Πανεπιστήμιο Πειραιά

Τμήμα Ψηφιακών Συστημάτων

Αυθεντικοποίηση με τη χρήση των προτύπων FIDO

Χαβατζόπουλος Παρασκευάς Μάριος MTE1231

Επιτηρητής: Ξενάκης Χρήστος,
Επίκουρος Καθηγητής,
Πανεπιστήμιο Πειραιά

Κενή σελίδα

Πίνακας περιεχομένων

Abstract

The society now has an existence in the electronic world. Each of us has an electronic identity, making people dependent on services offered online. This makes the security of these services critical and necessary to ensure that the service user is the one who says that is and not someone else.

Nowadays, users authenticate themselves using a variety of methods. The most common of all is the simple introduction of a password, which is far the most unsafe one. In principle, users store passwords properly with the simplest example to record it in a paper. Nor providers manage their passwords right after many of them do not even use a simple hash algorithm before storing it.

In addition to the problem of wrong storing of the password, there is the problem of the huge volume of users and an equally large number of services that makes it difficult to manage the online authentication. In 2007, the average user had 25 accounts, using 6.5 code and made 8 inputs the day. These numbers give us the opportunity to realize the number of authentications now and how difficult is the situation. In addition, simple methods of attack, such as phishing, fraud and exploitation of vulnerabilities (weaknesses in systems, but the word is used as such as mentioned throughout the literature) have even results.

Last and most important is the fact that the current networks carry large volume of sensitive information which require greater protection, especially regarding corporate environments.

As a result of all the above, it arises the need to start the authentication of the identity of someone which is unique to him and can be verified in the real world. In order to prevent deception and protection of any service by malicious users, there is a range of methods and technologies used, which includes biometrics (such as fingerprints, impressions iris, voice recognition and facial) and communication standards and existing technologies (USB security tokens, smartcards, Near Field Communication and embedded Secure Elements). There is a new standard called FiDO involving these methods. It separates the authentication method from the authentication protocol, defines the method in order to demonstrate the type of authentication of the interested party.

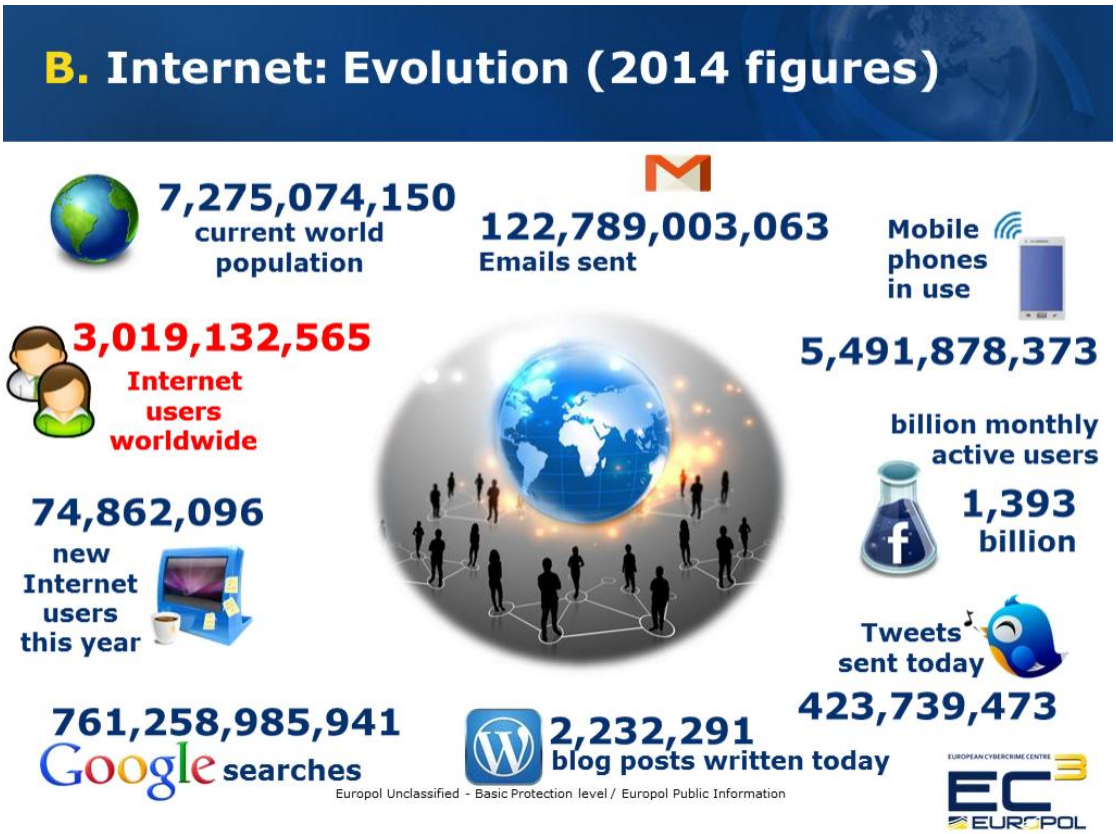
The FIDO (Fast IDentity Online) meets the online authentication. The use FIDO devices offers the user the option to replace passwords with one authentication method is more safe, easier to use with biometrics as well as existing methods of authentication and communications protocols such as USB security tokens and one time passwords.

This paper refers to existing authentication technologies that are incorporated in the specification of FiDO and similar advantages and disadvantages. In addition, there will be a hint to the possible application of FiDO in military environments, as well as in the public services.

Εισαγωγή

Η κοινωνία πλέον έχει υπόσταση στον ηλεκτρονικό κόσμο. Ο καθένας από εμάς διαθέτει μία ηλεκτρονική ταυτότητα, κάνοντας τους ανθρώπους εξαρτημένους σε υπηρεσίες που προσφέρονται μέσω διαδικτύου. Αυτό καθιστά την ασφάλεια αυτών των υπηρεσιών κρίσιμη και είναι απαραίτητο να διασφαλιστεί ότι ο χρήστης της υπηρεσίας είναι αυτός που δηλώνει ότι είναι και όχι κάποιος άλλος.

Τη σήμερον ημέρα, χρήστες αυθεντικοποιούνται με μία ποικιλία μεθόδων. Η πιο κοινή όλων είναι η απλή εισαγωγή ενός κωδικού, το οποίο είναι και εξ αρχής μη ασφαλές. Κατ' αρχήν οι χρήστες δεν αποθηκεύουν τους κωδικούς κατάλληλα με το



πιο απλό παράδειγμα την εγγραφή αυτού σε ένα χαρτί. Αλλά ούτε και οι πάροχοι διαχειρίζονται σωστά τους κωδικούς, αφού πολλοί από αυτούς δεν κάνουν καν χρήση ενός απλού hash αλγόριθμου πριν την αποθήκευσή του.

Εκτός από το πρόβλημα που έγκειται στην αποθήκευση του κωδικού, υπάρχει και το πρόβλημα του τεράστιου πλέον όγκου χρηστών και έναν εξίσου πολύ μεγάλο αριθμό υπηρεσιών το οποίο καθιστά δύσκολη τη διαχείριση της online αυθεντικοποίησης. Το 2007, ο μέσος χρήστης είχε 25 λογαριασμούς, χρησιμοποιούσε 6.5 κωδικούς και έκανε 8 εισόδους την μέρα. Αυτοί οι αριθμοί μας δίνουν την

δυνατότητα να αντιληφθούμε τον αριθμό των αυθεντικοποιήσεων που πλέον γίνονται και πόσο δυσκολεύει την κατάσταση. Επιπλέον, απλές μέθοδοι επίθεσης, όπως phishing, απάτη και εκμετάλλευση vulnerabilities (αδυναμίες συστημάτων, αλλά χρησιμοποιείται αυτούσια η λέξη όπως αναφέρεται σε όλη την βιβλιογραφία) έχουν ακόμα αποτελέσματα.

