσιών της εκάστοτε εφαρμογής ή εργαλείου.

Η χρηστικότητα των μηχανισμών αυθεντικοποίησης, γίνεται όλο και περισσότερο αναγκαία με το πέρασμα του χρόνου και την ανάπτυξη της τεχνολογίας και αφού οι μηχανισμοί ασφαλείας σχεδιάζονται, εφαρμόζονται, τίθενται σε εφαρμογή και παραβιάζονται από τους ανθρώπους, ο ανθρώπινος παράγοντας θα πρέπει να ληφθεί υπόψη στο σχεδιασμό τους. Η χρηστικότητα αποτελεί στρατηγικό θέμα στην καθιέρωση μεθόδων αυθεντικοποίησης του χρήστη και μπορεί να οριστεί ως ο βαθμός στον οποίο ένα προϊόν μπορεί να χρησιμοποιηθεί από συγκεκριμένους χρήστες για την επίτευξη συγκεκριμένων στόχων με αποτελεσματικότητα, αποδοτικότητα και ικανοποίηση σε ένα συγκεκριμένο πλαίσιο χρήσης.

Η χρηστικότητα της ασφάλειας από την άλλη, αφορά τη μελέτη του τρόπου χειρισμού των πληροφοριών ασφαλείας στο περιβάλλον του χρήστη και τον τρόπο με τον οποίο οι ίδιοι μηχανισμοί ασφαλείας και τα συστήματα αυθεντικοποίησης θα πρέπει να είναι πιο εύχρηστα καθώς και τα ζητήματα ασφάλειας των μεθόδων αυθεντικοποίησης του χρήστη, όσον αφορά την ασφάλεια υπολογιστών αλλά και περιοχών ελέγχου πρόσβασης.

Συνεπώς, στην εργασία αυτή μελετώνται, η εξέλιξη της ασφάλειας και της χρηστικότητας των μηχανισμών αυθεντικοποίησης με το πέρασμα των ετών και ταυτόχρονα η δημιουργία ενός εργαλείου που θα ακολουθεί τις επιταγές της σύγχρονης εποχής σε θέματα ασφαλείας, ενώ θα προσκαλεί το χρήστη να το χρησιμοποιήσει, διατηρώντας τα προσωπικά του δεδομένα ασφαλή. Ο σχεδιασμός λοιπόν χρήσιμων, ελκυστικών και κυρίως φιλικών προς το χρήστη, αλλά ταυτόχρονα ασφαλών εργαλείων αυθεντικοποίησης χρηστών εγείρει κρίσιμα ερωτήματα σχετικά με τον τρόπο επίλυσης των συγκρούσεων μεταξύ στόχων ασφάλειας και χρηστικότητας.

Κεφάλαιο 2
Μέθοδοι Αυθεντικοποίησης

2.1 Σύγκριση μεθόδων Ελέγχου ταυτότητας

Ο έλεγχος ταυτότητας μονού παράγοντα (SFA) είναι μια διαδικασία για την εξασφάλιση πρόσβασης σε ένα σύστημα, όπως ένα δίκτυο, ένας ιστότοπος ή μια εφαρμογή, η οποία αναγνωρίζει και ταυτοποιεί το χρήστη που ζητά πρόσβαση, μέσω μιας μόνο κατηγορίας διαπιστευτηρίων. Το πιο κοινό παράδειγμα αυτού είναι ένας κωδικός πρόσβασης σε σχέση με ένα όνομα χρήστη. Η ασφάλεια που προσδίδει ο κωδικός πρόσβασης βασίζεται στην επιμέλεια του διαχειριστή συστήματος ή του χρήστη που δημιουργεί το λογαριασμό. Οι βέλτιστες πρακτικές περιλαμβάνουν τη δημιουργία ενός ισχυρού κωδικού πρόσβασης και την εξασφάλιση ότι κανείς δεν μπορεί να έχει πρόσβαση σε αυτόν.

Η χρήση του δεύτερου παράγοντα (2FA) βοηθά να διασφαλιστεί ότι, ακόμη και αν ένας εισβολέας κλέψει τον κωδικό πρόσβασης του χρήστη, θα πρέπει να έχει και πρόσβαση στη φυσική συσκευή για να μπει στον λογαριασμό. Η χρήση δύο παραγόντων από την ίδια όμως κατηγορία δεν αποτελεί 2FA. Για παράδειγμα, η απαίτηση ενός κωδικού πρόσβασης και ενός κοινού μυστικού εξακολουθεί να θεωρείται ταυτότητα μονού παράγοντα, καθώς και οι δύο ανήκουν στον ίδιο παράγοντα επαλήθευσης ταυτότητας - γνώσης. Υπάρχουν πολλές διαφορετικές συσκευές και υπηρεσίες για την εφαρμογή του 2FA - από tokens , κάρτες RFID έως εφαρμογές για Smartphones.

Τα προϊόντα επαλήθευσης δύο παραγόντων μπορούν να χωριστούν σε δύο μέρη: σε tokens που δίδονται στους χρήστες για χρήση όταν συνδέονται, και υποδομή ή λογισμικό που τα αναγνωρίζει και επικυρώνει την πρόσβαση στους χρήστες. Τα tokens, ενδέχεται να είναι φυσικές συσκευές, όπως κλειδιά

fob ή έξυπνες κάρτες, ή ενδέχεται να υπάρχουν ως λογισμικό σαν εφαρμογές για κινητά ή για υπολογιστές που παράγουν κωδικούς PIN για έλεγχο ταυτότητας.

Τέλος ο σκοπός του ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) είναι να παρέχει υψηλότερο βαθμό αυθεντικοποίησης της ταυτότητας του ατόμου που προσπαθεί να αποκτήσει πρόσβαση σε έναν πόρο, όπως φυσική τοποθεσία, υπολογιστική συσκευή, δίκτυο ή βάση δεδομένων. Τα MFA δημιουργούν έναν μηχανισμό πολλαπλών επιπέδων που ένας μη εξουσιοδοτημένος χρήστης θα πρέπει να ξεπεράσει για να αποκτήσει πρόσβαση.

Η συνολική διαδικασία ελέγχου ταυτότητας για τα MFA απαιτεί τουλάχιστον δύο από τις τρεις μεθόδους πιστοποίησης / αυθεντικοποίησης, όπως περιγράφονται παρακάτω :

α) Κάτι που ο χρήστης γνωρίζει, όπως ένας κωδικός πρόσβασης ή μια φράση. Αυτή η μέθοδος περιλαμβάνει την επαλήθευση των πληροφοριών που παρέχει ένας χρήστης, όπως ένας κωδικός πρόσβασης / φράση, ο κωδικός PIN ή οι απαντήσεις σε μυστικές ερωτήσεις (πρόκληση-απόκριση).

β) Κάτι που ο χρήστης έχει, όπως ένα token ή μια έξυπνη κάρτα. Αυτή η μέθοδος περιλαμβάνει την επαλήθευση ενός συγκεκριμένου στοιχείου που έχει ο κάτοχός του, όπως ένα φυσικό ή λογικό σύμβολο ασφαλείας, έναν κωδικό μιας χρήσης / One Time Password (OTP), ένα key fob, μια κάρτα πρόσβασης των εργαζομένων ή μια κάρτα SIM του τηλεφώνου. Για τον έλεγχο ταυτότητας μέσω κινητού, ένα smartphone συχνά κάνει χρήση του παράγοντα κατοχής σε συνδυασμό με μια εφαρμογή OTP ή ένα κρυπτογραφικό υλικό (δηλ. πιστοποιητικό ή κλειδί) που είναι εγκατεστημένο στη συσκευή.

γ) Κάτι που ο χρήστης είναι, όπως ένα βιομετρικό στοιχείο. Αυτή η μέθοδος περιλαμβάνει την επαλήθευση χαρακτηριστικών εγγενών στο άτομο, όπως η σάρωση του αμφιβληστροειδούς, σάρωση ίριδας, σάρωση δακτυλικών αποτυπωμάτων, σάρωση φλεβών δαχτύλων, αναγνώριση

προσώπου, αναγνώριση φωνής, γεωμετρία χεριών, ακόμη και γεωμετρία λοβού.

δ) Τέλος είναι και η διαδικασία αυθεντικοποίησης του χρήστη βάση της τοποθεσία στην οποία βρίσκεται, ελέγχοντας το κατα πόσο έγκυρη είναι αυτή η τοποθεσία κατά την διαδικασία αυθεντικοποίησης [25].

Εν κατακλείδι, με βάση τις παραπάνω κατηγορίες που περιγράφηκαν, ο έλεγχος ταυτότητας ενός παράγοντα (SFA) απαιτεί διαπιστευτήρια μόνο από μία από αυτές τις κατηγορίες. Εν τω μεταξύ, ο έλεγχος ταυτότητας δύο παραγόντων (2FA) περιλαμβάνει δύο από τις κατηγορίες και, τέλος, ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) απαιτεί διαπιστευτήρια από τουλάχιστον δύο ή περισσότερες κατηγορίες.

2.2 Μειονεκτήματα και αδυναμίες (SFA,2FA,MFA)

Ωστόσο, υπάρχουν μειονεκτήματα και στις τρεις μεθόδους. Όσον αφορά το SFA, η μέθοδος αυτή αποτελεί το πιο αδύναμο επίπεδο ταυτοποίησης.Στα μειονεκτήματα των SFA το βασικότερο είναι το πόσο εύκολο είναι να τα σπάσουν. Είναι σύντομοι και βασίζονται σε προσωπικές πληροφορίες του χρήστη, όπως τα γενέθλια, τα ονόματα των παιδιών, κ.λπ. και είναι τυπικά μόνο γράμματα ή μόνο αριθμοί. Ένας μη εξουσιοδοτημένος χρήστης μπορεί να προσπαθήσει να αποκτήσει πρόσβαση χρησιμοποιώντας brute-force ή dictionary επιθέσεις, rainbow tables ή τεχνικές social engineering (δηλαδή ανθρώποι που ζητούν τον κωδικό πρόσβασης ή προσπαθούν να τον μαντέψουν), καθώς επίσης με την χρήση spyware. Επιπλέον όταν οι χρήστες χρησιμοποιούν λάθος κωδικό πρόσβασης, τα συστήματα δίνουν την επιλογή στο χρήστη να κάνει χρήση των ερωτήσεων ασφαλείας, όπως "ποιο είναι το πατρικό όνομα της μητέρας σας;" - πληροφορίες που είναι αρκετά εύκολο για τους hackers να ανακαλύψουν και να εκμεταλλευτούν κυρίως εξαιτίας των κοινωνικών μέσων δικτύωσης.

Η εναλλακτική μέθοδος διαχείρισης κωδικών πρόσβασης είναι η τακτική αλλαγή των κωδικών πρόσβασης. Αυτό έχει ως πλεονέκτημα ότι είναι πιο ασφαλές από τους στατικούς κωδικούς πρόσβασης αλλά ένα βασικό

μειονέκτημα των συχνά μεταβαλλόμενων κωδικών πρόσβασης είναι ότι μπορούν εύκολα να ξεχαστούν, οδηγώντας σε πολύ υψηλό κόστος υποστήριξης. Συνήθως, η ελάχιστη απαίτηση πολυπλοκότητας κωδικού πρόσβασης πρέπει να λαμβάνεται υπόψη κατά τη χρήση αυτού του τύπου πιστοποίησης

Στα 2FA, βασικά μειονεκτήματα είναι το κόστος αγοράς, έκδοσης και διαχείρισης των tokens ή των καρτών. Κάνοντας ένας χρήστης, χρήση περισσότερων από έναν μεθόδων, απαιτεί τη μεταφορά πολλαπλών tokens / καρτών που πιθανόν να χαθούν ή να κλαπούν. Η πιο συνηθισμένη μέθοδος 2FA βασίζεται σε κώδικες ασφαλείας που αποστέλλονται μέσω SMS ή τηλεφωνικών κλήσεων για τον έλεγχο ταυτότητας χρηστών. Ενώ αυτό μπορεί να είναι απλό και εύχρηστο, δημιουργεί ένα ψεύτικο αίσθημα ασφάλειας, καθώς οι σημερινοί εισβολείς (hackers) έχουν πολλούς τρόπους για να παρακάμψουν το αναγνωριστικό της συσκευής, τη γεω-τοποθεσία και άλλα στατικά μέσα πιστοποίησης.

Ένα άλλο ζήτημα με το 2FA είναι η τυποποιημένη διαδικασία για την αυθεντικοποίηση της ταυτότητας του χρήστη. Αυτό συμβαίνει εξαιτίας της διαλειτουργικότητα μεταξύ των εκάστοτε εργαλείων και δεδομένου ότι υπάρχουν διάφορες εφαρμογές, συνιστάται να λαμβάνεται υπόψη κατά τη συλλογή, δοκιμή, εφαρμογή και συντήρηση, όταν πρόκειται για ένα ασφαλές σύστημα ελέγχου ταυτότητας end to end.

Όπως αναφέρθηκε, το πρώτο και πιο προφανές ζήτημα που συνδέεται με τη χρήση των 2FA είναι το κόστος. Το κόστος δεν σημαίνει μόνο την αγορά του λογισμικού και του υλικού, αλλά και το κόστος της συντήρησης αλλά και εκπαίδευσης – ενημέρωσης των ανθρώπων / χρηστών για τη χρήση του συστήματος. Ομοίως, πολλά 2FA έχουν ένα τακτικό κόστος συντήρησης. Για παράδειγμα, το σύστημα RSA SecurID χρησιμοποιεί μια συσκευή κλειδιού που παράγει τακτικά κρυφά ψηφία για χρήση από τον ιδιοκτήτη. Οι συσκευές έχουν σχεδιαστεί μόνο για να διαρκέσουν ένα πεπερασμένο χρονικό διάστημα (συνήθως μερικά χρόνια), γεγονός που ενισχύει την ασφάλεια - αλλά ο

χρήστης θα αναγκαστεί να ξοδέψει αρκετά χρήματα σε μια τακτική βάση για την αντικατάστασή τους.

Με τα 2FA τέλος να πρέπει να ληφθεί υπόψη το γεγονός ότι το σύστημα θα χαλάσει κάποια στιγμή και μερικά σενάρια οπου τα 2FA δεν λειτουργούν σωστά, είτε λόγω ανθρώπινου παράγοντα αλλά είτε και εξαιτίας των εταιριών και του τρόπου αυθεντικοποίησης που χρησιμοποιούν είναι τα κάτωθι:

Η χρήση υπηρεσιών από τρίτους ή εξωτερικούς συνεργάτες (είτε παρόχων υπηρεσιών ελέγχου ταυτότητας είτε εταιρειών τηλεπικοινωνιών) είναι ευρέως διαδεδομένη και συνεπώς στόχος για τους χακερς. Μια πρόσφατη έρευνα της Soha Systems μέσω της MarketWired [27] αναφέρει ότι το 63% όλων των παραβιάσεων και υποκλοπών δεδομένων μπορεί να αποδοθεί στους εξωτερικούς συνεργάτες. Οι επιχειρήσεις δίνουν πρόσβαση στα πιο ευαίσθητα δεδομένα τους με περιορισμένη γνώση των πολιτικών ασφάλειας τους και της αξιοπιστίας των υπαλλήλων τους.

Τα 2FA, όπως και τα SFA, είναι επίσης επιρρεπή στο phishing. Εάν ένας hacker αποκτήσει στα χέρια του έναν κωδικό πρόσβασης και έναν έγκυρο 2FA pin ενός ανυποψίαστου θύματος, μπορεί να συνδεθεί στο λογαριασμό του και να δημιουργήσουν έναν άλλο κωδικό πρόσβασης για να χρησιμοποιηθεί ως backdoor.

Τα τηλέφωνα, στα οποία έχει εγκατασταθεί κακόβουλο λογισμικό (malware) ανακατευθύνουν μηνύματα SMS που περιέχουν έναν κωδικό επαλήθευσης και τα στέλνουν στον hacker χωρίς την γνώση του χρήστη. Επιπλέον υπάρχει μια επιλογή για λήψη κωδικών 2FA μέσω τηλεφωνικής κλήσης. Η τηλεφωνική κλήση μπορεί ενδεχομένως να μεταβεί στον τηλεφωνητή, συσκευή που δεν προσφέρει καθόλου ασφάλεια.