Τελευταίο και πιο σημαντικό είναι το γεγονός ότι στα σημερινά δίκτυα διακινείται όγκος ευαίσθητων πληροφοριών που απαιτούν μεγαλύτερη προστασία, ειδικά ότι αφορά εταιρικά περιβάλλοντα.

Σαν αποτέλεσμα όλων των παραπάνω, διαφαίνεται η ανάγκη να αρχίσει η αυθεντικοποίηση της ταυτότητας κάποιου που είναι μοναδική σε αυτόν και μπορεί να επαληθευτεί στον πραγματικό κόσμο. Με στόχο την αποφυγή της εξαπάτησης και την προστασία της όποιας υπηρεσίας από κακόβουλους χρήστες, υπάρχει ένα εύρος μεθόδων και τεχνολογιών που χρησιμοποιούνται, το οποίο περιλαμβάνει βιομετρικά στοιχεία (όπως δαχτυλικά αποτυπώματα, αποτυπώσεις της ίριδας, αναγνώριση φωνής και προσώπου) αλλά και πρότυπα επικοινωνιών και υπάρχουσες τεχνολογίες (USB security tokens, έξυπνες κάρτες, Near Field Communication και embedded Secure Elements). Σε αυτό το κομμάτι της αυθεντικοποίησης εμπλέκεται ένα νέο πρότυπο, το λεγόμενο FiDO το οποίο διαχωρίζει τη μέθοδο αυθεντικοποίησης από το πρωτόκολλο αυθεντικοποίησης και ορίζει την μέθοδο με σκοπό να αποδείξει τον τύπο αυθεντικοποίσης FiDO στον ενδιαφερόμενο μέρος.

Το FIDO (Fast IDentity Online) χρησιμοποιείται για να αντιμετωπίσει την online αυθεντικοποίηση. Χρησιμοποιεί FIDO συσκευές κα προσφέρει στον χρήστη την επιλογή να αντικαταστήσει κωδικούς με μία μέθοδο αυθεντικοποίησης που είναι πιο ασφαλής και ευκολότερη στη χρήση με την χρήση βιομετρικών στοιχείων καθώς επίσης και υπάρχουσες μεθόδους αυθεντικοποίησης και πρωτόκολλα επικοινωνιών, όπως USB security tokens και one time passwords.

Σε αυτή την εργασία γίνεται αναφορά στις υπάρχουσες τεχνολογίες αυθεντικοποίησης, πως αυτές ενσωματώνονται στις προδιαγραφές του FiDO και τα ανάλογα πλεονεκτήματα και μειονεκτήματα που παρουσιάζει. Επιπλέον, θα γίνει μία νύξη στην πιθανή εφαρμογή του FiDO σε στρατιωτικά περιβάλλοντα εργασίας.

Μέθοδοι αυθεντικοποίησης

Η αυθεντικοποίηση είναι η διαδικασία επαλήθευσης της ταυτότητας του εκάστοτε χρήστη που προσπαθεί να κάνει log in ή να αποκτήσει πρόσβαση σε πόρους κυρίως ώστε να απαγορευτεί η είσοδος στο σύστημα μη εγκεκριμένων χρηστών και να προφυλαχθούν οι πόροι. Αυτή η διαδικασία γίνεται με την σύγκριση της υποβεβλημένης διαπίστευσης προς τα ήδη καταχωρημένα. Αυτό μπορεί να περιέχει την επιβεβαίωση αυτού που γνωρίζει ο χρήστης (πχ κωδικός), ή αυτό που ο χρήστης έχει (πχ OTP token) ή αυτό που ο χρήστης είναι (πχ δαχτυλικό αποτύπωμα). Όσο περισσότεροι οι παράγοντες που ελέγχονται τόσο μεγαλύτερη η εμπιστοσύνη που μπορεί να εγκαθιδρυθεί. Είναι κρίσιμη για την ασφάλεια κάθε συστήματος.

Η ηλεκτρονική αυθεντικοποίηση αποτελείται από δύο διαδικασίες, την εγγραφή και την αυθεντικοποίηση.

Η μέθοδος εγγραφής έχει τη μέθοδο εγγραφής και ανάκλησης. Η εγγραφή είναι για να εξασφαλιστεί ότι όντως υπάρχει ο χρήστης και ότι είναι αυτός που λέει ότι είναι. Επίσης για να είναι σίγουρο ότι οι πληροφορίες που συνδέονται με τον χρήστη συνάδουν και είναι ακριβείς και καταγεγραμμένες ώστε να μπορέσει να εκδοθεί και ένα διαπιστευτήριο του χρήστη. Η ανάκληση συμβαίνει για να ανακληθεί κάποιο διαπιστευτήριο ή για να αντικατασταθεί όπου είναι απαραίτητο. Επίσης, χρησιμοποιείται στις περιπτώσεις αναστολής κάποιου διαπιστευτηρίου που υπάρχει υποψία παραποίησης, κλοπής ή σημαντικής αλλαγής και στην περίπτωση που αυτό ζητηθεί από τον χρήστη.

Η μέθοδος αυθεντικοποίησης είναι η διαδικασία για να αναγνωριστεί ο χρήστης και να αποδειχθεί η ταυτότητά αυτού που προσπαθεί να αποκτήση πρόσβαση. Σκοπός είναι να ελεγχθούν τα διαπιστευτήρια ότι είναι έγκυρα και ότι δεν έχουν λήξει ή ανακληθεί.

Υπάρχουν πολλοί φυσικοί τρόποι με τους οποίους μπορεί κάποιος να δώσει τα διαπιστευτήριά του στο σύστημα. Μερικές από αυτές τις μεθόδους παρουσιάζονται παρακάτω με στόχο να καταλάβει ο αναγνώστης καλύτερα τη διαδικασία αυθεντικοποίησης και πως το FIDO αλληλεπιδρά με κάθε ένα.

Μέθοδος Αυθεντικοποίησης	Επίπεδο Ασφαλείας	Τρόπος διανομής	Περιγραφή
Κωδικός	Επίπεδο 1-2 Εξαρτάται από πολιτική που χρησιμοποιείται.	Διαλέγεται από τον χρήστη	Καμία ή μικρή εμπιστοσύνη στην υποστηριζόμενη εγκυρότητα. Απαιτείται όταν δεν υπάρχει κίνδυνος ή είναι πολύ μικρός κίνδυνος έκθεσης
Συμμετρικό κλειδί / OTP token	Επίπεδο 3-4 Απαιτείται φυσικό token για το επίπεδο 4	Μέσω email ή παραλαβή από φυσικό πρόσωπο	Μέτρια εμπιστοσύνη στην υποστηριζόμενη εγκυρότητα. Απαιτείται όταν είναι μικρός κίνδυνος έκθεσης
Δημόσιο κλειδί	Επίπεδο 3-4 Απαιτείται φυσικό token για το επίπεδο 4	Μέσω email ή παραλαβή από φυσικό πρόσωπο	Υψηλή εμπιστοσύνη στην υποστηριζόμενη εγκυρότητα. Απαιτείται όταν είναι μέτριος ο κίνδυνος έκθεσης
Βιομετρικά	Επίπεδο 1-4 Εξαρτάται από το επίπεδο ασφαλείας του βιομετρικού αισθητήρα	Βιομετρικά στοιχεία ατόμου	Πολύ υψηλή εμπιστοσύνη στην υποστηριζόμενη εγκυρότητα. Απαιτείται όταν είναι ψηλός ο κίνδυνος έκθεσης

Password

Οι κωδικοί είναι η πιο διαδεδομένη μορφή αυθεντικοποίησης. Οι χρήστες δίνουν ένα αναγνωριστικό, το οποίο μπορεί να είναι μία λέξη, μία φράση ή ένα token μαζί με ένα κωδικό. Στα περισσότερα συστήματα αυτός ο κωδικός φυλάσσεται κωδικοποιήμενος και όχι σαν απλό κείμενο.

Αυτή η μέθοδος δεν απαιτεί εξειδικευμένα ή δυναμικά συστήματα hardware καθώς η αυθεντικοποίηση είναι γενικά απλή και δεν απαιτεί μεγάλη υπολογιστική ισχύ. Αλλά η μέθοδος αυτή παρουσιάζει μειονεκτήματα. Οι κωδικοί μπορεί να μαντευθούν ή οι χρήστες τηρούν εγγράφως σε εμφανές σημείο τον κωδικό για να μην τον ξεχάσουν είτε ο κωδικός μπορεί να ανακαλυφθεί μέσω κοινωνικών δικτύων αν ο χρήστης έχει χρησιμοποιήσει κάτι που μπορεί εύκολα να θυμάται ή συνδέεται άμεσα με αυτόν. Οι κωδικοί δεν μπορούν να υποκλαπούν με eavesdropping γιατί κατά κύριο λόγο χρησιμοποιούνται τεχνικές hash.

Πλεονεκτήματα – Μειονεκτήματα κωδικών

Τα πλεονεκτήματα της χρήσης κωδικών είναι τα εξής:

- Κάθε εφαρμογή μπορεί να έχει τον κωδικό που επιθυμεί ο χρήστης και εύκολα θα θυμάται.
- Είναι η πιο εύκολη και φθηνή λύση αυθεντικοποίησης για μεγάλους αριθμούς χρηστών.

Ενώ τα μειονεκτήματα της χρήσης κωδικών είναι τα κάτωθι:

- Ο χρήστης μπορεί να ξεχάσει τον κωδικό του. Δημιουργεί καινούργιο λογαριασμό με αποτέλεσμα πληθώρα άχρηστων λογαριασμών.

- Οι απλοί κωδικοί εύκολα μπορούν να σπάσουν, ενώ υπάρχει πληθώρα άλλων επιθέσεων για την υποκλοπή ακόμα και των πιο δύσκολων κωδικών.
- Πολλοί ιστότοποι απαιτούν την συχνή αλλαγή κωδικού.
- Δεν είναι ιδιαίτερα εύκολη η πληκτρολόγηση κωδικών σε κινητά τηλέφωνα.
- Οι κωδικοί μπορεί να πληκτρολογηθούν σε κακόβουλους ιστότοπους.

Βιομετρικά

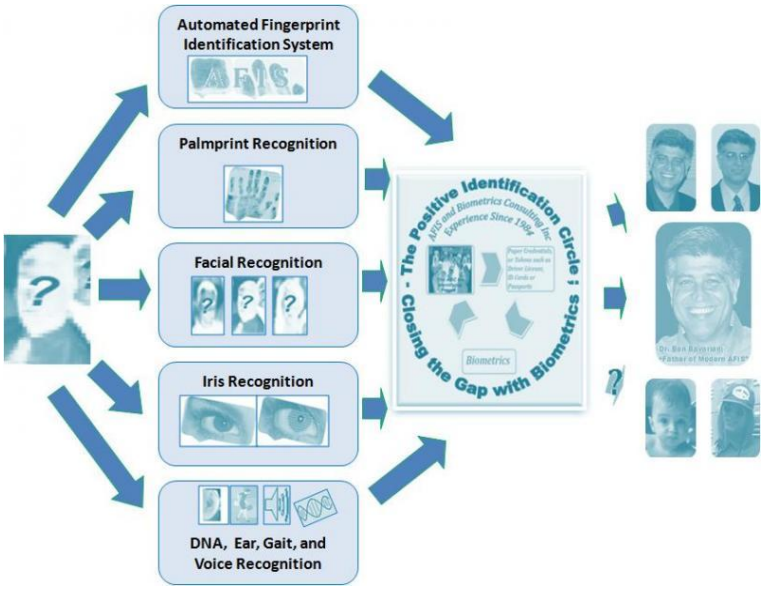
Τα βιομετρικά αναφέρονται σε μετρήσεις που σχετίζονται με τα ανθρώπινα χαρακτηριστικά και γνωρίσματα. Χρησιμοποιούνται για ταυτοποίηση και σαν διαδικασία ελέγχου(αυτοματοποιημένη αναγνώριση). Τα βιομετρικά αναγνωριστικά είναι τα διακριτικά και μετρήσιμα χαρακτηριστικά που χρησιμοποιούνται για να περιγράψουν και να ξεχωρίσουν ένα άτομο. Αυτά τα αναγνωριστικά κατηγοριοποιούνται σε φυσιολογικά/ανατομικά (physiological/anatomical) χαρακτηριστικά και χαρακτηριστικά συμπεριφοράς (behavioral). Τα φυσιολογικά χαρακτηριστικά σχετίζονται με το σχήμα του σώματος και τέτοια είναι η αναγνώριση προσώπου, το δακτυλικό αποτύπωμα και η γεωμετρία του χεριού. Τα χαρακτηριστικά συμπεριφοράς σχετίζονται με πρότυπο την συμπεριφορά ενός ατόμου, όπως είναι ο ρυθμός δαχτυλογράφησης ή η φωνή του.

Σαν αποτέλεσμα πολλοί τομείς της ανθρώπινης φυσιολογίας και συμπεριφοράς, μπορούν να χρησιμοποιηθούν για βιομετρική αυθεντικοποίηση. Οι βασικοί παράγοντες για την επιλογή ενός βιομετρικού στοιχείου ως μέσο αυθεντικοποίησης είναι η καθολικότητα (universality), ώστε κάθε άτομο να έχει αυτό το χαρακτηριστικό και να είναι μοναδικό (uniqueness) για κάθε άτομο και σταθερό στη πάροδο του χρόνου (permanence). Επίσης, πρέπει να χαρακτηρίζεται από την ικανότητα μέτρησής του (measurability), την απόδοση της τεχνολογίας (performance), όπως και την αποδοχή από τους χρήστες, για τη χρήση αυτού του βιομετρικού (acceptability). Τέλος, ο παράγοντας αυτός να προσφέρει αδυναμία παράκαμψής του με κάποιο υποκατάστατο μέσο (circumvention).

Ένα τυπικό βιομετρικό σύστημα αποτελείται από πέντε ενσωματωμένα στοιχεία. Έναν αισθητήρα που χρησιμοποιείται για συλλογή δεδομένων και μετατρέπει τη πληροφορία σε ψηφιακή. Απαιτείται επίσης μία αποθηκευτική μονάδα που θα διατηρεί τα δεδομένα και με τα οποία θα συγκρίνονται τα νέα ληφθέντα βιομετρικά στοιχεία. Επιπλέον, χρειάζεται ένας αλγόριθμος επεξεργασίας σήματος για να κάνει έλεγχο ποιότητας και να δημιουργεί το βιομετρικό template, ένας αλγόριθμος για την ταύτιση των βιομετρικών στοιχείων με τα υπάρχοντα templates

και ένας αλγόριθμός που θα αποφασίζει βάσει της ταύτισης, είτε αυτός είναι αυτοματοποιημένος είτε είναι υποβοηθούμενος από άνθρωπο.

Πρέπει να γίνει αποσαφήνιση των όρων αναγνώριση (recognition), ταυτοποίηση (identification) και αυθεντικοποίηση (verification). Αναγνώριση είναι ένας γενικός ορισμός που είτε υπονοεί ταυτοποίηση είτε αυθεντικοποίηση. Αυθεντικοποίηση είναι η διαδικασία κατά την οποία ένα σύστημα προσπαθεί αν επιβεβαιώσει την ταυτότητα κάποιου ατόμου συγκρίνοντας το ληφθέν στοιχείο με αυτό που υπάρχει ήδη στη βάση. Ταυτοποίηση είναι η διαδικασία κατά την οποία ένα βιομετρικό σύστημα προσπαθεί να καθορίσει την ταυτότητα ένας ατόμου. Ένα βιομετρικό στοιχείο συλλέγεται και μετά συγκρίνεται με όλα τα υπάρχοντα δείγματα στη βάση.