Όπως αναφέρθηκε και προγενέστερα, η ανάκτηση λογαριασμού μέσω της επαναφοράς τον τρέχων κωδικού πρόσβασης, στέλνει ένα προσωρινό μήνυμα, ώστε να μπορεί ο χρήστης να συνδεθεί ξανά. Σε ορισμένες περιπτώσεις, η ανάκτηση λογαριασμού παρακάμπτει το 2FA

απενεργοποιώντας το. Στη συνέχεια, οι hackers μπορούν να συνδεθούν ξανά στο λογαριασμό χωρίς 2FA, καθιστώντας τη δουλειά τους πολύ ευκολότερη.

Τέλος στα MFA, επί του παρόντος, μία από τις κύριες προκλήσεις – αδυναμίες τους είναι η έλλειψη συσχέτισης μεταξύ της ταυτότητας του χρήστη και των ταυτοτήτων των έξυπνων αισθητήρων της ηλεκτρονικής συσκευής / συστήματος. Όσον αφορά την ασφάλεια, πρέπει να οριστεί με τέτοιο τρόπο έτσι ώστε μόνο ο νόμιμος χρήστης, π.χ. αυτός του οποίου η ταυτότητα είναι πιστοποιημένη εκ των προτέρων, να αποκτήσει τα δικαιώματα πρόσβασης. Ταυτόχρονα, η διαδικασία αυθεντικοποίησης μέσω των MFA, θα πρέπει να είναι όσο το δυνατόν πιο φιλική προς το χρήστη

2.3 Συνολική Αξιολόγηση Τρόπων Αυθεντικοποίησης

Σε αυτή τη εργασία αναφέρθηκαν διαφορετικά συστήματα αυθεντικοποίησης. Από αυτό προκύπτει ότι, κατά την διαδικασία επαλήθευσης του χρήστη, υπάρχουν πολλές προσεγγίσεις (τόσο για κινητές όσο και για σταθερές συσκευές). Μπορεί να αναφερθεί ότι δεν υπάρχει μοναδική λύση κατάλληλη για κάθε κατάσταση και μπορεί να επισημανθεί ότι για να επιλεγεί μια μέθοδος ελέγχου ταυτότητας, πρέπει να ληφθούν υπόψη διάφοροι παράγοντες όπως η χρηστικότητα του εκάστοτε εργαλείου, η ασφάλεια, η συγκεκριμένη λειτουργικότητα της εφαρμογής / υπηρεσίας, η ιδιωτικότητα, οι απαιτήσεις των χρηστών. Επομένως, η εξεύρεση της σωστής ισορροπίας μεταξύ αυτών των παραγόντων και η επιλογή μιας τεχνικής ελέγχου ταυτότητας που είναι κατάλληλη για τη συγκεκριμένη υπηρεσία και αποδεκτή από τους χρήστες είναι το πιο δύσκολο ζήτημα. Ο σημερινός παραδοσιακός έλεγχος βασισμένος στον κωδικό πρόσβασης δεν θεωρείται πλέον ασφαλής στο Διαδίκτυο, ειδικά στις υπηρεσίες δικτύου. Δεδομένου ότι μπορούν εύκολα να μαντευθούν. Προκειμένου να ικανοποιηθούν οι απαιτήσεις των οργανισμών και να ενισχυθεί η αυθεντικότητα, έχουν εισαχθεί τα 2FA και MFA.

Πιο συγκεκριμένα, τα MFA λειτουργούν ως μια προσέγγιση στην αυθεντικοποίηση της ταυτότητας ενός χρήστη, που απαιτεί την παρουσίαση

δύο ή περισσότερων παραγόντων επαλήθευσης όπως ο συνδυασμός ενός παράγοντα γνώσης ("κάτι που γνωρίζει μόνο ο χρήστης"), ενός παράγοντα κατοχής ("κάτι που έχει μόνο ο χρήστης") και ενός προσωπικου παράγοντα ("κάτι που είναι μόνο ο χρήστης"). Επιπλέον, ειδικά στα χρηματοπιστωτικά ιδρύματα, τα MFA χαρακτηρίζονται από τη χρήση διαφορετικών ελέγχων σε διαφορετικά σημεία κατά την διαδικασίας μιας συναλλαγής. Έτσι ώστε η αδυναμία ενός ελέγχου να μπορεί γενικά να αντισταθμίζεται από τη δύναμη ενός άλλου [28]. Ως εκ τούτου, τα MFA μπορούν να ενισχύσουν σημαντικά τη συνολική ασφάλεια των υπηρεσιών που βασίζονται στο Διαδίκτυο, προστατεύοντας αποτελεσματικά τις ευαίσθητες πληροφορίες πελατών, εμποδίζοντας την κλοπή ταυτότητας και μειώνοντας την κατάχρηση ξένων λογαριασμών και τις οικονομικές απώλειες που προκύπτουν.

Γενικά, τα MFA θα μπορούσαν να χωριστούν σε τρεις ομάδες ανάλογα με την εφαρμογή τους:

(i) εμπορικές εφαρμογές [29,30], δηλ. Σύνδεση λογαριασμού, ηλεκτρονικό εμπόριο, ATM, έλεγχος φυσικής πρόσβασης κ.λπ.

(ii) κυβερνητικές εφαρμογές [31,32], δηλ. έγγραφα ταυτότητας, κυβερνητική ταυτότητα, διαβατήριο, άδεια οδήγησης, κοινωνική ασφάλιση, συνοριακός έλεγχος κλπ. και

(iii) εγκληματολογικές εφαρμογές [33,34], δηλαδή, ποινική έρευνα, εξαφανισμένα παιδιά, ταυτοποίηση πτώματος κλπ.

Γενικά, ο αριθμός των σεναρίων που σχετίζονται με την αυθεντικοποίηση είναι πράγματι μεγάλος. Σήμερα, τα MFA αποτελούν εξαιρετικά κρίσιμο παράγοντα για την επαλήθευση της ταυτότητας του χρήστη και της ηλεκτρονικής συσκευής (ή του συστήματος) [35], την επικύρωση της σύνδεσης υποδομής (infrastructure connection)[36] και τέλος την επαλήθευση των διασυνδεδεμένων συσκευών, όπως ένα smartphone, tablet, φορητή συσκευή ή οποιοδήποτε άλλο ψηφιακό διακριτικό (key dongle).

Σε αντίθεση με το SFA που περιλαμβάνει μόνο αναγνωριστικό χρήστη και κωδικό πρόσβασης, τα 2FA που απαιτούν ένα πρόσθετο στοιχείο όπως τα token. Τα MFA περιλαμβάνουν και βιομετρικά στοιχεία, όπως αναγνώριση

δακτυλικών αποτυπωμάτων, αναγνώριση προσώπου και ίριδας, τα οποία καθιστούν τη διαδικασία αυθεντικοποίησης ισχυρότερη και δύσκολη στο να παραβιαστεί η ασφάλειά τους. Τα MFA περιλαμβάνουν 3 βήματα πιστοποίησης που ομαδοποιούνται σε δύο στάδια. Το πρώτο βήμα απαιτεί από τον χρήστη να εισαγάγει το αναγνωριστικό του. Στη συνέχεια, ζητείται από τον χρήστη να επιβεβαιώσει την εικόνα ασφαλούς πρόσβασής του, την οποία επέλεξε κατά τη διάρκεια της εγγραφής του και μήνυμα για σύνδεση. Και τελικά υποχρεούται να παρέχει τον κωδικό πρόσβασης. Στη σημερινή εποχή η χρήση των MFA γίνεται όλο και πιο συχνή και είναι πολύ δύσκολο να παραβιαστούν. Οι παραπάνω τεχνικές επαλήθευσης έχουν εφαρμοστεί, δοκιμαστεί και γίνει ευρέως αποδεκτές και έχουν αποδειχθεί ισχυρές και ασφαλείς.

Κεφάλαιο 3

Χρηστικότητα

3.1 Χρηστικότητα των μεθόδων αυθεντικοποίησης MFA

Η ασφάλεια (Security) και η χρηστικότητα (Usability) αποτελούν βασικές αρχές στη πραγματοποίηση της διαδικασίας ελέγχου ταυτότητας. Ωστόσο, οι ολοένα αυξανόμενες απαιτήσεις σε ότι αφορά το ζητούμενο ενός υψηλού επίπεδου ασφάλειας, ταυτόχρονα με την απαίτηση για τη διατήρηση της χρηστικότητας της εφαρμογής κατά την διεπαφή με τους χρήστες, έρχονται συχνά σε αντίθεση μεταξύ τους. Το ιδανικό σενάριο, περιλαμβάνει την εξεύρεση μιας λύσης στην οποία να διατηρείται η ισορροπία μεταξύ ασφάλειας – χρηστικότητας την ίδια στιγμή.

Θα πρέπει αρχικά να ληφθεί υπόψη το γεγονός ότι η επαλήθευση ταυτότητας (Authentication) είναι μια πολύπλοκη ιδέα και την ίδια στιγμή, τα στοιχεία σχετικά με τον μηχανισμό ελέγχου ταυτότητας θα πρέπει να παρουσιάζονται με συνοπτικό και κατανοητό τρόπο στους χρήστες. Ένας τυπικός καθημερινός χρήστης δεν έχει εξεζητημένες γνώσεις ασφάλειας και το περιβάλλον διεπαφής του χρήστη, όπως π.χ. το πρόγραμμα περιήγησης στο Web, έχει σχεδιαστεί προκειμένου να αποκρύψει τους μηχανισμούς ελέγχου ταυτότητας και να παρέχει τα ελάχιστα στοιχεία για το τι συμβαίνει κάθε φορά στο υπόβαθρο. Αυτό το γεγονός πιθανώς να αποτελεί μια “σωστή” διαδικασία, όσον αφορά τη γενική φιλοσοφία της χρηστικότητας προς τους χρήστες, αφού δίνει τη δυνατότητα στους τελευταίους να δώσουν βάση και να ασχοληθούν κυρίως με τη διεργασία που επιθυμούν να εκτελέσουν.

Την ίδια στιγμή όμως εντοπίζονται αδυναμίες και αντιθέσεις με τη φιλοσοφία της ουσιαστικής και επαρκούς εξακρίβωσης ταυτότητας. Το εκάστοτε σύστημα δεν είναι σε θέση να γνωρίζει το όνομα της οντότητας με την οποία ο χρήστης θέλει τελικά να επικοινωνήσει και συνεπώς δεν είναι σε

θέση να κρίνει ως προς τα αποτελέσματα της απεικονιζόμενης διαδικασίας επαλήθευσης ταυτότητας. Μια κοινή φιλοσοφία σχεδιασμού των συστημάτων αυθεντικοποίησης βέβαια είναι να καταστήσει την διαδικασία εξακρίβωσης της γνησιότητας της ταυτότητας χρήστη όσο το δυνατόν πιο διαφανή, προκειμένου να μειωθεί η πνευματική επιβάρυνση του χρήστη και ως εκ τούτου χαρακτηρίσει το σύστημα ως δύσχρηστο. Ο έλεγχος ταυτότητας μπορεί να εφαρμοστεί χρησιμοποιώντας διάφορους μηχανισμούς και αν οι αυτοί παραμένουν εντελώς κρυφοί από τον χρήστη, τότε αυτός δεν θα ήταν σε θέση να συμπεράνει εάν τελικά είναι αποτελεσματικοί ή όχι. Αυτό προφανώς επιτρέπει ώστε να παραμείνουν αδιευκρίνιστες οι επιτυχείς επιθέσεις και κατ' αυτόν τον τρόπο τελικά να καθίσταται το σύστημα ανασφαλές.

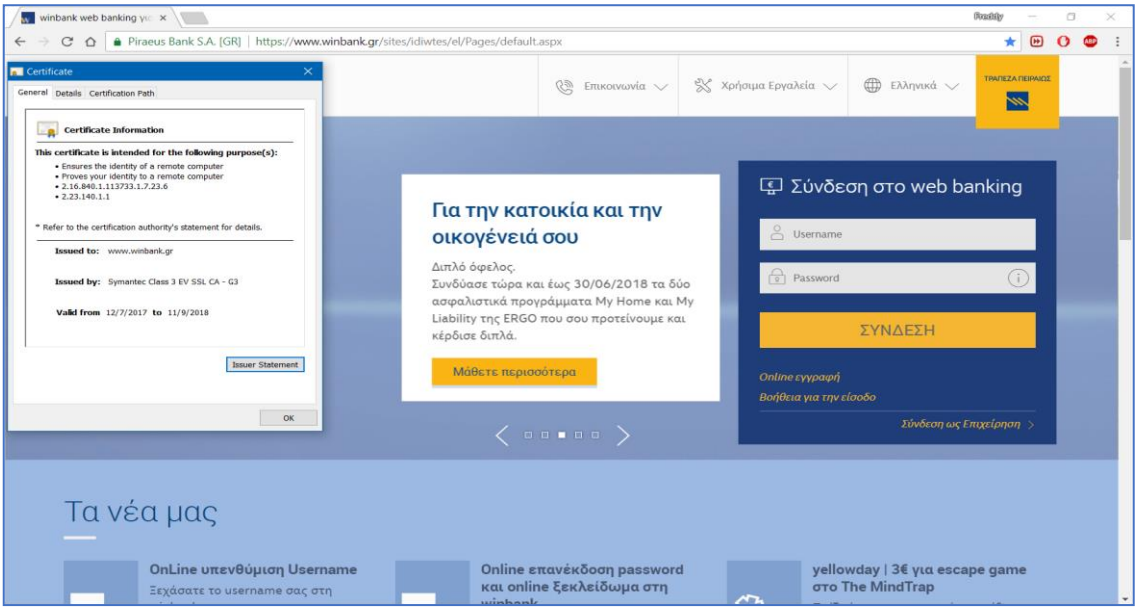
Ταυτόχρονα, η δυνατότητα του ανθρώπου να δώσει προσοχή σε πολλές διαφορετικές διαδικασίες και συμβάντα την ίδια στιγμή είναι περιορισμένη και εάν παρουσιαστούν πάρα πολλά στοιχεία στο ίδιο χρονικό πλαίσιο, στις περισσότερες περιπτώσεις είτε θα συγχυστεί είτε απλά θα αποσυντονιστεί. Κάτι τέτοιο θα μπορούσε να επιτρέψει στην ύπαρξη διάφορων αποτυχημένων προσπαθειών ελέγχου ταυτότητας, ακόμη και αν έχουν παρουσιαστεί στο χρήστη στοιχεία για την συγκεκριμένη αποτυχία. Το γεγονός αυτό δημιουργεί το εξής δίλημμα στους προγραμματιστές: Πολλές πληροφορίες την ίδια στιγμή είναι πιθανό να δημιουργήσουν τα ίδια προβλήματα όσα και οι ελάχιστες πληροφορίες. Προφανώς δεν μπορεί να υπάρχουν περισσότερα δεδομένα απ' ότι ο χρήστης μπορεί να καταλάβει και να χειριστεί, αλλά ταυτόχρονα θα πρέπει να είναι επαρκής για το απαιτούμενο επίπεδο ασφάλειας της εφαρμογής. Η πρόκληση είναι να επιλεγούν τα καταλληλότερα στοιχεία και να τα παρουσιαστούν με τρόπο κατανοητό στον χρήστη.

3.2 Πρότυπα χρηστικότητας αυθεντικοποίησης

Οι δυνητικές συγκρούσεις μεταξύ ασφάλειας και χρηστικότητας, υπάρχει πιθανότητα να ελαχιστοποιηθούν χρησιμοποιώντας κάποιες γενικές

αρχές σχεδίασης όπως η ελαχιστοποίηση προσπάθειας της εισόδου του χρήστη, λήψη αποφάσεων στο όνομα του χρήστη, ενημέρωση του χρήστη για τις ενέργειες που έγιναν για λογαριασμό του και δυνατότητα ο χρήστης τη να αναιρέσει αυτές τις ενέργειες όταν είναι δυνατόν και αν όχι να ελαχιστοποιήσει τον αντίκτυπό τους.