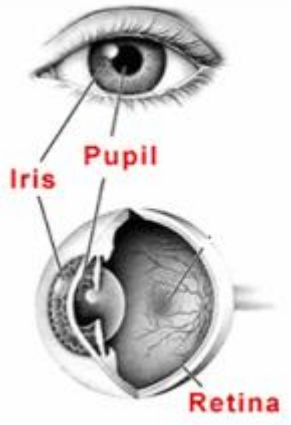
Υπάρχουν πολλές τεχνολογίες αυθεντικοποίησης με βιομετρικά στοιχεία. Αυτές οι τεχνολογίες είναι αναγνώριση με αποτύπωμα (fingerprint recognition), με ίριδα (iris recognition), γεωμετρία παλάμης (hand geometry), αναγνώριση με πρότυπο φλέβας (vascular pattern recognition), δυναμικής υπογραφής (dynamic signature), αναγνώριση προσώπου (face recognition), φωνής (voice recognition) και αποτύπωμα παλάμης (palm print recognition).

Fingerprint Recongition

Η αναγνώριση με χρήση δακτυλικού αποτυπώματος είναι η πιο διαδεδομένη μέθοδος χρήσης βιομετρικών στοιχείων. Είναι πολύ εύκολη η ανάκτησή τους, καθ'όσον υπάρχει σύνολο πηγών από τα οποία μπορούν να ανακτηθούν (το σύνολο των 10 δαχτύλων) και παράλληλα είναι μοναδικά για κάθε άτομο.

Η πληροφορία που μπορεί να συλλεχθεί από ένα αποτύπωμα χωρίζεται σε τρία επίπεδα. Το πρώτο επίπεδο περιλαμβάνει τη ροή της παρυφής του αποτυπώματος(flow of the friction ridges). Στο επόμενο επίπεδο εξετάζονται η παρουσία ή απουσία χαρακτηριστικών κατά μήκος των μονοπατιών των επιμέρους μονοπατιών των friction ridges και των διακλαδώσεών τους. Τέλος, ελέγχεται η ιδιαίτερη λεπτομέρεια μίας συγκεκριμένης παρυφής αποτυπώματος.

Iris Recognition



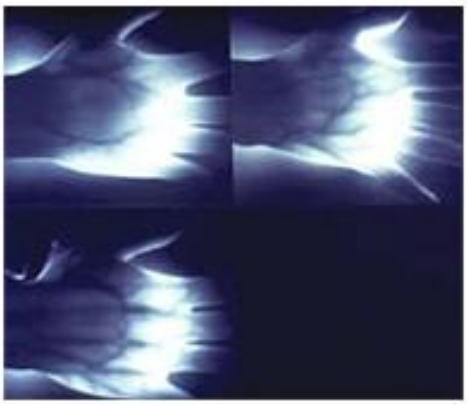
Είναι η διαδικασία αναγνώρισης ενός ατόμου με την ανάλυση των τυχαίων μοτίβων που υπάρχουν στην ίριδα, η οποία είναι το χρωματισμένο τμήμα του ματιού ενός ατόμου. Η ίριδα είναι μοναδική κατά άτομο και κατασκευαστικά ξεχωριστή, το οποίο την καθιστά κατάλληλη για αναγνώριση. Χρησιμοποιείται υπέρυθρο φως για να φωτίσει την ίριδα χωρίς να προκαλέσει ζημιά ή δυσαρέσεια στο άτομο.

Υπάρχει και η δυνατότητα αναγνώρισης της ρέτινας, το οποίο χρησιμοποιεί τα μοναδικά pattern των φλεβών της ρέτινας στο πίσω μέρος του ματιού.

Hand/Finger Geometry

Στη μέτρηση αυτή γίνεται απλή μέτρηση του μήκους, του πλάτους, του πάχους και της επιφανείας της παλάμης του ατόμου. Δυστυχώς δεν είναι ιδιαίτερα μοναδικό και μπορεί να χρησιμοποιηθεί μόνο για επαλήθευση.

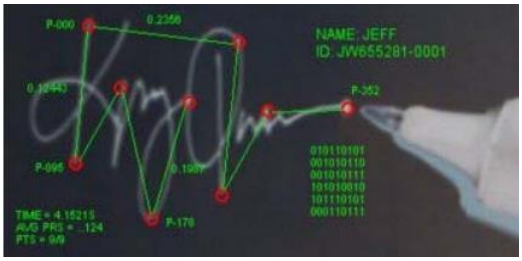
Vascular Pattern Recognition



Έχει καθοριστεί ότι η pattern των αρτηριών είναι μοναδική για κάθε άτομο και δεν αλλάζει με την ηλικία. Γίνεται χρήση σχεδόν υπέρυθρου φωτός και λαμβάνεται η ανακλώμενη εικόνα των αρτηριών της παλάμης ή ενός δαχτύλου. Είναι πολύ καλή μέθοδος γιατί είναι σχετικά δύσκολο να αντιγραφεί και δεν απαιτεί επαφή.

Dynamic Signature

Η δυναμική υπογραφή χρησιμοποιεί για την αναγνώριση στα ανατομικά χαρακτηριστικά και χαρακτηριστικά συμπεριφοράς, που εμφανίζονται όταν κάποιος υπογράφει.



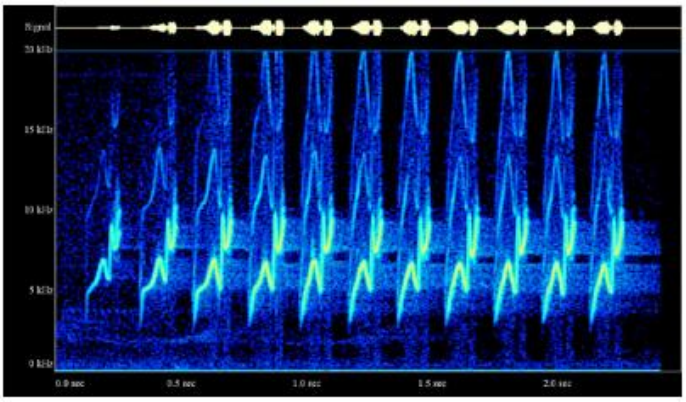
Τα περισσότερα στοιχεία που χρησιμοποιεί είναι δυναμικά χαρακτηριστικά παρά στατικά και γεωμετρικά χαρακτηριστικά. Τα συνήθη δυναμικά στοιχεία είναι η ταχύτητα και η επιτάχυνση γραφής, η πίεση, ο συγχρονισμός και η κατεύθυνση της υπογραφής. Αυτά τα χαρακτηριστικά είναι σχεδόν αδύνατο να αντιγραφούν, καθώς τα δυναμικά χαρακτηριστικά είναι πολύπλοκα και μοναδικά για κάθε άτομο.

Face Recognition

Ο συγκεκριμένος τρόπος αναγνώρισης χρησιμοποιεί μία εικόνα της φυσικής κατασκευής του προσώπου του χρήστη. Για την αναγνώριση προσώπου πλέον υπάρχουν τρεις διαδεδομένες μέθοδοι, η PCA, η LDA και η EBGM. Το PCA (Principal Components Analysis).