Ωστόσο είναι σημαντικό να ληφθεί σοβαρά υπόψη πως δεν υπάρχει καθορισμένη και αναγνωρισμένη αρχή χρηστικότητας και πρότυπα για τις μεθόδους ελέγχου ταυτότητας. Ένα χαρακτηριστικό παράδειγμα που απεικονίζει τις λεπτές διαχωριστικές γραμμές μεταξύ της χρηστικότητας και ταυτόχρονα της ασφάλειας των μέσων αυθεντικοποίησης είναι το εικονίδιο λουκέτου στα προγράμματα περιήγησης στο Web. Ένα ανοικτό λουκέτο, εύκολο να το διακρίνει ο χρήστης και να καταλάβει πως η ασφάλεια επικοινωνίας δεν είναι εγγυημένη, ενώ ένα κλειστό λουκέτο δείχνει ασφαλή επικοινωνία με το χρήστη να νιώθει πως μπορεί να εκτελέσει οποιαδήποτε ενέργεια σε ασφαλείς συνθήκες. Αυτός είναι φαινομενικά ένας διακριτός τρόπος υπολογισμού του γεγονότος ότι ένας διακομιστής Web έχει πιστοποιηθεί με SSL και ότι τα διαβιβαζόμενα και τα ληφθέντα δεδομένα κρυπτογραφούνται (3.1) .



3.1 Σύνδεση χρήστη σε τραπεζικό λογαριασμό σε ιστότοπο με HTTPS

Ωστόσο, ένα κλειστό λουκέτο λέει μόνο στο χρήστη ότι κάποιος διακομιστής Web έχει πιστοποιηθεί αλλά όχι ποιος διακομιστής Web ειδικότερα. Εφόσον ο χρήστης δεν κάνει τα επιπλέον κλικ του ποντικιού για να δει το πιστοποιητικό διακομιστή, αυτός ή αυτή στην πραγματικότητα δεν έχει πιστοποιήσει τίποτα καθόλου. Παρά την καθησυχαστική εμφάνισή του, το λουκέτο αποκρύπτει κρίσιμες πτυχές της ασφάλειας, οι οποίες απαιτούνται για την ουσιαστική εξακρίβωση της ταυτότητας.

Η χρηστικότητα λοιπόν ενός συστήματος ελέγχου ταυτότητας συνδέεται στενά με την ταχύτητα και την ακρίβεια. Εάν το σύστημα ελέγχου ταυτότητας είναι πολύ αργό στη διαδικασία αξιολόγησης και επαλήθευσης του χρήστη, δεν θα είναι επιτυχής. Η αποδοχή από τους χρήστες είναι μια κρίσιμη πτυχή για την υιοθέτηση ισχυρών συστημάτων επαλήθευσης ταυτότητας και πολλαπλών παραγόντων. Καθώς εφαρμόζονται και αναπτύσσονται νέα συστήματα MFA, είναι σημαντικό να υιοθετηθεί από τους προγραμματιστές μια προσεκτική και ενδελεχής προσέγγιση με σκοπό την σταδιακή αποδοχή τους από τους χρήστες. Οι κύριες προκλήσεις χρηστικότητας που προκύπτουν στη διαδικασία επαλήθευσης ταυτότητας μπορούν να χαρακτηριστούν από τρεις προοπτικές [37]:

- Αποδοτικότητα του συστήματος - Ο χρόνος που απαιτείται για εγγραφή και επαλήθευση της ταυτότητας.
- Αποτελεσματικότητα του συστήματος - Ο αριθμός προσπαθειών που απαιτείται για είσοδο στο σύστημα.
- Προτιμήσεις χρήστη - αν ο χρήστης προτιμά ένα συγκεκριμένο σχήμα ελέγχου ταυτότητας σε σχέση με ένα άλλο.

Οι ερευνητές έχουν ήδη ξεκινήσει έρευνα για πιο συγκεκριμένες επιδράσεις στις διαδικασίες επαλήθευσης ταυτότητας βασισμένες σε διάφορους ανθρώπινους παράγοντες που προέκυψαν από προηγούμενες μελέτες. Οι συγγραφείς της έρευνας [37] παρείχαν μια μελέτη βασιζόμενοι και σε προηγούμενες, όσον αφορά την επιρροή που έχουν στην χρηστικότητα και αποδοτικότητα ενός συστήματος οι διαφορετικές ιδιότητες των χρηστών. Από

αυτή προκύπτει τελικά πως οι νεότερες γενιές χρηστών είναι ικανοί να αφιερώσουν 50% λιγότερο χρόνο προκειμένου να εκτελέσουν τον έλεγχο ταυτότητας. Την ίδια στιγμή το φύλο φαίνεται πως δεν επηρεάζει τα αποτελέσματα των μηχανισμών ελέγχου ταυτότητας, ενώ μια άλλη κατεύθυνση στο βαθμό χρηστικότητας των μηχανισμών ελέγχου ταυτότητας σχετίζεται με τις γνωστικές ιδιότητες του επιλεγμένου χρήστη. Στα συμπεράσματα της μελέτης παρατίθεται μια επισκόπηση για το πώς είναι δυνατό να είναι οι κωδικοί πρόσβασης ταυτόχρονα εύκολο να αφομοιωθούν και σχετικά εύκολοι στη χρήση, διατηρώντας το επίπεδο ασφάλειας υψηλό.

Επιπλέον, οι ιδιότητες της συσκευής ελέγχου ταυτότητας διαδραματίζουν σημαντικό ρόλο σε αυτή τη διαδικασία. Οι συγγραφείς της μελέτης [38] διερεύνησαν τη χρηστικότητα των κωδικών πρόσβασης με κείμενο σε κινητές συσκευές. Αποδείχθηκε ότι η χρήση ενός smartphone ή άλλου πληκτρολογίου εξοπλισμού για τη δημιουργία κωδικού πρόσβασης δεν ευνοούν τους χρήστες σε σύγκριση με συμβατικούς προσωπικούς υπολογιστές. Μιαν ακόμα εργασία [39] επιβεβαιώνει την ίδια θεωρία από την άποψη της αποτελεσματικότητας. Σήμερα, οι περισσότερες από τις υπηρεσίες ηλεκτρονικής πιστοποίησης βασίζονται στη γνώση, δηλαδή εξαρτώνται από το συνδυασμό ονόματος χρήστη και κωδικού πρόσβασης. Πιο πολύπλοκα συστήματα απαιτούν από τον χρήστη να αλληλοεπιδρά με επιπλέον tokens (κωδικοί μίας χρήσης, γεννήτριες κωδικών, τηλέφωνα κλπ.).

Προκειμένου λοιπόν να επιτευχθεί ο ιδανικός συνδυασμός χρηστικότητας και ασφάλειας στα μέσα ελέγχου ταυτότητας, είναι πολύ σημαντικό να κατανοήσουμε τα δεδομένα των χρηστών που χρειάζονται προστασία και έλεγχο της πρόσβασης στο σύστημα, καθώς και να καθιερωθεί ο ιδανικός τρόπος διαχείρισης των δικαιωμάτων των χρηστών του συστήματος. Εξαιτίας του ολοένα και πιο δυναμικού τρόπου ζωής, όπου επιτρέπεται στους χρήστες να συνδέονται με συστήματα πληροφοριών από οπουδήποτε με οποιαδήποτε σχεδόν συσκευή διατίθεται στην αγορά, κρίνεται ως απολύτως απαραίτητη η δυνατότητα μεταφοράς ενός μέρους του συστήματος πληροφοριών από την ασφαλή υποδομή σε οποιοδήποτε μέσο.

Η ανασφάλεια στο περιβάλλον διεπαφής (user interface) χρηστών προκαλείται από το γεγονός πως ο χρήστης αγνοεί τις πιο εξεζητημένες λειτουργίες ενός συστήματος, όπου ορισμένες δεν αποτελούν μόνο απειλή, αλλά μπορούν να βλάψουν το ίδιο το σύστημα, π.χ. αφήνοντας τις υπηρεσίες δικτύου ενεργές, παρόλο που ο χρήστης δεν τις χρειάζεται, ή όταν ένας χρήστης έχει ελάχιστες ή καθόλου πληροφορίες σχετικά με τα διαθέσιμα μέτρα ασφαλείας. Έτσι δημιουργήθηκε το ζήτημα της ασφάλειας στο περιβάλλον διεπαφής χρήστη.

Από τη μια πλευρά, υπάρχει η προοπτική της χρηστικότητας ενός συστήματος λοιπόν, που περιγράφεται σαν την δυνατότητα που δίνει ένα σύστημα ή μια υπηρεσία στο χρήστη, να εκτελέσει ικανοποιητικά μια διεργασία. Η τήρηση και ενημέρωση των διαδικασιών ασφάλειας και προστασίας της ιδιωτικής ζωής είχαν στο παρελθόν αφεθεί στους διαχειριστές συστημάτων που είναι έμπειροι και μπορούσαν να αφιερώσουν χρόνο στη μελέτη της χρήσης πολύπλοκων περιβαλλόντων διεπαφής χρήστη, όμως τελικά οι ευθύνες αυτές μετακινούνται προοδευτικά στην πλευρά των χρηστών [41]. Η εξασφάλιση της χρηστικότητας του περιβάλλοντος μέσω του οποίου ο χρήστης έρχεται σε επαφή με το σύστημα, είναι μια απαίτηση προκειμένου να εξασφαλιστεί η ασφάλεια της διασύνδεσης, δεδομένου ότι είναι η κύρια πλατφόρμα που χρησιμοποιούν οι χρήστες για να αλληλοεπιδράσουν με το σύστημα. Αυτό σημαίνει ότι πρέπει να υπάρξει συμβιβασμός και μια κάποια ισορροπία μεταξύ χρηστικότητας και ασφάλειας.

Ωστόσο, [42] ο λόγος για τον οποίο τα συστήματα ασφαλείας αποτυγχάνουν, είναι επειδή κατά το σχεδιασμό των συστημάτων δεν λαμβάνονται υπόψη οι ανάγκες χρηστικότητας και οι απαιτήσεις των χρηστών. Με απλά λόγια τελικά και όπως προκύπτει από τις διάφορες μελέτες [43], είναι δύσκολο για τους διαχειριστές και τους προγραμματιστές να κατανοήσουν και να ενσωματώσουν αρχικά την απλότητα που αναζητούν οι χρήστες σε μια εφαρμογή και την ίδια στιγμή, είναι δύσκολο για τους τελικούς χρήστες να καταλάβουν ότι οι διαφορετικές εφαρμογές μπορεί να είναι λίγο

περισσότερο περίπλοκες προκειμένου να είναι πιο ασφαλέστερες και προστατευμένες από διαφορετικούς κινδύνους.

Όταν αναφερόμαστε λοιπόν στην έννοια της χρηστικότητας, ουσιαστικά αναφερόμαστε σε ένα σύνολο το οποίο περιλαμβάνει το περιβάλλον διεπαφής χρήστη καθώς και τις λειτουργίες και τις επιδόσεις ενός συστήματος. Η δυνατότητα πρόσβασης σε ένα σύστημα εξαρτάται από το επίπεδο των τεχνικών δεξιοτήτων και γνώσεων του χρήστη. Κατά συνέπεια, τα συστήματα ελέγχου ταυτότητας που χρειάζονται ξεχωριστό υλικό, λογισμικό ή τεχνική τεχνογνωσία μπορούν επίσης να αγνοούν τους χρήστες και να παραβιάζουν το κοινό πρότυπο προσπελασιμότητας και απεριόριστης κατάστασης. Επομένως, για να μετρηθεί η απαίτηση, είναι απαραίτητο να εισαχθεί μια μικρή διαμόρφωση του υλικού και του λογισμικού που δεν απαιτεί τεχνική εμπειρογνωμοσύνη για το τμήμα του χρήστη.

Με βάση την ανασκόπηση βιβλιογραφίας [44, 45]: σχετικά με τη χρηστικότητα των συστημάτων, κάποιες από τις κύριες παραμέτρους χρηστικότητας, περιγράφονται συνοπτικά:

1. **Χρόνος εκμάθησης.**

Η φάση εκμάθησης επηρεάζει τόσο το κόστος εγκατάστασης και εφαρμογής του συστήματος όσο και την αποδοχή του από τους χρήστες. Εάν η φάση μάθησης απαιτεί πολύ χρόνο και υπομονή, δεν είναι βέβαιο ότι οι χρήστες, συχνά υπάλληλοι, θα είναι τελικά τόσο πρόθυμοι να χρησιμοποιήσουν το σύστημα. Αυτό θα καταστήσει την εφαρμογή του σχετικά ανούσια και ταυτόχρονα υπέρμετρα δαπανηρή σε χρόνο και χρήμα. Η προσπάθεια συνδέεται στενά με την κατανάλωση χρόνου, και η προσπάθεια που απαιτείται διαφέρει ανάλογα με το χρήστη.

2. **Ταχύτητα απόδοσης**.

Η ταχύτητα απόδοσης συνδέεται στενά με την έννοια του αποδεκτού χρόνου χρήσης. Οι χρήστες τείνουν να δυσανασχετούν στη χρήση ενός συστήματος εάν χρειάζεται πολύς χρόνος και προσπάθεια.

3. Υποκειμενική ικανοποίηση

Οι πιο σημαντικές πληροφορίες σχετικά με τη χρηστικότητα του συστήματος αυθεντικοποίησης είναι τα σχόλια και η κριτική από το χρήστη. Οι υποκειμενικές απόψεις των χρηστών είναι πολύτιμες αλλά κάπως δύσκολο να μετρηθούν. Είναι επομένως σημαντικό να χρησιμοποιείται μια προκαθορισμένη κλίμακα όταν ζητείται από τους χρήστες σχετικά η γνώμη τους σχετικά με το σύστημα.

4. Ποσοστό σφαλμάτων από τους χρήστες

Εάν ένα σύστημα ελέγχου ταυτότητας πρόκειται να τεθεί σε εφαρμογή και να χρησιμοποιηθεί, είναι εξαιρετικά σημαντικό το ποσοστό των σφαλμάτων που προκαλούνται από το σύστημα να είναι μικρό ή μηδενικό. Ικανός αριθμός δοκιμών θα πρέπει να εφαρμοστεί με σκοπό να προκύψουν όσο το δυνατόν πιο ρεαλιστικά αποτελέσματα, προκειμένου να αποφευχθούν λάθη κατόπιν διάθεσης του συστήματος στους χρήστες.

5. Ευκολία

Η ασφάλεια ενός συστήματος δε θα πρέπει να είναι χρονοβόρα ή εμφανής και αυτό διότι αυτό προκαλεί δυσφορία στον χρήστη, ο οποίος πιθανόν να απενεργοποιήσει το χαρακτηριστικό ασφαλείας (security feature) για να αποτρέψει την επίμονη ενόχληση του [44]. Σημειώνεται ότι η διάρκεια ανοχής του χρήστη σε ένα χαρακτηριστικό ασφαλείας είναι εξαιρετικά μικρή επειδή ανταποκρίνεται αρνητικά σε συστήματα που αισθάνεται ότι του καταναλώνουν το χρόνο του χωρίς εμφανές αποτέλεσμα. Εξετάζοντας την έννοια της άνεσης λοιπόν για ένα σύστημα ελέγχου ταυτότητας λαμβάνεται υπόψη ο χρόνος που καταναλώνεται για την πραγματοποίηση ενός ελέγχου ταυτότητας ή αντικατάστασης και εγγραφής ενός χρήστη. [45] Ο χρόνος ελέγχου ταυτότητας αναφέρεται στον χρόνο που διαρκεί καθώς ο χρήστης προσπαθεί να εισάγει τα προσωπικά του στοιχεία προκειμένου να αποκτήσει πρόσβαση σε ένα σύστημα. Ο χρόνος αντικατάστασης είναι ο χρόνος ανάκτησης των πληροφοριών ελέγχου ταυτότητας για έναν χρήστη όταν δεν

είναι πλέον ενεργός. Τέλος, ο χρόνος εγγραφής είναι ο χρόνος που διαρκεί όταν ο κωδικός ελέγχου ταυτότητας έχει εκχωρηθεί πρόσφατα για πρώτη φορά. Από αυτούς τους τρεις, ο χρόνος που δαπανάται για την εξακρίβωση της γνησιότητας είναι ο πιο σημαντικός, διότι επηρεάζει την επάρκεια αυτού του κριτηρίου ποιότητας της χρηστικότητας.

6. Κατανόηση

Η ικανότητα των χρηστών ενός συστήματος να κατανοούν τα χαρακτηριστικά ασφαλείας δείχνει την έκταση της χρηστικότητας αυτού του συστήματος [44]. Μια από τις αρχές του σχεδιασμού περιβάλλοντος διεπαφής χρήστη, είναι ότι ο χρήστης θα πρέπει να είναι σε θέση να αναγνωρίσει αντί να χρειάζεται να ανακαλέσει την ιδιότητα μιας συγκεκριμένης λειτουργίας.

7. Περιεκτικότητα

Δεδομένου ότι η χρήση της τεχνολογίας δεν είναι προαιρετική αλλά μάλλον κάτι που πρέπει να χρησιμοποιούν οι χρήστες, ο σχεδιασμός του περιβάλλοντος διεπαφής χρήστη θα πρέπει να μπορεί να περικλείει διάφορους τύπους χρηστών [46,47]. Αυτό εξασφαλίζει ότι κάθε χρήστης, ανεξάρτητα από το επίπεδο της κατανόησης, της δεξιότητας και των γνώσεων του, μπορεί να χρησιμοποιήσει ένα σύστημα με χαρακτηριστικά ελέγχου ταυτότητας. Αυτό το κριτήριο ποσοτικοποιείται με υπολογισμό της προσθήκης χρηστών σε ταξινομήσεις αναπηρίας. Οι χρήστες πρέπει να λαμβάνουν σαφή ένδειξη τι πρέπει να κάνουν σε οποιοδήποτε επίπεδο.

8. Αποδοτικότητα

Ικανότητα του λογισμικού να επιτρέπει στους χρήστες να καταναλώνουν τα ελάχιστα δυνατά ποσά πόρων (π.χ. MB) σε σχέση με την αποτελεσματικότητα που επιτυγχάνεται.

9. Αποτελεσματικότητα

Η ικανότητα του εργαλείου να επιτρέπει στους χρήστες να επιτυγχάνουν συγκεκριμένες εργασίες με ακρίβεια και πληρότητα.

10. Παραγωγικότητα

Το επίπεδο αποτελεσματικότητας που επιτυγχάνεται σε σχέση με τους πόρους (δηλαδή ο χρόνος για την ολοκλήρωση των εργασιών, οι προσπάθειες των χρηστών, τα υλικά ή το οικονομικό κόστος χρήσης) που καταναλώνουν οι χρήστες και το σύστημα. Οι παραγωγικές ενέργειες χρήστη είναι εκείνες που συμβάλλουν στην παραγωγή των εργασιών. Ως εκ τούτου, ο ορισμός της παραγωγικότητας θεωρεί τους παραγωγικούς πόρους που δαπανώνται για την εκπλήρωση των καθηκόντων των χρηστών.

11. Ικανοποίηση

Αναφέρεται στις υποκειμενικές απαντήσεις των χρηστών σχετικά με τα συναισθήματά τους κατά τη χρήση του λογισμικού (δηλ. Ο χρήστης είναι ικανοποιημένος ή ευχαριστημένος με το σύστημα;).

12. Ευκολία Μάθησης

Η ευκολία με την οποία μπορούν να κυριαρχήσουν τα χαρακτηριστικά που απαιτούνται για την επίτευξη συγκεκριμένων στόχων. Είναι η δυνατότητα του προϊόντος λογισμικού να επιτρέπει στους χρήστες να αισθάνονται ότι μπορούν να χρησιμοποιήσουν παραγωγικά το προϊόν λογισμικού αμέσως και έπειτα γρήγορα να μάθουν άλλες νέες λειτουργίες.

13. Ασφάλεια

Αφορά το αν ένα προϊόν λογισμικού περιορίζει τον κίνδυνο βλάβης σε άτομα ή άλλους πόρους, όπως υλικό ή αποθηκευμένες πληροφορίες. Στο πρότυπο ISO / IEC 9126-4 (2001) αναφέρεται ότι υπάρχουν δύο πτυχές της ασφάλειας των προϊόντων λογισμικού, της ασφάλειας λειτουργίας και της ασφάλειας έκτακτης ανάγκης. Η λειτουργική ασφάλεια αναφέρεται στην ικανότητα του προϊόντος λογισμικού να ικανοποιεί τις απαιτήσεις του χρήστη κατά τη διάρκεια της κανονικής λειτουργίας χωρίς να βλάπτει άλλους πόρους και το περιβάλλον. Τα κριτήρια που πρέπει να ληφθούν υπόψη κατά την αξιολόγηση της λειτουργικής ασφάλειας περιλαμβάνουν τη συνοχή, την ακρίβεια, την πληρότητα, την ασφάλεια και την ασφάλεια. Η ασφάλεια σε

περίπτωση έκτακτης ανάγκης αφορά την ικανότητα του προϊόντος λογισμικού να λειτουργεί εκτός της κανονικής λειτουργίας του, αλλά εξακολουθεί να αποτρέπει τους κινδύνους. Τα κριτήρια για την ασφάλεια έκτακτης ανάγκης περιλαμβάνουν ανοχή σφάλματος και ασφάλεια των πόρων.

14. Προσβασιμότητα

Η ικανότητα ενός προϊόντος λογισμικού να χρησιμοποιείται από άτομα με κάποιον τύπο αναπηρίας (π.χ. οπτική, ακοή, ψυχοκινητική) [48]. Η Κοινοπραξία World Wide Web (Caldwell et al., 2004) πρότεινε διάφορες κατευθυντήριες γραμμές σχεδίασης για τη δημιουργία ιστοσελίδων πιο προσιτών σε άτομα με αναπηρίες.

15. Η καθολικότητα

Κατά πόσον ένα προϊόν λογισμικού φιλοξενεί μια ποικιλία χρηστών με διαφορετικό πολιτισμικό υπόβαθρο (π.χ. θεωρείται η τοπική κουλτούρα), διαφορετική γλώσσα, διαφορετικές κοινωνικές αντιλήψεις κλπ.

16. Χρησιμότητα

Εάν ένα προϊόν λογισμικού επιτρέπει στους χρήστες να λύσουν πραγματικά προβλήματα με αποδεκτό τρόπο. Η χρησιμότητα συνεπάγεται ότι ένα προϊόν λογισμικού έχει πρακτική χρησιμότητα, η οποία εν μέρει αντικατοπτρίζει το πόσο στενά το προϊόν υποστηρίζει το μοντέλο εργασίας του χρήστη. Η χρησιμότητα εξαρτάται προφανώς από τα χαρακτηριστικά και τη λειτουργικότητα που προσφέρει το προϊόν λογισμικού. Αντικατοπτρίζει επίσης τη γνώση και το επίπεδο δεξιοτήτων των χρηστών κατά την εκτέλεση ορισμένων εργασιών (δηλαδή δεν λαμβάνεται υπόψη μόνο το προϊόν λογισμικού).

17. Φορητότητα

Η ικανότητα ενός συστήματος να εμφανίζεται σε διαφορετικές πλατφόρμες, Φυσικά οι παράγοντες που μόλις περιγράφηκαν δεν θεωρούμε ότι είναι ανεξάρτητοι. Στο ηλεκτρονικό εμπόριο (e-commerce), για

παράδειγμα, οι ηλεκτρονικοί πελάτες ενδέχεται να εμπιστεύονται έναν ιστότοπο μόνο εάν αρχικά αισθάνονται ασφαλείς όμως την ίδια στιγμή ικανοποιημένοι από την πλοήγηση, την εμφάνιση, την εύκολη αναζήτηση κλπ. όταν το χρησιμοποιούν.

Είναι προφανές ότι τα ποιοτικά κριτήρια χρηστικότητας και ασφάλειας δεν μπορούν να συζητηθούν ανεξάρτητα. Είναι αναγκαίο να εξεταστούν μαζί ενώ σχεδιάζεται το περιβάλλον διεπαφής χρήστη. Αυτό θα εμποδίζει τους προγραμματιστές από το να επινοήσουν και να δημιουργήσουν ένα σύστημα στο οποίο όλες οι διεργασίες ασφαλείας να μένουν κρυφές, να γίνονται αυτόματα χωρίς ο χρήστης να κατανοεί ουσιαστικά τα χαρακτηριστικά ασφαλείας του συστήματος Μια καλύτερη λύση θα ήταν να γνωρίζουν οι χρήστες τα πράγματα που κάνουν καθώς και τις επιπτώσεις που μπορεί να προκληθούν εξαιτίας των ενεργειών τους. Υπάρχει η γενική πεποίθηση ότι η ασφάλεια και η χρηστικότητα είναι ασυμβίβαστες έννοιες όταν πρόκειται για σχεδιασμό που περιλαμβάνει την εμπλοκή χρήστη, αλλά δεν θα έπρεπε να είναι έτσι.

Η χρηστικότητα και η ασφάλεια πρέπει να εξεταστούν κατά τέτοιο τρόπο που να επιτρέπει στους χρήστες να κάνουν προτάσεις στους προγραμματιστές για το σχεδιασμό του περιβαλλόντων χρήστη που βρίσκουν άνετα ώστε να μπορούν να απολαμβάνουν και ταυτόχρονα να χρησιμοποιούν με ασφάλεια τα πληροφοριακά συστήματα. Με την εμφάνιση της χρήσης υπηρεσιών Διαδικτύου που καθιστά τη ζωή πολύ πιο εύκολη και βολική για τους χρήστες, τίθεται το ερώτημα σχετικά με την χρηστικότητα και την ασφάλεια του συστήματος που χρησιμοποιούν. Το ζήτημα της χρηστικότητας φαίνεται να τονίζεται περισσότερο με νέους τρόπους που καταλήγουν στη βελτίωση του σχεδιασμού της ανθρώπινης αλληλεπίδρασης με το σύστημα, με ελάχιστα λόγια για την ασφάλεια.

Κεφάλαιο 4

SQRL

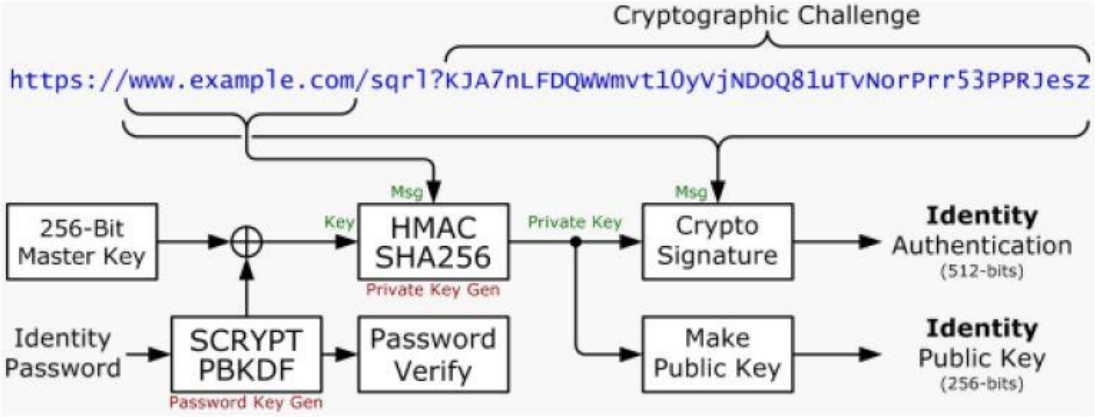
4.1 Η μέθοδος – τεχνολογία SQRL

Το Secure Reliable Quick Login - SQRL (Ασφαλής Γρήγορη Αξιόπιστη Σύνδεση) είναι ένα νέο ισχυρό πρωτόκολλο ελέγχου ταυτότητας το οποίο δημιουργήθηκε από τον Steve Gibson [49]. Λειτουργεί σαν ένα challenge / response μοντέλο και χρησιμοποιεί την ασύμμετρη κρυπτογράφηση κλειδιών. Το SQRL στοχεύει να αντικαταστήσει τα ονόματα χρηστών και τους κωδικούς πρόσβασης που αποτελούν την ταυτότητά του εκάστοτε χρήστη.

Με την τεχνολογία αυτή δεν δίνονται «σημαντικές» πληροφορίες που μπορούν να εκθέσουν την ταυτότητά του χρήστη μέσω του Διαδικτύου. Απεναντίας ο διακομιστής πρέπει να αποθηκεύσει μόνο ένα σύνολο δημόσιων κλειδιών, τα οποία, έστω κι αν χαθούν, αποτελούν ελάχιστη απειλή για την κλοπή της ταυτότητας του χρήστη. Ως εκ τούτου, προτείνεται ένας νέος μηχανισμός μέσω του οποίου ο χρήστης πρέπει να σαρώσει μόνο τον κώδικα QR που αποστέλλεται από το διακομιστή για να συνδεθεί. Η ταυτότητα του χρήστη μέσω του Διαδικτύου προέρχεται από ένα κύριο κλειδί που είναι αποθηκευμένο στην εφαρμογή SQRL και αυτό το κλειδί προστατεύεται από έναν κύριο κωδικό πρόσβασης. Με αυτόν τον τρόπο, οι χρήστες πρέπει να θυμούνται μόνο έναν κύριο κωδικό πρόσβασης για την ίδια την εφαρμογή SQRL και όχι πολλαπλούς κωδικούς πρόσβασης για όλες τις διαφορετικές υπηρεσίες που χρησιμοποιούν.

Για να πιστοποιήσει την ταυτότητά σε μια υπηρεσία που χρησιμοποιεί SQRL, ο χρήστης πρέπει να κατεβάσει στο smartphone του (android / iphone) ή στην επιφάνεια εργασίας του υπολογιστή του, μια εφαρμογή SQRL που θα περιέχει ένα μυστικό 256-bit Master κώδικα. Αυτός είναι ένας τυχαία παραγόμενος μυστικός κώδικας, ο οποίος ποτέ δεν αποκαλύπτεται σε

κανέναν άλλο. Ο ίδιος ο κώδικας QR θα περιέχει μια διεύθυνση URL, συμπεριλαμβανομένου του ονόματος τομέα του ιστότοπου στον οποίο προσπαθεί ο χρήστης να συνδεθεί. Κατά τη σάρωση του κώδικα, η εφαρμογή δημιουργεί ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού από το κύριο κλειδί και το όνομα τομέα του ιστότοπου (4.1).



4.1 Διαδικασία κρυπτογράφησης SQRL-ID (www.grc.com/sqrl)

Στη συνέχεια, η εφαρμογή επικοινωνεί απευθείας με τον ιστότοπο, αποστέλλοντας το δημόσιο κλειδί ως την ταυτότητά του χρήστη (το ισοδύναμο ενός ονόματος χρήστη) και τον κρυπτογραφημένο κώδικα QR ως τον έλεγχο ταυτότητας (το ισοδύναμο ενός κωδικού πρόσβασης). Εφόσον ο μυστικός κωδικός δεν αλλάζει ποτέ, το δημόσιο κλειδί που προκύπτει δεν θα αλλάξει. Αυτό σημαίνει ότι ο ιστότοπος θα ξέρει ότι είστε εσείς. Και με την κρυπτογράφηση του κώδικα QR του ιστότοπου με το ιδιωτικό σας κλειδί, ο ιστότοπος μπορεί να επιβεβαιώσει ότι πράγματι ο χρήστης διαθέτει το ιδιωτικό κλειδί που ταιριάζει, χωρίς να το έχει πραγματικά, χάρη στην τεχνολογία της κρυπτογραφίας δημόσιου κλειδιού. Το κύριο πλεονέκτημα της χρήσης του SQRL είναι ότι οι χρήστες πρέπει μόνο να θυμούνται έναν κύριο κωδικό πρόσβασης για την ίδια την εφαρμογή SQRL και όχι κωδικούς πρόσβασης σε όλες τις διαφορετικές υπηρεσίες ελέγχου ταυτότητας που χρησιμοποιούν.