Voice Recognition (Speaker Recognition)

Η συγκεκριμένη τεχνική αξιοποιεί μία βιομετρική τυπικότητα (biometric modality). Βασίζεται σε χαρακτηριστικά που επηρεάζονται επιπρόσθετα από τη φυσική δομή των φωνητικών χορδών και τα χαρακτηριστικά συμπεριφοράς ενός ατόμου. Διαφέρει από το speech recognition ,στο οποίο γίνεται απλή αναγνώριση της άρθρωσης μιας συγκεκριμένης λέξης.

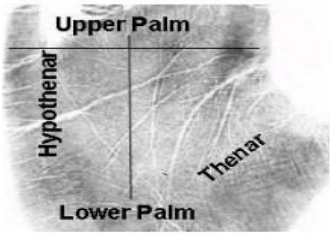


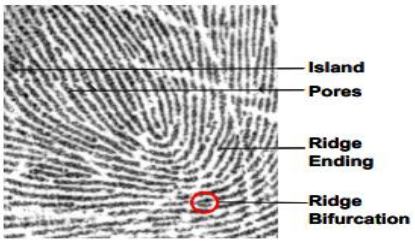
Είναι διαφορετικός από άλλους τρόπους βιομετρικής πιστοποίησης αφού τα δείγματα φωνής λαμβάνονται δυναμικά ή για ένα συγκεκριμένο χρονικό διάστημα. Δηλαδή, η ανάλυση γίνεται σε ένα μοντέλο στο οποίο παρατηρούνται οι αλλαγές στη διάρκεια του χρόνου.

Υπάρχουν δύο τρόποι αναγνώρισης, είτε να εξαρτάται από το κείμενο είτε να μην εξαρτάται καθόλου από αυτό. Στη πρώτη περίπτωση, ο χρήστης είτε δίνει συγκεκριμένη κωδική λέξη είτε λέει μία λέξη που του ζητάει το σύστημα. Η δεύτερη περίπτωση είναι πολύ πιο ευέλικτη αν και το σύστημα δεν διαθέτει καμία πρότερη γνώση.

Palm Print Recognition

Η παλαμική αναγνώριση μοιάζει πολύ με την αναγνώριση του δαχτυλικού αποτυπώματος, καθώς και τα δύο είναι μοναδικά και δεν αλλάζουν με τον χρόνο. Εστιάζει στις κορυφογραμμές τριβής. Συγκεκριμένα ασχολείται με την ροή της κορυφογραμμής, τα χαρακτηριστικά της και τη δομή της ανυψωμένης περιοχής του δέρματος.Η αναγνώριση του αποτυπώματος των κορυφογραμμών τρίβης γίνεται σε τρία επίπεδα. Στο πρώτο επίπεδο είναι η ροή του αποτυπώματος, στο δεύτερο περιλαμβάνεται η παρουσία ή απουσία ιδιαίτερων χαρακτηριστικών και τέλος ελέγχεται ιδιαίτερη λεπτομέρεια μίας συγκεκριμένης αποτύπωσης.





Άλλες μέθοδοι βιομετρικών

Άλλες μέθοδοι βιομετρικών στοιχείων είναι η αναγνώριση δυναμικής πληκτρολόγησης, η οποία ελέγχει το μοτίβο πληκτρολόγησης, η αναγνώριση βαδίσματος στην οποία ελέγχεται ο τρόπος βαδίσμαος κάποιου και η θερμογραφία προσώπου που ελέγχεται η θερμότητα που αναδίδει το πρόσωπο κάποιου.

Πλεονεκτήματα – Μειονεκτήματα Βιομετρικών

Τα πλεονεκτήματα των βιομετρικών στοιχείων είναι:

- Τα βιομετρικά χαρακτηριστικά δεν μπορούν να απολεσθούν, να χαθούν ή να κλαπούν.
- Τα βιομετρικά χαρακτηριστικά παραμένουν σχεδόν ανέπαφα στον χρόνο.
- Δεν είναι κάτι που μπορεί να υποκλαπεί με social engineering, ή να μοιραστεί.
- Δεν απαιτεί από τον χρήστη να θυμάται κωδικούς.
- Είναι συνέχεια διαθέσιμο προς χρήση.
- Προσφέρει υψηλό βαθμό εμπιστοσύνης ως προς την ταυτότητα του χρήστη.

Παρά τα πολλά πλεονεκτήματα εξακολουθεί να έχει και μειονεκτήματα:

- Έλλειψη προτυποποίησης
- Η αξιοπιστία και η ακρίβεια των βιομετρικών επιδέχεται βελτίωσης
- Τα βιομετρικά συστήματα πρέπει να μπορούν να υποστηρίζουν αλλαγές στο βιομετρικό χαρακτηριστικό αφού δεν παραμένει σταθερό.
- Η αποτελεσματικότητα της λήψης του βιομετρικού στοιχείου επηρεάζεται ιδιαίτερα από τις περιβαλλοντικές συνθήκες, την εκπαίδευση του χρήστη και την χρηστικότητα.

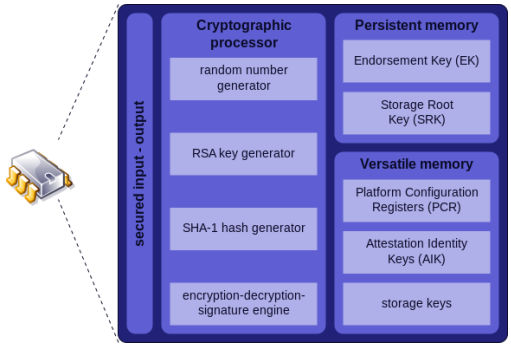
Άλλες Μέθοδοι

USB Security Tokens/ Keys

Τα USB token είναι ηλεκτρονικές συσκευές που εξωτερικά μοιάζουν με μνήμη USB Flash, είναι όμως ειδικές συσκευές όπου αποθηκεύονται με ασφάλεια τα ψηφιακά πιστοποιητικά. Η επίσημη ονομασία αυτών των συσκευών στα ελληνικά είναι ΑΔΔΥ (Ασφαλής Διάταξη Δημιουργίας Υπογραφής).

TPM

Το Trusted Platform Module (TPM) είναι ένα διεθνές πρότυπο για ασφαλή cryptoprocessor, ο οποίος είναι ένας ειδικός μικροεπεξεργαστής με σκοπό την εξασφάλιση του υλικού με την ενσωμάτωση κλειδιών κρυπτογράφησης σε συσκευές. Η πλατφόρμα προσφέρει δυνατότητα για ασφαλή παραγωγή κλειδιών κρυπτογράφησης και τον περιορισμό της χρήσης τους. Περιλαμβάνει επίσης δυνατότητες όπως απομακρυσμένη βεβαίωση και σφραγισμένη αποθήκευση.

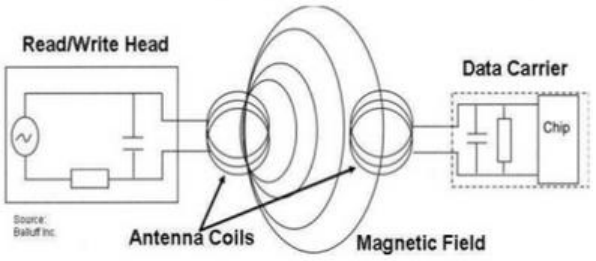


Η Απομακρυσμένη Βεβαίωση δημιουργεί ένα hash της διαμόρφωσης του υλικού και του λογισμικού. Αυτό επιτρέπει σε τρίτους να βεβαιωθούν ότι το λογισμικό δεν έχει αλλάξει. Η Δέσμευση κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το κλειδί TPM (ένα μοναδικό κλειδί RSA το οποίο παράγεται από ένα κλειδί αποθήκευσης). Η Σφράγιση κρυπτογραφεί τα δεδομένα με παρόμοιο τρόπο, αλλά επιπλέον καθορίζει την κατάσταση, στην οποία το TPM πρέπει να είναι εντάξει για τα στοιχεία που πρέπει να αποκρυπτογραφήσει. Το λογισμικό μπορεί να χρησιμοποιήσει μια μονάδα Trusted Platform Module για την επικύρωση συσκευών. Δεδομένου ότι κάθε μονάδα TPM έχει ένα μοναδικό και μυστικό κλειδί RSA που καίγεται καθώς παράγεται, είναι ικανό να εκτελεί αυθεντικοποίηση πλατφόρμας.