Το SQRL χρησιμοποιεί ασύμμετρη κρυπτογράφηση κλειδιού για την παροχή ασφάλειας. Ο χρήστης έχει ένα κύριο κλειδί (Master Key) που αντιπροσωπεύει ολόκληρη την ταυτότητά του μέσω του Διαδικτύου. Δημιουργείται ένα ζεύγος δημόσιου / ιδιωτικού κλειδιού χρησιμοποιώντας το HMAC (SHA-256). Το Master Key και το όνομα τομέα (ο ιστότοπος στον οποίο ο χρήστης προσπαθεί να ταυτοποιήσει) έχουν κατακερματιστεί (hashed) για να παραγάγουν ένα ιδιωτικό κλειδί, το οποίο επεξεργάζεται περαιτέρω για να αποκτήσει ένα ταιριαστό δημόσιο κλειδί. Κάθε ιστότοπος έχει διαφορετικό ζεύγος δημόσιου / ιδιωτικού κλειδιού για διαφορετικούς χρήστες, αλλά ο ίδιος χρήστης θα έχει πάντα το ίδιο ζεύγος δημόσιου / ιδιωτικού κλειδιού για τον ίδιο ιστότοπο, επειδή το κύριο κλειδί και το όνομα τομέα δεν αλλάζουν ποτέ (4.2)

4.2 Δημιουργία SQRL κλειδιών

Για την εγγραφή, ο χρήστης στέλνει αίτημα στον διακομιστή. Ο διακομιστής απαντά με μια μακροσκελή ασφαλής πρόκληση που κωδικοποιείται σε έναν κώδικα QR. Η εφαρμογή SQRL σαρώνει τον κώδικα, δημιουργεί ζεύγος δημόσιου / ιδιωτικού κλειδιού για αυτόν τον ιστότοπο, υπογράφει την πρόκληση με το ιδιωτικό κλειδί συγκεκριμένου ιστότοπου και στη συνέχεια στέλνει ένα αίτημα POST στο διακομιστή που περιέχει το συγκεκριμένο δημόσιο κλειδί και την υπογεγραμμένη πρόκληση. Ο διακομιστής επαληθεύει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί και στη συνέχεια αποθηκεύει το δημόσιο κλειδί για τον έλεγχο ταυτότητας του χρήστη στο μέλλον (4.3) .

4.3 Δημιουργία SQRL token

Μετά την εγγραφή του χρήστη σε έναν ιστότοπο και την δημιουργία του συγκεκριμένου ζεύγους κλειδιών για κάθε τοποθεσία, κάθε φορά που ο χρήστης προσπαθεί να πιστοποιήσει τον εαυτό του στον εκάστοτε ιστότοπό, η υπηρεσία αυθεντικοποίησης θα στείλει μια πρόκληση (έναν ασφαλή μακρύ τυχαίο αριθμό) που κωδικοποιείται σε ένα QR κώδικα, τον οποίο ο χρήστης μπορεί είτε να σαρώσει (χρησιμοποιώντας αναγνώστη κωδικών QR), να πατήσει (στις οθόνες αφής) ή να κάνει κλικ (σε τηλέφωνα ή επιφάνεια εργασίας). Ο χρήστης υπογράφει την πρόκληση με το ιδιωτικό κλειδί του για συγκεκριμένο ιστότοπο (ο οποίος μπορεί να αναδημιουργηθεί εκ νέου πολύ γρήγορα) και στέλνει ένα ερώτημα POST στην υπηρεσία που περιέχει την υπογραφή. Η υπηρεσία χρειάζεται μόνο να εφαρμόσει μερικές μεθόδους, μία από τις οποίες είναι σε θέση να επαληθεύσει την υπογραφή χρησιμοποιώντας το αποθηκευμένο δημόσιο κλειδί και εάν το επιτυγχάνει , πιστοποιεί τον χρήστη (4.4) .

4.4 Αυθεντικοποίηση SQRL token

Το κύριο κλειδί είναι το μόνο σημαντικό πράγμα που πρέπει να διατηρηθεί ασφαλές. Για το σκοπό αυτό, το κύριο κλειδί είναι κρυπτογραφημένο με έναν κωδικό πρόσβασης, ο οποίος είναι ο μόνος

κωδικός που χρειάζεται να γνωρίζει ο χρήστης. SCrip - μια συνάρτηση εξαγωγής κλειδιών με βάση τον κωδικό πρόσβασης χρησιμοποιείται για την προστασία του κύριου κλειδιού με τον κωδικό πρόσβασης της εφαρμογής χρήστη SQRL.

Δεδομένου ότι κάθε nonce (αριθμός που χρησιμοποιείται μόνο μία φορά) ενσωματωμένο στον κώδικα QR αποδίδει έναν διαφορετικό κώδικα QR, δεν είναι δυνατό ένα replay attack. Επίσης, λόγω της τυχαιότητας του nonce, οποιαδήποτε brute force attack δεν θα είναι εφικτή, για έναν εισβολέα. Ένας διακομιστής με δυνατότητα SQRL δεν μπορεί να μιμηθεί έναν χρήστη επειδή το SQRL χρησιμοποιεί ασύμμετρη κρυπτογράφηση κλειδιών, σε αντίθεση με το YubiKey που χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού και, ως εκ τούτου, εκθέτει τον χρήστη να δίνοντας την δυνατότητα στον διακομιστή να τον υποδυθεί. Οι επιθέσεις Man In The Middle (MITM) ματαιώνεται σε κάποιο βαθμό. Στην κρυπτογραφία και την ασφάλεια των υπολογιστών, ο όρος Man In The Middle (MITM) αναφέρεται στην επίθεση όπου ο επιτιθέμενος αποκρύπτει κρυφά και ενδεχομένως μεταβάλλει την επικοινωνία μεταξύ δύο πλευρών (χρήστης / σέρβερ ή χρήστης / χρήστης) που πιστεύουν ότι επικοινωνούν άμεσα μεταξύ τους. Ένα παράδειγμα των MITM είναι η ενεργή παρακολούθηση, στην οποία ο επιτιθέμενος πραγματοποιεί ανεξάρτητες συνδέσεις με τα θύματα και στέλνει μηνύματα μεταξύ τους για να τους κάνει να πιστεύουν ότι μιλάνε άμεσα μεταξύ τους μέσω μιας ιδιωτικής σύνδεσης, όταν στην πραγματικότητα ολόκληρη η συνομιλία ελέγχεται από τον εισβολέα. Ο επιτιθέμενος πρέπει να είναι σε θέση να παρακολουθήσει όλα τα σχετικά μηνύματα που περνούν ανάμεσα στα δύο θύματα και να προσθέσει νέα.

Στην τεχνολογία SQRL όμως, δεδομένου ότι το ζεύγος δημόσιου / ιδιωτικού κλειδιού είναι συγκεκριμένο και εάν κάποιος προσπαθήσει να αλλάξει το όνομα τομέα ακόμη και ελαφρώς, το ζεύγος κλειδιών θα ήταν διαφορετικό από το πραγματικό και ο διακομιστής θα ήξερε ότι είναι υπό επίθεση. Επίσης, κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης, στον χρήστη εμφανίζεται το όνομα του κεντρικού υπολογιστή και ερωτάται αν θέλει

πραγματικά να συνδεθεί στον συγκεκριμένο ιστότοπο. Εάν το legit.com έδειχνε έναν κώδικα QR που ενσωματώνει ένα nonce που αποστέλλεται από το evil.com, η εφαρμογή χρήστη θα ρωτούσε τον χρήστη εάν θέλει να συνδεθεί στο evil.com (επειδή η πρόκληση προέρχεται από την υπηρεσία ελέγχου ταυτότητας του evil.com) και με τον τρόπο αυτόν μπορεί εύκολα να εντοπίσει την ανακατεύθυνση. Αλλά η ανάθεση μιας τόσο μεγάλης ευθύνης στον χρήστη είναι ένας κίνδυνος.

Στο παρακάτω σενάριο (4.5) ένας χρήστης συνδέεται στο evil.com από λάθος του μπερδεύοντάς το με το legit.com. Το evil.com στη συνέχεια στέλνει ένα αίτημα ελέγχου ταυτότητας στο legit.com. Το legit.com στέλνει πίσω έναν έγκυρο κωδικό QR στον αιτούντα -evil.com. Το evil.com το παρουσιάζει στο χρήστη. Ο χρήστης σαρώνει τον κώδικα και εξακριβώνει τον εαυτό του στο legit.com, αλλά το evil.com διαθέτει ένα πιστοποιημένο cookie για τη σύνοδο του χρήστη. Αυτό συμβαίνει κυρίως επειδή η συσκευή όπου στέλνεται η πρόκληση και η συσκευή που ανταποκρίνεται στην πρόκληση αυτή δεν είναι πάντοτε η ίδια (λόγω της λειτουργίας απομάκρυνσης) και δεν υπάρχει μηχανισμός στην πλευρά του διακομιστή για συσχέτιση της διεύθυνσης IP του υπολογιστή με το τη διεύθυνση IP του τηλεφώνου και δεν υπάρχει κανένας τρόπος από την πλευρά του χρήστη να μάθει ποιος είναι ο πραγματικός απομακρυσμένος κεντρικός υπολογιστής, αν υπάρχει σωστή κρυπτογράφηση SSL κ.λπ.

4.5 Σενάριο MIMT

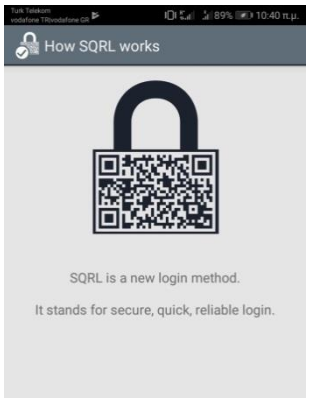
4.2 Πρακτική εφαρμογή

Ενέργειες που πρέπει να γίνουν από τον χρήστη:

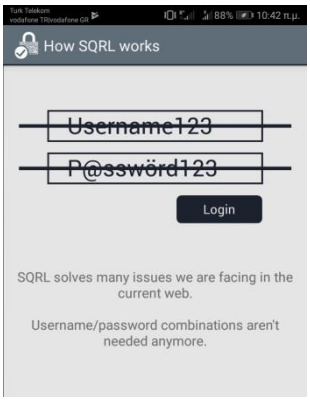
Κατέβασμα (download), είτε από το Play Store για Android συσκευές, είτε από Apple Store για Iphone συσκευές, κάποια εφαρμογή SQRL. Στο συγκεκριμένο παράδειγμα έγινε χρήση της εφαρμογής SQRL του Ralf Wondatschek.

Με την έναρξη της εφαρμογής γίνεται μια μικρή παρουσίαση του τι είναι το SQRL (εικόνες α, β, γ, δ, ε) και δίνει την δυνατότητα στη τελευταία σελίδα (εικόνα στ), εάν ο χρήστης επιθυμεί να μεταβεί στον ιστότοπο του κατασκευαστή της τεχνολογίας SQRL (https://www.grc.com/sqrl/sqrl.htm) για περαιτέρω ενημέρωση.

α.

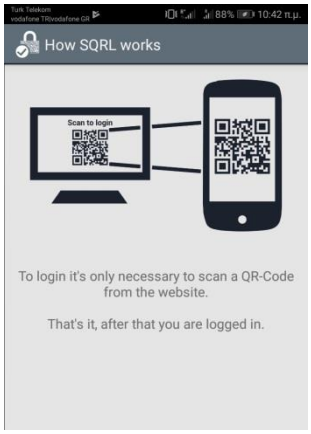


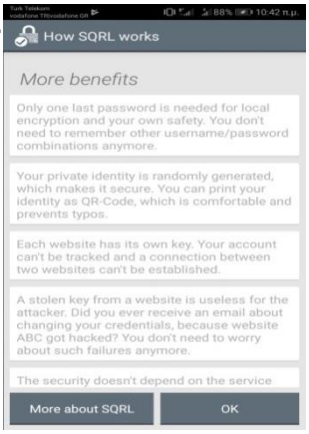
β.



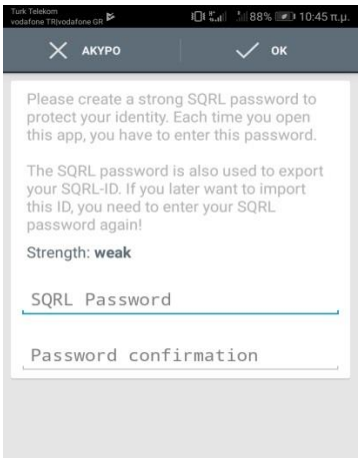
γ.

δ. 

ε. 

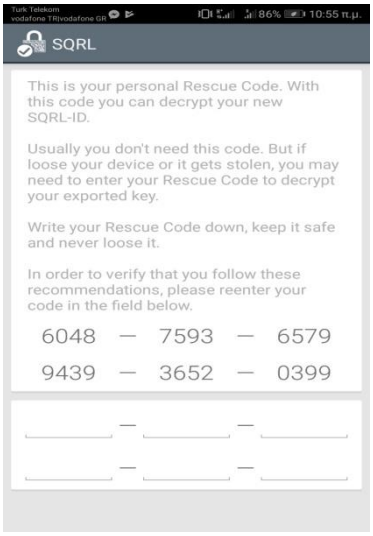
ζ. 

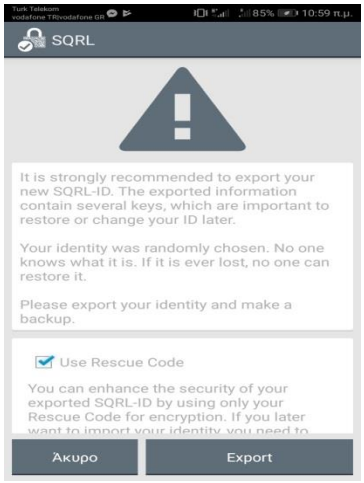
Στη συνέχεια η εφαρμογή ζητάει από τον χρήστη να δημιουργήσει το Master Key, δηλαδή το μόνο κωδικό που θα χρειαστεί πλέον από εδώ και πέρα.



Μετά την δημιουργία του Master Key δίνεται στο χρήστη η επιλογή να δημιουργήσει ένα καινούργιο SQRL-ID ή να εισάγει ένα προγενέστερο σε περίπτωση που έχει ξαναδημιουργήσει.

Εάν επιλέξει να κάνει εισαγωγή το SQRL-ID (import SQRL-ID), τότε ακολουθεί τις οδηγίες που δίνονται αναλυτικά από την εφαρμογή, σκανάροντας το προϋπάρχον QR κωδικό και εισάγοντας τον κωδικό επαναφοράς (Rescue Code)

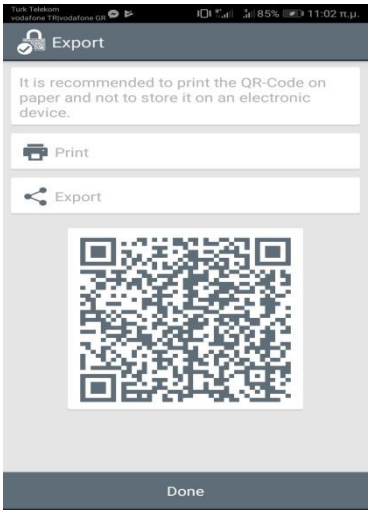




Ενώ εάν θέλει να δημιουργήσει ένα καινούργιο SQRL-ID επιλέγει τη δημιουργία νέου SQRL-ID (Create SQRL-ID). Εμφανίζεται τότε ο Κωδικός Επαναφοράς (Rescue Code) καθώς και οδηγίες. Ο Κωδικός Επαναφοράς πρέπει να γραφτεί μια φορά στα κελιά για να καταχωρηθεί.