NFC

Το NFC είναι μία τεχνολογία μικρής εμβέλειας που χρησιμοποιεί ασύρματη επικοινωνία μεγάλης συχνότητας. Είναι προέκταση του RFID για κινητά τηλέφωνα

και συσκευές χειρός. Εγκαθιδρύεται μία ραδιοεπικοινωνία έχοντας τα δύο κινητά τηλέφωνα σε κοντινή απόσταση.



Βασίζεται στην μαγνητική επαγωγή μεταξύ δύο κυκλικών κεραιών. Λειτουργεί είτε παθητικά είτε ενεργητικά. Στην ενεργητική λειτουργία υπάρχουν δύο συσκευές με NFC που επικοινωνούν, ενώ στη παθητική λειτουργία υπάρχει μία ενεργή συσκευή ενώ η άλλη χρησιμοποιεί το πεδίο για να αποστείλει δεδομένα.

eSE

Το eSE (embedded Secure Element) είναι ένα απαραβίαστο τσιπ διαθέσιμο σε διάφορα μεγέθη και σχέδια, που είναι ενταγμένο σε οποιαδήποτε κινητή συσκευή. Διασφαλίζει τα δεδομένα αποθηκεύοντας τα σε ασφαλές μέρος και οι πληροφορίες δίνονται μόνο σε εγκεκριμένες εφαρμογές και ανθρώπους. Είναι σαν μια προσωπική ταυτότητα για τον τελικό χρήστη και για την ίδια τη συσκευή.

Πιθανές επιθέσεις

Επιθέσεις κατά την εγγραφή

Προσωποποίηση (impersonation)

Ο επιτιθέμενος προσπαθεί να αποκτήσει τα διαπιστευτήρια στη θέση κάποιου άλλου χρήστη.

Fictitious subscriber

Ο επιτιθέμενος υποστηρίζει ότι είναι κάποιος μη εγγεγραμμένος χρήστης με σκοπό να δημιουργήσει μία σχέση χρήσης του συστήματος.

Rogue registration entity

Μία εκ των έσω εκμετάλλευση κάποιας διαπιστευμένης θέσης για να δημιουργήσει ή να αποκτήσει διαπιστευτήρια σαν ένας πιθανός χρήστης ή ένας μη υπαρκτός χρήστης

Επιθέσεις κατά την αυθεντικοποίηση

Eavesdropper/replay attack

Ένας παρατηρητής των δεδομένων αυθεντικοποίησης στο δίκτυο για μετέπειτα ανάλυση ή υποκλοπή μηνυμάτων μεταξύ δύο διαπιστευμένων οντοτήτω ν. Αυτός ο παρατηρητής κάνει μία παράτυπη προσπάθεια να αποκτήσει τα tokens προσποιούμενος έναν χρήστη του συστήματος. Συχνά χρησιμοποιείται μαζί με replay attack, στο οποίο μία εκπομπή έγκυρων δεδομένων είναι κακόβουλη ή επαναλαμβάνεται απατηλά ή καθυστερείται.

Password guessing

Ο πιο συνήθης τρόπος απόκτησης ενός κωδικού που γίνεται με χρήση λεξικού.

Verifier impersonation

Ο επιτιθέμενος προσποιείται ότι είναι το σύστημα διαπίστευσης και προκαλεί τον χρήστη να του αποκαλύψει το μυστικό token.

Hijacker

Κάποιος που καταλαμβάνει ένα αυθεντικοποιημένο session και εμφανίζεται σαν τον αληθινό χρήστη ώστε να μάθει ευαίσθητα δεδομένα ή να εισάγει λανθασμένες πληροφορίες

Άλλες επιθέσεις

Phishing/Bogus website

Ο επιτιθέμενος χρησιμοποιεί email το οποίο φαίνεται ότι προήλθε από νόμιμο οργανισμό και ζητάει από το θύμα να παράσχει ευαίσθητες πληροφορίες όπως είναι ο κωδικός και το όνομα χρήστη ή προωθεί τον χρήστη σε ένα κάλπικο ιστότοπο για να εισάγει τα δεδομένα του.

Hacking

Ο επιτιθέμενος εκμεταλλεύεται τις ευπάθειες του συστήματος για να αποκτήσει πρόσβαση και να κλέψει δεδομένα.

Cross site scripting

Ο επιτιθέμενος εγκαθιστά κακόβουλο κώδικα σε νόμιμους ιστότοπους ώστε όταν μπει ο χρήστης να εκτελεστούν με στόχο να κλέψει ευαίσθητα δεδομένα ή να τον προωθήσει σε κάποιο κάλπικο ιστότοπο.

FIDO

Στις μέρες μας γίνεται όλο και μεγαλύτερη προσπάθεια για γρήγορη και ασφαλή αυθεντικοποίηση του χρήστη σε διάφορες υπηρεσίες του διαδικτύου. Πολλές εταιρίες προσπαθούν να επιλύσουν επιθέσεις στη διαπίστευση των χρηστών με ένα μεγάλο αριθμό συσκευών και τεχνικών (smart cards, hardware και software OTP συσκευές, one time SMS κωδικούς).

Ένας από τους τρόπους αυτούς είναι το FIDO. Το FIDO (Fast IDentity Online) πρόκειται για σύνολο προτύπων για την αυθεντικοποίηση ενός χρήστη. Είναι ανοικτό για όλους και δεν απαιτεί την συνδρομή τρίτων.

e-ID

Η ασφαλής ηλεκτρονική ταυτοποίηση (ηλεκτρονική ταυτότητα) είναι πολύ σημαντική για την προστασία δεδομένων και την αποτροπή της διαδικτυακής εξαπάτησης. Αυτά είναι απαραίτητα στοιχεία για την e-Διακυβέρνηση αλλά και το ηλεκτρονικό εμπόριο.

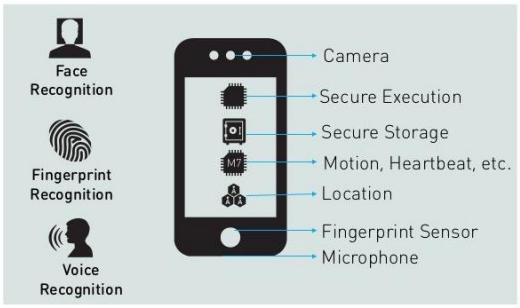
Fast IDentity Online

Στη προσπάθεια ενίσχυσης της ασφάλειας πρόσβασης, απλοποιεί προτείνοντας δύο διαφορετικά πρότυπα ανοικτά, ασφαλή και εύκολα στη χρήση, το UAF και το U2F. Και τα δύο πρότυπα χρησιμοποιούν κοινές τεχνικές αυθεντικοποίησης με τη διαφορά ότι το UAF είναι πρότυπο που χρησιμοποιεί βιομετρικά στοιχεία ενώ το U2F ένα συγκεκριμένο USB thumb drive.

FIDO Στόχοι

Για να αντιμετωπιστούν τα ζητήματα ισχυρής αυθεντικοποίησης σήμερα και να αναπτυχθεί ένα ομαλά λειτουργικό οικοσύστημα, μια ολοκληρωμένη, ανοικτή αρχιτεκτονική λύση για πολλαπλά συστήματα, το FIDO περιλαμβάνει τα εξής:

- Να μπορεί να χρησιμοποιηθεί από συσκευές των χρηστών, είτε προσωπικές, είτε έχουν εκδοθεί από επιχειρήσεις ή προσωπικές συσκευές χρηστών που τις χρησιμοποιούν στην εργασία τους (BYOD – Bring Your Own Device) και να λειτουργεί σε δυναμικό περιβάλλον λειτουργίας της συσκευής, (το σπίτι, το γραφείο, στο πεδίο, κ.λπ.).

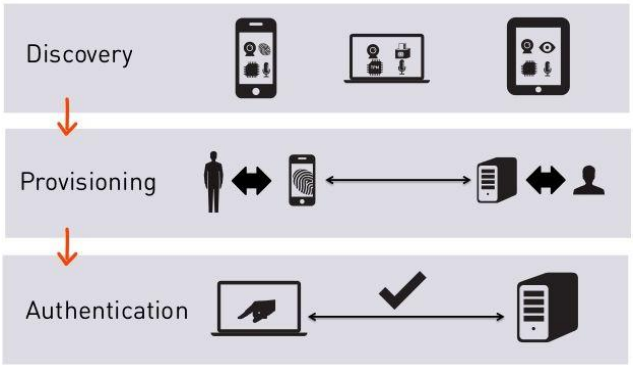


- Να περιέχει αυθεντικοποιητές ταυτότητας.
- Να διαθέτει εφαρμογές τρίτων αξιόπιστων οντοτήτων και τα διαφορετικά περιβάλλοντα ανάπτυξης τους.
- Να εξασφαλίζει την ικανοποίηση των αναγκών τόσο των τελικών χρηστών όσο και των Τρίτων Συμβαλλόμενων. Ιδιαίτερη έμφαση στην εμπειρία του τελικού χρήστη τόσο στον φυλλομετρητή όσο και σε native εφαρμογές.
- Να έχει Cross-platform πρωτόκολλα ελέγχου ταυτότητας.
- Να διαθέτει ένα ενιαίο cross-platform authenticator API.
- Να χρησιμοποιεί απλούς μηχανισμούς για την ένταξη Αξιόπιστων Οντοτήτων.

FIDO Ιδιωτικότητα

Ο στόχος της τεχνολογίας FIDO είναι η διαφάνεια.

Η εγγραφή (registration) δίνει τη δυνατότητα στον ιστότοπο του Αξιόπιστου (Relying Party) να αυθεντικοποιήσει τον χρήστη. Η εγγραφή είναι βασικότερη λειτουργία πάνω στην οποία βασίζεται το FIDO



Κατά τη διάρκεια της εγγραφής η εγκυρότητα ενός Αυθεντικοποιητή FIDO επαληθεύεται για να επιβεβαιωθεί η integrity.

Ορίζεται ότι μία συσκευή FIDO δεν πρέπει να ταυτοποιείται μοναδικά σε όλες τις ιστοσελίδες. Στο FIDO ένα κλειδί εκδιδόμενο από έναν συγκεκριμένο ιστότοπο μπορεί να χρησιμοποιηθεί από ένα φυλλομετρητή στο συγκεκριμένο ιστότοπο και μόνο. Αυτή η απαίτηση αχρηστεύει την κλοπή δημοσίου κλειδιού με σκοπό το phishing από άλλη πηγή και εμποδίζει πολλαπλούς συνομωτούντες ιστότοπους από το να χρησιμοποιήσουν έναν αυθεντικοποιητή για να πιστοποιήσουν έναν χρήστη και να συνδέσουν την ταυτότητά του.

Επίσης, έχει δικλείδες ιδιωτικότητας στην πολιτική του συστήματος όπως είναι οι ειδοποιήσεις για όποια ενέργεια κάνει το σύστημα.

Οι αρχές ιδιωτικότητας FIDO είναι οι εξής :

1. Η απαίτηση άδειας χρήστη για οποιαδήποτε ενέργεια η οποία κάνει χρήση προσωπικών δεδομένων.
2. Η πλήρης ενημέρωση του χρήστη για όλες τις διεργασίες του FIDO.
3. Η συλλογή προσωπικών δεδομένων να περιορίζεται αποκλειστικά για χρήση από το FIDO.
4. Τα βιομετρικά δεδομένα του χρήστη να παραμένουν μόνο στην δική του κατοχή.
5. Η απαγόρευση ταυτοποίησης του χρήστη για διεργασίες εκτός του FIDO.
6. Η προστασία δεδομένων που αφορούν το FIDO από μη εξουσιοδοτημένη πρόσβαση.
7. Η εξουσιοδότηση αδείας στους χρήστες να δουν και να διαχειριστούν τους αυθεντικοποιητές FIDO.

Πρωτόκολλα FIDO

Οι U2F συσκευές δεν απαιτούν ιδιαίτερους drivers, παρά μόνο ένα υποστηριζόμενο φυλλομετρητή. Μετά την επιβεβαίωση του κωδικού του χρήστη, γίνεται αυθεντικοποίηση με το U2F. Το U2F κάνει χρήση ζεύγους ιδιωτικού κα δημοσίου κλειδιού. Ο ιστότοπος στέλνει μία πρόκληση στον φυλλομετρητή την οποία υπογράφει η συσκευή U2F και την επιστρέφει. Οι συσκευές U2F ενσωματώνονται απευθείας στον φυλλομετρητή για να αποτρέψει τις σύγχρονες τεχνικές κλοπής διαπιστευτηρίων, όπως είναι το key logging, το phishing ή το man in the middle.

Το UAF είναι πραγματικά ένα πρότυπο που δεν χρησιμοποιεί κανένα κωδικό, μειώνοντας έτσι την πολυπλοκότητα και τον αριθμό των κωδικών που πρέπει να θυμάται ένας χρήστης.

UAF	**U2F**
• Ο χρήστης κουβαλάει μία συσκευή με εγκατεστημένο το UAF	• Ο χρήστης μεταφέρει μία συσκευή U2F με υποστήριξη από φυλλομετρητές
• Ο χρήστης απλά δίνει ένα βιομετρικό του στοιχείο ή ένα PIN	• Ο χρήστης εμφανίζει τη συσκευή
• Ο ιστότοπος αποφασίζει αν θα συγκρατήσει τον κωδικό	• Ο ιστότοπος μπορεί να απλοποιήσει τον κωδικό

Universal 2nd Factor (U2F) Protocol

Το πρωτόκολλο U2F επιτρέπει στις διαδικτυακές υπηρεσίες να αυξήσει την ασφάλεια των υπαρχόντων κωδικών εισάγοντας ένα δεύτερο επίπεδο αυθεντικοποίησης. Αφού ο χρήστης καταχωρίσει το όνομά του και τον κωδικό του, η εφαρμογή του ζητάει οποιαδήποτε χρονική στιγμή να εισάγει το usb dongle ή να tapping over nfc. Έτσι, επιτρέπεται η απλοποίηση του κωδικού χωρίς να επηρεάζει την ασφάλεια.

Το σύστημα U2F έχει σχεδιαστεί για να παρέχει ισχυρό έλεγχο ταυτότητας των χρηστών στο διαδίκτυο, διατηρώντας παράλληλα την προστασία της ιδιωτικής ζωής του χρήστη. Ο χρήστης φέρει έναν «μηχανισμό U2F» για δεύτερο παράγοντα.