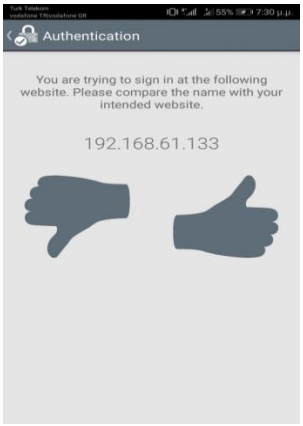
Με την καταχώρηση του Κωδικού Επαναφοράς εμφανίζεται μία προειδοποίηση, εξαγωγής του Κωδικού Επαναφοράς καθώς και την δυνατότητα κρυπτογράφησης του SQRL-ID.

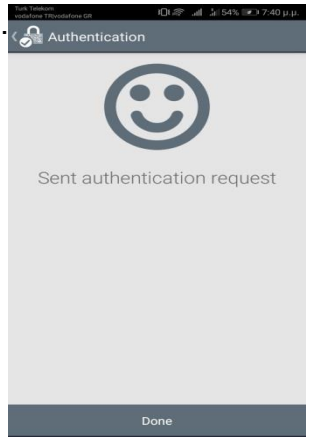
Κατά την εξαγωγή του Κωδικού επαναφοράς εμφανίζεται ένας QR κωδικός ο οποίος περιέχει όλες τις απαραίτητες πληροφορίες



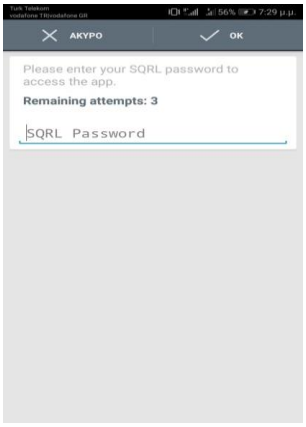
Ενεργοποιείται η κάμερα για άμεση χρήση της τεχνολογίας SQRL στον επιθυμητό ιστότοπο που την υποστηρίζει (α). Η κάμερα σκανάρει τον QR κωδικό του ιστότοπου συνδέεται, κάνοντας έλεγχο των κλειδιών, ενημερώνοντας το χρήστη για τον ιστότοπο που προσπαθεί να συνδεθεί (β). Με τον τρόπο αυτό ενημερώνεται ο χρήστης αν ο ιστότοπος είναι αυτός που επιθυμεί και όχι ένας ψεύτικος. Όταν δοθεί η έγκριση από τον χρήστη τότε ολοκληρώνεται η αυθεντικοποίηση με μήνυμα επιτυχίας ότι το αίτημα αυθεντικοποίησης στάλθηκε (γ).

α.


β.


γ.


Σε περίπτωση που ο χρήστης κλείσει την εφαρμογή και την ξανά ανοίξει για να τη χρησιμοποιήσει πρέπει να εισάγει το Master Key (ή SQRL-ID).



Κεφάλαιο 5
Ανάλυση και Συμπεράσματα

Όπως διαπιστώθηκε από τη θεωρητική ανάλυση αλλά και την πρακτική εφαρμογή του, το SQRL είναι μια λύση στο πρόβλημα της ξεπερασμένης καιι ανασφαλούς πλέον μεθόδου όνομα χρήστη / κωδικός πρόσβασης. Παρέχει μια απλή εναλλακτική λύση, με λειτουργία που γίνεται εύκολα αντιληπτή και κατανοητή από τους χρήστες, χωρίς συμβιβασμούς στην ασφάλεια. Είναι πρακτικά εξίσου ασφαλές με οποιοδήποτε από τα κοινά μοντέλα αυθεντικοποίησης που χρησιμοποιούνται σήμερα, ειδικά αν η χρήση του συνδυάζεται με άλλα MFA, αρκεί οι χρήστης να είναι ενήμεροι για την ασφάλεια. Το ίδιο το SQRL από μόνο του δεν παρέχει απαραίτητα την καλύτερη ή χειρότερη ασφάλεια. Εάν ο ίδιος ο υπολογιστής / Smartphone έχει παραβιαστεί ή ο χρήστης έχει εξαπατηθεί μέσω phishing, τότε πρόκειται για side-channel attack αντί για σημαντικό μειονέκτημα του ίδιου του SQRL. Κάθε συμβατική μέθοδος αυθεντικοποίησης έχει αυτό το πρόβλημα με τις side-channel attacks. Στην αρχική παρουσίαση της ιδέας κατά την διάρκεια του podcast του Steve Gibson (https://www.grc.com/securitynow.htm), στην διάρκεια των ερωτοαπαντήσεων, απαντήθηκαν πολλές από τις ανησυχίες που δημιουργήθηκαν. Επίσης, ο ίδιος ο δημιουργός του SQRL, δήλωσε ότι “Αυτή η "απλή" και "έξυπνη" ιδέα θα πρέπει να "εξεταστεί" και να "σφυρηλατηθεί" από ειδικούς ασφαλείας, καθώς μόνο ο χρόνος θα πει εάν πρόκειται για ασφαλή λύση”

5.1 Σύγκριση SQRL με άλλους μηχανισμούς αυθεντικοποίησης

SQRL vs Κωδικών Πρόσβασης

Το SQRL είναι εξαιρετικά ανώτερο από τους κωδικούς πρόσβασης με πολλούς τρόπους. Όχι μόνο είναι πιο βολικό στη χρήση, μετά την αρχική του ρύθμιση, αφού οι χρήστες δεν χρειάζεται να ανησυχούν για την υπενθύμιση ή την επανάληψη πολλαπλών κωδικών πρόσβασης για κάθε ιστότοπο, αλλά επίσης προστατεύει από την επαναχρησιμοποίηση κωδικών πρόσβασης, τους αδύναμους κωδικούς πρόσβασης, το keylogging και, σε κάποιο βαθμό, από το phishing.

Τα μειονεκτήματα του SQRL σε σύγκριση με τους κωδικούς πρόσβασης είναι ότι είναι πιο δύσκολο να υλοποιηθεί από τους διαχειριστές ιστότοπων, δεν χρησιμοποιείται σε ευρεία κλίμακα, απαιτεί περισσότερο χρόνο για αρχική ρύθμιση, απαιτεί κάποια προσπάθεια σε περίπτωση εγκατάστασης σε μια νέα συσκευή και έχει ένα single point of failure για όλους τους λογαριασμούς του χρήστη, εάν το κύριο κλειδί κλαπεί, κάτι που ισχύει και για τους κωδικούς πρόσβασης εάν ένας χρήστης χρησιμοποιεί τον ίδιο κωδικό πρόσβασης σε κάθε ιστότοπο.

SQRL vs Password Managers

Με πολλούς τρόπους, το SQRL είναι πολύ παρόμοιο με τους Password Managers. Και οι δύο παρέχουν μια ενιαία, κεντρική βάση εμπιστοσύνης, η οποία χρησιμεύει ως είδος διακομιστή μεσολάβησης αυθεντικοποίησης μεταξύ χρηστών και μεμονωμένων υπηρεσιών.

Το κύριο πλεονέκτημα του SQRL σε σχέση με τους Password Managers είναι ότι είναι πιο εύκολο και πιο ασφαλές στη χρήση σε μη αξιόπιστους ή μόνο μερικώς αξιόπιστους υπολογιστές. Για παράδειγμα, εάν ένας χρήστης θέλει να συνδεθεί σε μια ιστοσελίδα με έναν υπολογιστή σε μια δημόσια βιβλιοθήκη, χρησιμοποιώντας Password Managers θα έπρεπε είτε να έχει πρόσβαση στον κωδικό πρόσβασης για τον συγκεκριμένο ιστότοπο

στο τηλέφωνό του και να το ξαναγράψει στον υπολογιστή με μη αυτόματο τρόπο είτε να κατεβάσει τον Password Manager και τη βάση δεδομένων στον υπολογιστή της βιβλιοθήκης, να ξεκλειδώσει τη βάση δεδομένων χρησιμοποιώντας το Master Key. Το πρώτο σενάριο είναι ακατάλληλο για τον χρήστη και αποκαλύπτει τον κωδικό πρόσβασης του χρήστη για τον συγκεκριμένο ιστότοπο στον μη αξιόπιστο υπολογιστή (και σε οποιοδήποτε κακόβουλο λογισμικό στον μη αξιόπιστο υπολογιστή, συμπεριλαμβανομένων των keyloggers).

Το δεύτερο σενάριο είναι ακόμα χειρότερο, καθώς είναι ταυτόχρονα άβολο και εκθέτει ολόκληρη τη βάση δεδομένων κωδικών πρόσβασης και τον κύριο κωδικό πρόσβασης του χρήστη στον μη αξιόπιστου υπολογιστή. Με το SQRL, ο χρήστης θα πρέπει μόνο να σαρώσει έναν κώδικα QR στην οθόνη του μη αξιόπιστου υπολογιστή, ο οποίος είναι πολύ πιο βολικός για τον χρήστη και εκθέτει μόνο έναν υπολογιστή, χωρίς επαναλαμβανόμενα διαπιστευτήρια (όπως κωδικό πρόσβασης) στον μη αξιόπιστο υπολογιστή.

Ένα άλλο πλεονέκτημα του SQRL είναι ότι είναι ευκολότερο να ανακάμψει από το σενάριο της παραπάνω χειρότερης περίπτωσης: κλοπής της βάση δεδομένων του Password Manager του χρήστη και το Master Key. Με έναν Password Manager δεν θα χρειαστεί ο χρήστης μόνο να αλλάξει τον κωδικό πρόσβασής του σε κάθε ιστότοπο, θα πρέπει επίσης να σκεφτεί και για τον εισβολέα που αλλάζει τους κωδικούς πρόσβασής του και ενδεχομένως τον κλειδώνει εκτός από τους λογαριασμούς του. Ο επιτιθέμενος έχει επίσης το πλεονέκτημα ότι κατέχει μια λίστα με όλους τους ιστότοπους στους οποίους ο χρήστης έχει λογαριασμό, καθιστώντας την εκμετάλλευση των κωδικών πρόσβασης πολύ πιο εύκολη. Με το SQRL, έχοντας κλέψει το Master Key του χρήστη ο επιτιθέμενος δεν έχει κατάλογο ιστότοπων στους οποίους έχει λογαριασμό και δεν μπορεί να αλλάξει τον κωδικό πρόσβασής για να τον αποκλείσει από τους λογαριασμούς του. Σε αυτή τη περίπτωση μόλις ο χρήστης χρησιμοποιήσει το identity unlock key (που παράγεται κατά την δημιουργία του λογαριασμού), είναι επίσης λίγο πιο βολικό να αλλάξει τα διαπιστευτήριά της σύνδεσης του σε κάθε ιστότοπο, καθώς το SQRL έχει τη

δυνατότητα να το κάνει αυτόματα για κάθε ιστότοπο που χρησιμοποιεί ο χρήστης χωρίς να χρειάζεται να κάνει τη διαδικασία "αλλαγής κωδικού πρόσβασης".

Τέλος, το SQRL έχει ακόμα ένα μικρό αλλά σημαντικό πλεονέκτημα έναντι των Password Managers, όσον αφορά το στόχο του να αντικαταστήσει τους κωδικούς πρόσβασης εξ ολοκλήρου και αυτό είναι ότι οι ιστότοποι έχουν την επιλογή να επιβάλλουν τη χρήση του SQRL στους παραδοσιακούς κωδικούς πρόσβασης. Αν το SQRL αρχίσει να χρησιμοποιείται ευρέως, οι ιστότοποι θα μπορέσουν να ξεκινήσουν την κατάργηση της χρήσης κωδικών πρόσβασης. Αυτό δεν μπορεί να γίνει με τους Password Managers, καθώς βασίζονται στη χρήση κωδικών πρόσβασης για να λειτουργήσουν.

SQRL vs Client Certificates

Το κύριο πλεονέκτημα που έχει το SQRL σε σχέση με τα Client Certificates είναι η χρηστικότητα του. Τα Client Certificates είναι επί του παρόντος πολύπλοκα στη ρύθμιση, είναι δύσκολο να μεταφερθούν μεταξύ υπολογιστών και έχουν προβλήματα με την προστασία της ιδιωτικής ζωής, όταν το ίδιο το Client Certificate χρησιμοποιείται σε διαφορετικούς ιστότοπους. Ενώ θεωρητικά, ένα σύστημα μπορεί να κατασκευαστεί με τη χρήση Client Certificates που θα λύσουν αυτά τα ζητήματα, θα υπήρχε και το πρόβλημα της κακής ενσωμάτωσης στα User Interface (UI) των ιστοσελίδων καθώς και στους εκάστοτε web servers, προβλήματα τα οποία είναι πιο δύσκολα να λυθούν.

Όσον αφορά την ασφάλεια, τα Client Certificates έχουν το μειονέκτημα ότι απαιτούν τη συμμετοχή μιας Certification Authority (CA). Αυτό είναι δαπανηρό και απαιτεί εμπιστοσύνη στην third party CA. Επιπλέον, εάν ο χρήστης επιλέξει να αγνοήσει τις CA και να υπογράψει μόνος του τα πιστοποιητικά, υπάρχει μεγάλη δυνατότητα ανάκλησης των πιστοποιητικών. Τα Client Certificates επίσης έχουν τα ίδια προβλήματα ασφάλειας και χρηστικότητας με τους Password Managers, όταν οι χρήστες επιθυμούν να συνδεθούν σε έναν μη αξιόπιστο υπολογιστή, πρέπει να μεταφέρουν τα

πιστοποιητικά τους στον μη αξιόπιστο υπολογιστή, το οποίο είναι ταυτόχρονα δύσχρηστο και ενδεχομένως εκθέτει την κύρια ταυτότητα τους σε κακόβουλο λογισμικό σε αυτόν τον υπολογιστή.

5.2 Ανάλυση προτερημάτων και αδυναμιών SQRL.

Αφού αναλύθηκε θεωρητικά η σκοπιμότητα δημιουργίας του και εφαρμόστηκε πρακτικά το εργαλείο SQRL, κατέστη δυνατό να αναλυθούν

Ασφαλές (Secure)

Το SQRL σχεδιάστηκε ως ένα ασφαλές εργαλείο αντικατάστασης της τεχνολογίας των κωδικών πρόσβασης κάνοντας χρήση των παρακάτω διεργασιών :

- Trust No One (TNO) - Συνδέεται απευθείας με τον ιστότοπο στον οποίο επιθυμεί ο χρήστης. Δεν παρακολουθείται η δραστηριότητά του χρήστη.
- Proven Crypto - Χρησιμοποιεί αποδεδειγμένες κρυπτογραφικές τεχνικές για να καταστήσει το SQRL ID σχεδόν αδύνατο να υποκλαπεί.
- Ανωνυμία - Κάθε ιστότοπος λαμβάνει ξεχωριστό identity token. Εάν ένας ιστότοπος δεχθεί επίθεση, το συγκεκριμένο token δεν έχει νόημα σε άλλους ιστότοπους, ελαχιστοποιώντας τον κίνδυνο.
- Δεν υπάρχει αλληλεπίδραση με το πληκτρολόγιο: Η σύνδεση σε έναν υπολογιστή σε μια μη ασφαλής τοποθεσία, όπως μια βιβλιοθήκη ή ένα ξενοδοχείο, πραγματοποιείται χωρίς να εισαχθούν προσωπικές πληροφορίες διαπιστευτηρίων στον υπολογιστή. Δεν παρέχεται κανένα όνομα χρήστη ή κωδικός πρόσβασης που να μπορεί να καταγραφεί από κάποιο keylogger ή κακόβουλο λογισμικό (malware).

Γρήγορο (Quick)

Το αναγνωριστικό SQRL υπάρχει στον υπολογιστή ή στο smarphone κωδικοποιημένο σε κατάσταση αδράνειας, έως ότου χρειαστεί να χρησιμοποιηθεί.. Όταν θα είναι απαραίτητο ο χρήστης να συνδεθεί σε έναν ιστότοπο με δυνατότητα SQRL, απλώς κάνει κλικ ή σαρώνει τον κώδικα QR.

Αξιόπιστο (Reliable)

Το SQRL είναι ακριβώς εκεί που το χρειάζεται ο κάθε χρήστης. Αν σταματήσει να λειτουργεί ή καταστραφεί, μπορεί να γίνει χρήση του rescue code για να επαναφορά του αναγνωριστικού SQRL.

- Σε περίπτωση κλοπής της συσκευής, το SQRL ID του χρήστη, προστατεύεται κρυπτογραφικά, καθιστώντας σχεδόν αδύνατο να χρησιμοποιηθεί από τρίτους.
- Υπάρχει η δυνατότητα να αντικατασταθεί το SQRL ID ώστε να αποκλειστεί ο πιθανός εισβολέας από τους διάφορους λογαριασμούς του χρήστη.
- Υπάρχει η δυνατότητα μεταφοράς του SQRL ID κατά την αλλαγή συσκευής του χρήστη ώστε να εξασφαλίζεται η συνέχεια της διαλειτουργικότητας.

Απλό - εύκολα προσβάσιμο

Το SQRL είναι απλό και ανοιχτό, από σχεδιασμού του. Το ίδιο το πρωτόκολλο καθώς και ο πηγαίος κώδικας είναι ανοικτός (open source), σε όποιον επιθυμεί να το επεξεργαστεί. Πολλοί επαγγελματίες ασφαλείας θα αναθεωρήσουν το SQRL και με τον τρόπο αυτό, θα εντοπιστούν τυχόν προβλήματα. Επιτρέπει τη δημιουργία λογαριασμού χωρίς τη χρήση διεύθυνσης ηλεκτρονικού ταχυδρομείου μέσω ενός διαμεσολαβητή (a third-party provider). Αυτό έχει ως αποτέλεσμα να :

- Μην είναι απαραίτητο ένα επιβεβαιωτικό μήνυμα ηλεκτρονικού ταχυδρομείου.

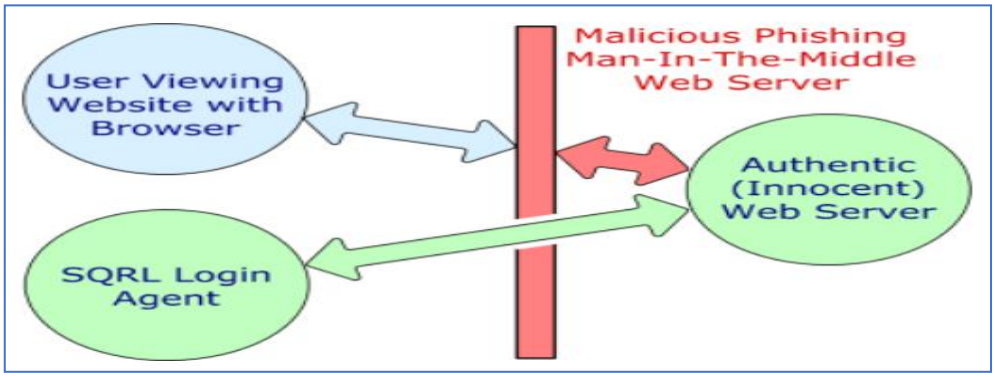
- Η ταυτότητά του χρήστη παραμένει κρυφή και το απόρρητό προστατεύεται.
- Μην υπάρχει ανάγκη δημιουργίας μοναδικού ονόματος χρήστη
- Μην υπάρχει ανάγκη επιλογής ενός κακού κωδικού πρόσβασης
- Μην υπάρχει ανησυχία για διπλότυπους λογαριασμούς (άτομα με το ίδιο όνομα λογαριασμού)

Αποτροπή επιθέσεων phishing.

Αν και το σύστημα σύνδεσης ταυτότητας SQRL δεν προωθείται ως λύση κατά του ηλεκτρονικού "ψαρέματος" (phishing), θα μπορούσε επίσης να παρέχει κάποια ασφάλεια λόγω της διαδεδομένη διαδικτυακή ανησυχία που προκαλείται από το phishing. Όπως αποδεικνύεται, η αρχιτεκτονική ελέγχου ταυτότητας SQRL παρουσιάζει σημαντικές ευκαιρίες αποτροπής τέτοιου είδους επιθέσεων.

Κατά τη χρήση του SQRL, οι χρήστες δεν αναγνωρίζουν και πιστοποιούν τον εαυτό τους με ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Απεναντίας, η μοναδική τους ταυτότητα προέρχεται από το μυστικό Master Key και το πλήρες όνομα χώρου του ιστότοπου. Δεδομένου ότι το SQRL δημιουργεί μια μοναδική ταυτότητα χρήστη για κάθε τομέα ιστού, η ταυτότητα του χρήστη για ένα ιστότοπο phishing όπως paypol.com ή paypal.cn ή οτιδήποτε άλλο εκτός από τον αυθεντικό ιστότοπο που ο χρήστης πιστεύει ότι επισκέπτεται, θα ήταν άχρηστο σε οποιονδήποτε εισβολέα.

Αυτό σημαίνει ότι ο σύνδεσμος σύνδεσης SQRL που παρέχεται από μια ιστοσελίδα που είναι κακόβουλη, πρέπει να είναι σωστή και αυθεντική. Στο παράδειγμά μας, θα έπρεπε να είναι "paypal.com" γιατί αυτή η συμβολοσειρά ονόματος τομέα χρησιμοποιείται στη δημιουργία της ταυτότητας με την οποία το Paypal γνωρίζει τον χρήστη. Αυτό σημαίνει ότι η εφαρμογή SQRL του χρήστη θα συνδεθεί απευθείας με τον αυθεντικό ιστότοπο και όχι με τον πλαστό ιστότοπο ηλεκτρονικού "ψαρέματος" (1).



1. Τρόπος αντιμετώπισης M.I.T.M / Phishing

Από την προοπτική της χρηστικότητας του εργαλείου (usability), τα κυριότερα προτερήματα που προκύπτουν είναι:

Αποτελεσματικότητα του συστήματος.

Ο χρόνος που θα απαιτηθεί από το χρήστη, προκειμένου να δημιουργήσει έναν νέο λογαριασμό στην εφαρμογή έτσι ώστε να αποκτήσει το προσωπικό και μοναδικό SQRL ID που θα τον συνοδεύει από εδώ και στο εξής, είναι ο ελάχιστος που απαιτείται για τη δημιουργία ενός οποιουδήποτε λογαριασμού σε οποιοδήποτε εργαλείο και λογισμικό.

Ευκολία Μάθησης

Η χρηστικότητα του εργαλείου καθορίζεται εν πολλοίς από την ευκολία με την οποία το λογισμικό εφαρμόζεται και υποστηρίζεται από τους ίδιους τους χρήστες. Λειτουργεί πολύ πιο εύκολα από έναν ή περισσότερους πολύπλοκους ή μη κωδικούς, πιο γρήγορα από την απάντηση προσωπικών ερωτήσεων και ταυτόχρονα διαφυλάττει τα προσωπικά δεδομένα του χρήστη.

Εμπιστοσύνη.

Σε περίπτωση που ο χρήστης, ξεχάσει ποτέ το Master Key ή θέλει να το αλλάξει για κάποιο λόγο ή κλαπεί η ταυτότητά του χρήστη με κάποιο είδος επιτυχούς hack, υπάρχει ένα Rescue Code (κλειδί ανάκτησης ταυτότητας) που δημιουργείται μετά την δημιουργία του Master Key, πρέπει να εκτυπωθεί και να δημιουργηθούν αντίγραφα ασφαλείας, όπως ακριβώς γίνεται με ένα

bitcoin wallet key. Φυσικά, αν όλα πάνε καλά, δεν θα χρειαστεί να γίνει η χρήση του ποτέ.

Φορητότητα σε όλες τις συσκευές διασύνδεσης

Αν και η αρχική πηγή έμπνευσης για την ανάπτυξη αυτού του συστήματος ήταν ένα smartphone το οποίο σαρώνει έναν QR κώδικα σε μια σελίδα σύνδεσης ενός ιστότοπου, μια μικρή αναβάθμιση επιτρέπει πλέον δύο πιο σημαντικούς τρόπους λειτουργίας:

- Σάρωση του κώδικα με ένα smartphone: Χρησιμοποιώντας το μοντέλο που περιγράφηκε παραπάνω, το smartphone ενός χρήστη σαρώνει τον κωδικό QR που εμφανίζεται στη σελίδα σύνδεσης ενός ιστοτόπου και ο χρήστης είναι συνδεδεμένος σε αυτόν τον ιστότοπο.
- TAP THE CODE σε ένα smartphone: Για να συνδεθείτε σε έναν ιστότοπο μέσω του smartphone, μπορεί να γίνει χρήση του οπτικού κώδικας SQRL ο οποίος αποτελεί επίσης έναν σύνδεσμο τύπου URL (χρησιμοποιώντας το sqrl: // ως σχέδιο), η εφαρμογή SQRL που είναι εγκατεστημένη στο smartphone θα λάβει αυτόν τον σύνδεσμο και θα συνδέσει με ασφάλεια τον χρήστη με την τοποθεσία.
- Τέλος TAP THE CODE σε pc / laptop : Για να χρησιμοποιήσει ο χρήστης το σύστημα SQRL σε οποιοδήποτε επιτραπέζιο ή φορητό σύστημα, πρέπει αρχικά να εγκατασταθεί μια εφαρμογή SQRL στην επιφάνεια εργασίας για να λάβει τα sqrl: // links. (Αυτό είναι παρόμοιο με τον τρόπο που ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου εγγράφεται για να λαμβάνει mailto: links.) Αυτό επιτρέπει την ίδια διαδικασία που χρησιμοποιείται από τους χρήστες στην επιφάνεια εργασίας τους, να χρησιμοποιείται και στα Smartphones τους. Όταν οποιοσδήποτε ιστότοπος προσφέρει έναν κώδικα SQRL, ο χρήστης απλώς επιλέγει τον κώδικα με το δρομέα του ποντικιού του και η τοπικά εγκατεστημένη εφαρμογή SQRL θα εμφανιστεί, θα ζητήσει τον κωδικό SQRL, θα επιβεβαιώσει τον τομέα και στη συνέχεια θα συνδεθεί.

Από την άλλη, ένα καινοτόμο λογισμικό όπως το SQRL, το οποίο δεν έχει εφαρμοστεί σε μεγάλο ποσοστό συσκευών και websites προκειμένου να εξαχθούν ασφαλή συμπεράσματα και να αναβαθμιστεί κατά τέτοιο τρόπο που να βελτιωθεί τόσο σε επίπεδο ασφάλειας αλλά και χρηστικότητας, έχει ως φυσικό επακόλουθο την ύπαρξη κάποιων μειονεκτημάτων, τουλάχιστον μέχρι την περεταίρω ανάπτυξη του προκειμένου ει δυνατόν να ξεπεραστούν.

Αρχική Ρύθμιση

Ένα μεγάλο μείον της τεχνολογίας αυτής, όσον αφορά την χρηστικότητα (usability), είναι η αρχική ρύθμισή της. Αφού πρώτα ο χρήστης κατεβάσει την εφαρμογή SQRL, πρέπει να περάσει από μια διαδικασία για να ρυθμίσει / δημιουργήσει την κύρια ταυτότητά του (Master Key) και στη συνέχεια να αποθηκεύσει το Rescue Code. Το οποίο όμως γίνεται μία φορά και δεν θα χρειαστεί να επαναληφθεί, οπότε είναι ταυτόχρονα και πλεονέκτημα.

Χρήση QR Code – Νέας Εφαρμογής

Πρόκειται για κάτι καινούριο και καινοτόμο προκειμένου οι χρήστες να ξεπεράσουν την χρήση τετριμμένων ονομάτων χρήστη και ανασφαλών επαναλαμβανόμενων κωδικών πρόσβασης. Αυτό το γεγονός από μόνο του αποτελεί το πρώτο και κυριότερο «αγκάθι» στην εφαρμογή του SQRL. Οι χρήστες και οι οργανισμοί-εταιρείες θα πρέπει να μεταβάλλουν σε ένα βαθμό τη συνήθη διαδικασία επαλήθευσης ταυτότητας κάτι που απαιτεί χρόνο, χρήμα και ανθρώπινο δυναμικό.

Αλληλεπίδραση με το χρήστη.

Δεν υπάρχει ξεκάθαρος διαχωρισμός σε ότι αφορά τα μειονεκτήματα του, όσον αφορά την προοπτική της ασφάλειας και της χρηστικότητας, καθώς το λογισμικό είναι ιδιαίτερο και άρρηκτα συνδεδεμένο με τον εκάστοτε χρήστη. Είναι προφανές λοιπόν ότι τα σφάλματα των ίδιων των χρηστών υπάρχει

περίπτωση να έχουν έχουν σοβαρό αντίκτυπο στην ασφαλή λειτουργία του SQRL. Μια κλεμμένη συσκευή για παράδειγμα δίνει το δικαίωμα κλοπής των προσωπικών δεδομένων αλλά και του Master Key.

Εφαρμογή και προσάρτηση του σε Websites και εφαρμογές.

Οι ιστότοποι και οι εφαρμογές πρέπει πρώτα να ενεργοποιήσουν οι ίδιες τις συνδέσεις μέσω SQRL και έτσι όπως συμβαίνει για όλα τα νέα πρωτόκολλα, θα υπάρξει μια περίοδος προσαρμογής που πρέπει να ξεπεραστεί πριν είναι πραγματικά χρήσιμη. Ωστόσο, τα οφέλη που θα προκύψουν από αυτό είναι εντυπωσιακά.

Δεν χρησιμοποιούνται διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Παρουσιάζεται σαν ένα μεγάλο πλεονέκτημα του SQRL, το γεγονός ότι δεν είναι απαραίτητο το ηλεκτρονικό ταχυδρομείο. Πρόκειται φυσικά για εξαιρετικό γεγονός για το χρήστη που επιθυμεί να παραμείνει ανώνυμος. Ωστόσο, πολλές τοποθεσίες απαιτούν μια επαφή μέσω ηλεκτρονικού ταχυδρομείου για πολλούς λόγους, με κυριότερο το ότι επιθυμούν να έχουν τη δυνατότητα μάρκετινγκ και το ηλεκτρονικό ταχυδρομείο, τους επιτρέπει να αποστείλουν διαφημιστικό υλικό. Επίσης είναι ένας τρόπος επικοινωνίας με τα μέλη τους οποιαδήποτε στιγμή, καθώς επίσης, ότι εμποδίζουν τα αυτοματοποιημένα συστήματα και τους spammers να δημιουργήσουν αυθαίρετα εκατομμύρια λογαριασμών για τον ιστότοπό τους.

Μυστικότητα όχι ανωνυμία.

Μπορεί χρησιμοποιώντας το, ένας χρήστης, να μην αποκαλύπτει απαραίτητα τα «φυσικά» προσωπικά του στοιχεία, όμως η διεύθυνση IP και άλλες λεπτομέρειες του προγράμματος περιήγησης μπορούν να ληφθούν, οπότε ουσιαστικά η ηλεκτρονική ταυτότητα του χρήστη υπάρχει.

Ανάγκη χρήσης επιπρόσθετων εφαρμογών.

Το Master Key αποθηκεύεται στο Smartphone με τεχνολογία "deep encryption", για την κωδικοποίηση αυτού του μυστικού κλειδιού κατά την

εξαγωγή του και από τον δημιουργό της εφαρμογής προτείνεται το «Scrypt». Το Scrypt όμως χρησιμοποιεί μεγάλο ποσοστό της μνήμης της συσκευής, και αρκετές έχουν περιορισμένη μνήμη RAM.

Το SQRL δεν αναγνωρίζει περιπτώσεις DNS spoofing.

Το SQRL δεν μπορεί από μόνο του να χρησιμοποιηθεί για την ανίχνευση κακόβουλου ιστότοπου χρησιμοποιώντας DNS spoofing. Ένας hacker μπορεί να εισάγει μια ψεύτικη διεύθυνση IP σε ένα διακομιστή DNS και να εξαπατήσει έναν χρήστη να συνδεθεί σε μια ψεύτικη τοποθεσία. Εκτός εάν χρησιμοποιείται Secure DNS, το SQRL δεν εντοπίζει την παρακολούθηση.

5.3 Συμπεράσματα - Παρατηρήσεις

Κατά τη διάρκεια αυτής της εργασίας, εξετάστηκε και αναλύθηκε η εξέλιξη κατά τη διάρκεια των ετών καθώς και τα προτερήματα και οι αδυναμίες διαφορετικών μεθόδων αυθεντικοποίησης. Πιο συγκεκριμένα, περιγράφηκαν οι διαφορετικές τεχνολογίες αυθεντικοποίησης (SFA,2FA,MFA) που δημιουργήθηκαν με το πέρασμα του χρόνου, προκειμένου να ενισχυθεί η ασφάλεια ενάντια στους σύγχρονους κινδύνους και ταυτόχρονα η χρηστικότητα (usability) σε ότι αφορά το περιβάλλον διεπαφής με το χρήστη.

Πιο συγκεκριμένα, εντοπίστηκε, αναλύθηκε και έγινε χρήση της καινοτόμας τεχνολογία SQRL προκειμένου να διαπιστωθεί κατά πόσο μπορεί να αντικαταστήσεις τις παραδοσιακές μεθόδους ταυτότητας SFA και 2FA. Κατόπιν διαφορετικών δοκιμών και τεστ διαπιστώθηκε πως η τεχνολογία του SQRL, μία τεχνολογία για ασφαλή αυθεντικοποίηση μέσω διαδικτύου, χρησιμοποιώντας σύγχρονες συσκευές όπως τα Smartphones, παρέχει αρκετά πλεονεκτήματα σε σχέση με τα παραδοσιακά μέσα ελέγχου ταυτότητας. Η ανάλυση αφορούσε την ασφάλεια της αυθεντικότητας, την αλληλεπίδραση με το χρήστη και την προοπτική βελτίωσης του εργαλείου. Από την ανάλυση προκύπτει ότι η κύρια ευπάθεια προκαλείται κυρίως από τον τρόπο χρήσης και των σφαλμάτων του χρήστη, κοινώς του ανθρωπίνου παράγοντα. Ένας χρήστης SQRL πρέπει να κρατήσει ένα σταθερό μυστικό

κλειδί (Rescue Code) σε ένα ασφαλές μέρος που δεν θα πρέπει να κοινοποιηθεί πουθενά και κυρίως στο διαδίκτυο. Ένα δεύτερο κλειδί, που είναι το PIN του χρήστη (Master Key), χρησιμοποιείται συχνά και το οποίο επίσης πρέπει να παραμένει ιδιωτικό. Εκτός από την αποθήκευση, η χρήση αυτών των μυστικών κλειδιών μέσω εργασιών εισαγωγής ή / και εξαγωγής μπορεί να έχει ως αποτέλεσμα κλοπή ταυτότητας εξαιτίας συσκευών που έχουν προσβληθεί από κακόβουλο λογισμικό. Οι απρόσεκτοι χρήστες είναι επιρρεπείς σε phishing καθώς επίσης κ σε shoulder surfing.

Ως αντίμετρα, που απαλλάσσουν τους χρήστες από την κουραστική χρήση αλλά και διαχείριση κλειδιών και μπλοκάρουν τα κακόβουλα προγράμματα (malware) είναι εφαρμογές που μπορούν να χρησιμοποιήσουν ένα πρόσθετο ασφαλές περιβάλλον, όπως εισάγωντας την τεχνολογία SQRL σε μία smartcard ή σε μία ετικέτα NFC. Επιπροσθέτως, η ενημέρωση και η ευαισθητοποίηση των χρηστών πάνω στην ασφάλεια των δεδομένων τους, θα συμβάλει σε υψηλότερο επίπεδο ευθύνης. Οι χρήστες που έχουν σαφή εικόνα των μεθόδων κλοπής ταυτότητας είναι λιγότερο ευάλωτοι.

Τα αδύναμα σημεία που προκαλούνται λόγω σφαλμάτων στην υλοποίηση και τη δημιουργία της εφαρμογής δεν αποτελούν μέρος αυτού του έργου. Λόγω της σχετικής πρόσφατης εισαγωγής του SQRL (Οκτώβριος 2013), δεν υπάρχουν ακόμη ώριμες υλοποιήσεις και η ανάπτυξή του αν και έχει «παγώσει» από τον ίδιο τον εφευρέτη, εν μέρη συνεχίζεται με πολύ μικρα βήματα.

Εν κατακλείδι, το SQRL στοχεύει στην ανωνυμία και έχοντας αυτό σαν κύριο στόχο σχεδιασμού, η τεχνολογία αυτή είναι κατάλληλη για αυθεντικοποίηση, χωρίς να αποκαλύπτεται η ταυτότητα του χρήστη

5.4 Πιθανοί τρόποι εξέλιξης και βελτίωσης του.

Επί του παρόντος δεν παρέχεται πληθώρα υλοποιήσεων του SQRL και ενσωμάτωση του σε αρκετές εφαρμογές. Λόγω αυτού, ο αντίκτυπος των σφαλμάτων της εφαρμογής δεν μπορεί να προσδιοριστεί. Ωστόσο, η ιστορία δείχνει ότι πολλά σημεία ευπάθειας προέρχονται από τον τομέα της

αυθεντικοποίησης. Οι έλεγχοι ασφαλείας πρέπει να εκτελούνται τόσο σε εφαρμογές όσο και σε εφαρμογές διακομιστή.

Οι συσκευές που έχουν μολυνθεί από κακόβουλο λογισμικό που χρησιμοποιείται για αυθεντικοποίηση επιτρέπουν την κλοπή ταυτότητας. Η πρακτική δείχνει ότι το κακόβουλο λογισμικό είναι επίμονο. Αυτό δικαιολογεί την ανάγκη για όσο το δυνατόν ασφαλέστερο περιβάλλον. Οι προτεινόμενες λύσεις είναι μια ατέρμονη διαδικασία.

Το SQRL υποστηρίζει την ανάκτηση ταυτότητας με το Rescue Code σε περίπτωση που έχει εκτεθεί ή κλαπεί η ταυτότητα του χρήστη. Η τρέχουσα τεχνολογία δεν έχει αυτοματοποιημένη διαδικασία «κλειδώματος» και «αλλαγής ταυτότητας» και οι διαδικασίες πρέπει να εκτελεστούν από τους ίδιους τους χρήστες σε όλους τους ιστότοπους που επισκέπτονται.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Sangare Mamoudou, Wajdi Al-Khateeb, An Overview on Authentication Approaches and Their Usability in Conjunction with Internet and Mobile Applications - August 2014
2. ISO 9241-11:2018(en) Ergonomics of human system interaction – Part 11 : Usability : Definitions and Concepts
3. Marilyn Chun. Authentication mechanisms, which is best ?, 2001. http://www.giac.org/practical/gsec/Marilyn_Chun_GSEC.pdf.
4. John Abbott. Smart cards: How secure are they? GSEC Practical v1.3, 2002. http://www.sans.org/rr/papers/index.php?id=131.
5. Bruce Schneier and Adam Shostack. Breaking up is hard to do: Modeling security threats for smart cards, 1999. http://www.schneier.com/paper-smart-card-threats.
6. David D. Zhang, editor. Biometric Solutions For Authentication in an E-World. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 2002.
7. Marijana Kosmerlj. Passport of the future - biometrics against identity theft. Master's thesis, Royal Institute of Technology, Sweden, 2004.
8. Gregory Williams. More than a pretty face: Biometrics and smartcard tokens. GSEC, 2002. http://www.sans.org/rr/papers/6/125.pdf .
9. G. R. Ganger. Authentication confidences. ,2001. Technical Report CMU-CS-01-123. http://citeseer.ist.psu.edu/456656
10. L. Bechelli, S. Bistarelli, and A. Vaccarelli. Biometrics authentication with smartcard, 2002, http://citeseer.ist.psu.edu/bechelli02biometrics
11. N. Poh, S. Bengio, and J. Korczak. A multi-sample multi-source model for biometric authentication, 2002. http://citeseer.ist.psu.edu/thian02multisample.

12. S.Brostoff and A.Sasse. Are Pass faces more usable than passwords? A field trial investigation. 2000 http://oneman.cs.ucl.ac.uk/brostoff_sasse.pdf.
13. Vaclav Matyas and Zdenek Riha. Biometric authentication- security and usability. 2002. http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf
14. Y. Deswarte and M. Kaaniche Quantitative assessment of operational security: Models and tools. 1996 www.citeseer.ist.psu.edu/dacier96quantitative
15. Timothy J. Hazen, Eugene Weinstein, and Alex Park. Towards robust person recognition on handheld devices using face and speaker identification technologies. In Proceedings of the 5th international conference on Multimodal interfaces, pages 289– 292. ACM Press, 2003. http://doi.acm.org/10.1145/958432.958485 .
16. Niall A. Fox, Ralph Gross, Philip de Chazal, Jeffery F. Cohn, and Richard B. Reilly. Person identification using automatic integration of speech, lip, and face experts. In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pages 25–32. ACM Press, 2003.
17. R. Dhamija. Hash visualization in user authentication, 2000. http://citeseer.ist.psu.edu/dhamija00hash
18. Rachna Dhamija and Adrian Perrig. Deja vu: A user study using images for authentication. In Proceedings of the 9th USENIX Security Symposium, 2000. http://citeseer.ist.psu.edu/326534.html
19. Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication, 2003. http://www.research.avayalabs.com/user/logorman/compareAuthent.pdf
20. Chiara Braghi. Biometric authentication. http://citeseer.ist.psu.edu/436492.html

21. Richard E. Smith. Authentication: From Passwords to Public Keys. Addison-Wesley Pub Co, 2001.
22. Ruud Bolle Anil Jain and Sharath Pankanti, editors. Biometric, Personal Identification in Networked Society. The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, 1998.
23. Dirk Scheuermann Ulrich Waldmann and Claudia Eckert. Protected transmission of biometric user authentication data for on card-matching. 2004, http://www.sit.fhg.de/ZAVIR/WSE04.pdf
24. Bruno Struif. Use of biometrics for user verification in electronic signature smart- cards. 2001 http://www.sit.fhg.de/ZAVIR/str01.pdf ,.
25. A Secure Method for Signing In Using Quick Response Codes With Mobile Authentication - Kalpesh Adhatrao, Aditya Gaykar, Rohit Jha, Vipul Honrao - Department of Computer Engineering, Fr. C.R.I.T., Vashi, Navi Mumbai, India
26. http://en.wikipedia.org/wiki/Location-based_authentication
27. http://www.marketwired.com/press-release/soha-systems-survey-reveals-only-two-percent-it-experts-consider-third-party-secure-2125559.htm
28. M.M. Mohammed, Dr. M. Elsadig, " A Multi-layer of Multi Factors Authentication Model for Online Banking Services" . 2013 International Conference on Computing and Electronic Engineering (ICCEEE) .978-1-4673-6232-0/13/2013 IEEE
29. Neha; Chatterjee, K. Authentication techniques for e-commerce applications: A review. In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 693–698.
30. Fan, K.; Ge, N.; Gong, Y.; Li, H.; Su, R.; Yang, Y. An ultra -lightweight RFID authentication scheme for mobile commerce. Peer-to-Peer Netw. Appl. 2017, 10, 368–376. 51. Nor, N.A.; Narayana Samy, G.; Ahmad, R.; Ibrahim, R.; Maarop, N. The Proposed Public Key Infrastructure

31. Authentication Framework (PKIAF) for Malaysian Government Agencies. Adv. Sci. Lett. 2015, 21, 3161–3164.52. Labati, R.D.; Genovese, A.; Muñoz, E.; Piuri, V.; Scotti, F.; Sforza, G. Biometric recognition in automated border control: A survey. ACM Comput. Surv. (CSUR) 2016.
32. Grigoras, C. Applications of ENF analysis in forensic authentication of digital audio and video recordings. J. Audio Eng. Soc. 2009, 57, 643–661. 54. Gill, P.; Jeffreys, A.J.;Werrett, D.J. Forensic application of DNA 'fingerprints'. Nature 1985, 318, 577–579.
33. Han, K.; Potluri, S.D.; Shin, K.G. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. In Proceedings of the International Conference on Cyber-Physical Systems (ICCPS), Philadelphia, PA, USA, 8–11 April 2013; pp. 160–169.
34. Ishtiaq Roufa, R.M.; Mustafaa, H.; Travis Taylora, S.O.; Xua, W.; Gruteserb, M.; Trappeb, W.; Seskarb, I. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In Proceedings of the 19th USENIX Security Symposium, Washington, DC, USA, 11–13 August 2010; pp. 11–13.
35. Chaurasia, B.K.; Verma, S. Infrastructure based authentication in VANETs. Int. J. Multimed. Ubiquitous Eng. 2011, 6, 41–54.
36. Rossi, B. Connected car security: why identity should be in the driving seat. 2016. http://www.information-age.com/connected-car-security-why-identity-should-be-driving-seat
37. A Review on Authentication Methods - Syed Zulkarnain Syed Idrus1,2, Estelle Cherrier2, Christophe Rosenberger2,and Jean-Jacques Schwartzmann-University Malaysia Perlis, 01000 Kangar, Perlis, Malaysia.
38. Article:Multi-Factor Authentication: A Survey. By Aleksandr Ometov 1, Sergey Bezzateev,Niko Mäkitalo, Sergey Andreev,Tommi Mikkonen and Yevgeni Koucheryavy.

39. Robert Stocker. Applying usability testing and techniques to develop user centered security 2000 http://eies.njit.edu/~turoff/coursenotes/CIS732/samplepro/testing_and_security.htm
40. Von Zezschwitz, E.; De Luca, A.; Hussmann, H. Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, Helsinki, Finland, 26–30 October 2014
41. De Luca, A.; Hang, A.; Von Zezschwitz, E.; Hussmann, H. I Feel Like I'm Taking Selfies All Day!:Towards Understanding Biometric Authentication on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015 New York, NY, USA, 2015; pp. 1411–1414.
42. R. W. Reeder, C.-M. Karat, J. Karat, and C. Brodie, Usability challenges in security and privacy policy-authoring interfaces, in Human-Computer Interaction–INTERACT 2007, Springer. p. 141-155. doi:10.1007/978-3-540-74800-7_11.
43. S. Möller, N. Ben-Asher, K.-P. Engelbrecht, R. Englert and J. Meyer, "Modeling the behavior of users who are confronted with security mechanisms, " Computers & Security, vol. 30, pp. 242-256, 2011. http://dx.doi.org/10.1016/j.cose.2011.01.001
44. L. F. Cranor and N. Buchler, "Better together: Usability and security go hand in hand" IEEE Security & Privacy, pp. 89-93, 2014.
45. T. Fischer, A.-R. Sadeghi, and M. Winandy, "A pattern for secure graphical user interface systems," vol. pp. 186-190, 2009. doi:10.1109/DEXA.2009.76
46. M. Mihajlov, B. Jerman-Blazic, and S. Josimovski, "A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives," pp. 332-336, 2011. doi: 10.1109/ICNSS.2011.6060025.

47. D. Reed and A. Monk, "Inclusive design: beyond capabilities towards context of use," Universal Access in the Information Society, vol. 10, pp. 295-305, 2011. doi: 10.1007/s10209-010-0206-8
48. Mieczakowski, P. Langdon, and P. J. Clarkson, "Investigating designers‟ and users‟ cognitive representations of products to assist inclusive interaction design," Universal access in the information society, vol. 12, pp. 279-296, 2013. doi: 10.1007/s10209-012-0278-8.
49. Usability measurement and metrics:A consolidated model / Ahmed Seffah/ ·Mohammad Donyaee · Rex B. Kline/Harkirat K. Padda.
50. https://en.wikipedia.org/wiki/Steve_Gibson_(computer_programmer)
51. A closer look at SQRL,Jos van Dijk,University of Amsterdam,Faculty of Science,Informatics Institute,System & Network Engineering,February 9, 2014.master