Όταν ο χρήστης καταχωρεί τη συσκευή U2F σε ένα λογαριασμό σε μια συγκεκριμένη προέλευση (όπως http://www.company.com) η συσκευή δημιουργεί ένα νέο ζεύγος κλειδιών που μπορούν να χρησιμοποιηθούν μόνο από αυτή την διεύθυνση. Έπειτα, δίνει στην ιστοσελίδα αυτή το δημόσιο κλειδί για να το συνδέσει με το λογαριασμό του χρήστη. Όταν ο χρήστης αυθεντικοποιείται, εκτός από το όνομα χρήστη και τον κωδικό πρόσβασης, η ιστοσελίδα (σε αυτή την περίπτωση, http://www.company.com) μπορεί να ελέγχει αν ο χρήστης έχει τη συγκεκριμένη συσκευή U2F που έχει συνδεθεί με το λογαριασμό επαληθεύοντας την υπογραφή που δημιουργείται από τη συσκευή.

Ο χρήστης είναι σε θέση να χρησιμοποιήσει την ίδια συσκευή σε πολλούς ιστότοπους στο διαδίκτυο. Ο χρήστης έχει στη διάθεσή του πολλαπλά εικονικά κλειδιά για διαφορετικές τοποθεσίες οι οποίες παράγονται από μια φυσική συσκευή. Χρησιμοποιώντας το ανοιχτό πρότυπο U2F, οποιαδήποτε ιστοσελίδα θα είναι σε θέση

να χρησιμοποιήσει οποιοδήποτε πρόγραμμα περιήγησης (ή OS), η οποία έχει υποστήριξη U2F για να μιλήσει σε οποιαδήποτε συσκευή συμβατή με U2F επιτρέποντας στο χρήστη να ενεργοποιήσει ισχυρή αυθεντικοποίηση.

Οι διαδικασίες εγγραφής και πιστοποίησης της συσκευής U2F γίνονται μέσω Javascript APIs που είναι ενσωματωμένη στο πρόγραμμα περιήγησης και στα native APIs σε κινητά λειτουργικά συστήματα.

Η συσκευή U2F μπορεί να ενσωματωθεί σε διάφορους παράγοντες, όπως stand alone συσκευές USB, stand alone Near Field Communication (NFC) συσκευή, stand alone συσκευές BlueTooth LE, ενσωματωμένο στον υπολογιστή/κινητή συσκευή του χρήστη. Είναι προτιμότερο να έχουμε υλικό το οποίο υποστηρίζει ασφάλεια, αλλά δεν είναι απαίτηση. Ωστόσο, το πρωτόκολλο προβλέπει ένα μηχανισμό πιστοποίησης που επιτρέπει την αποδοχή της ηλεκτρονικής υπηρεσίας ή την ιστοσελίδα για να προσδιορίσει την κατηγορία της συσκευής και είτε να αποδεχθεί ή όχι, ανάλογα με την πολιτική του συγκεκριμένου ιστότοπου.

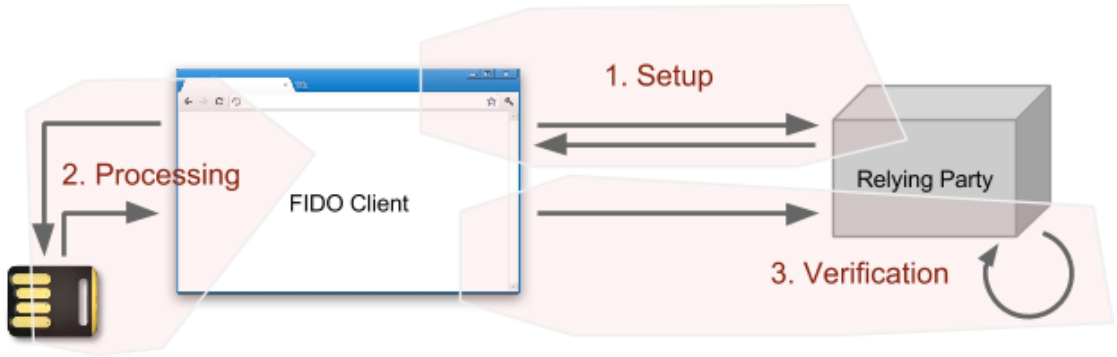
Οι προδιαγραφές για U2F είναι σε δύο layers. Το ανώτερο στρώμα καθορίζει τον κρυπτογραφικό πυρήνα του πρωτοκόλλου. Το κατώτερο καθορίζει τον τρόπο με τον οποίο θα επικοινωνήσει ο client του χρήστη με αιτήματα U2F κρυπτογράφησης στη συσκευή U2F πάνω από ένα συγκεκριμένο πρωτόκολλο μεταφοράς (π.χ. USB, NFC, Bluetooth LE, ενσωματωμένη σε ένα συγκεκριμένο λειτουργικό σύστημα, κλπ).

Ένας κρίσιμος παράγοντας για την επιτυχία θα είναι ότι μια συσκευή U2F «απλά δουλεύει» με οποιαδήποτε συσκευή που ανήκει στον χρήστη, χωρίς να χρειάζεται επιπλέον οδηγό ή εγκατάσταση. Η συσκευή USB U2F έχει σχεδιαστεί για να λειτουργεί με τα υπάρχοντα λειτουργικά συστήματα χωρίς οδηγό εγκατάστασης ή αλλαγές λογισμικού. Ένας φυλλομετρητής που είναι συμβατός με συσκευές U2F είναι σε θέση να ανακαλύψει και να επικοινωνήσει με τις συσκευές U2F χρησιμοποιώντας τυποποιημένα built- in OS APIs.

Η συσκευή U2F και το πρωτόκολλο πρέπει να εγγυάται προστασία της ιδιωτικότητας των χρηστών και την ασφάλεια αυτών. Στον πυρήνα του πρωτοκόλλου, η συσκευή U2F έχει την ικανότητα να παράγει ένα ζευγάρι δημόσιου / ιδιωτικού κλειδιού και ιδανικά να ενσωματώνεται σε ένα ασφαλές στοιχείο. Η συσκευή U2F

δίνει το δημόσιο κλειδί και ένα Διαχειριστή Κλειδιού (key handle) στην online υπηρεσία ή την ιστοσελίδα κατά το στάδιο της εγγραφής χρήστη.

Αργότερα, όταν ο χρήστης πραγματοποιεί έλεγχο ταυτότητας, η online υπηρεσία ή η ιστοσελίδα στέλνει τον Διαχειριστή Κλειδιού στη συσκευή U2F μέσω του browser. Η συσκευή χρησιμοποιεί τον Διαχειριστή για να διαπιστώσει ότι όντως είναι το ιδιωτικό κλειδί του χρήστη, και δημιουργεί μια υπογραφή η οποία στέλνεται πίσω στην ιστοσελίδα για την επαλήθευση της παρουσίας της συσκευής U2F. Έτσι, ο Διαχειριστής Κλειδιού είναι απλά ένα αναγνωριστικό ενός συγκεκριμένου κλειδιού στη συσκευή U2F.



Το ζεύγος κλειδιών δημιουργείται από τη συσκευή U2F κατά την εγγραφή είναι για τη συγκεκριμένη υπηρεσία, είναι service oriented. Κατά την εγγραφή, το πρόγραμμα περιήγησης στέλνει στη συσκευή U2F έναν hash της υπηρεσίας (συνδυασμός του πρωτοκόλλου, hostname και τη πόρτα που χρησιμοποιεί). Η συσκευή U2F επιστρέφει ένα δημόσιο κλειδί και ένα Διαχειριστή Κλειδιού. Είναι πολύ σημαντικό, η συσκευή U2F να κωδικοποιεί την αιτούσα αρχή στον Διαχειριστή Κλειδιού.

Αργότερα, όταν ο χρήστης προσπαθεί να πραγματοποιήσει έλεγχο ταυτότητας, ο διακομιστής στέλνει τον Διαχειριστή Κλειδιού του χρήστη πίσω στο πρόγραμμα περιήγησης. Το πρόγραμμα περιήγησης στέλνει αυτό τον Διαχειριστή και το hash της υπηρεσίας που ζητά τον έλεγχο ταυτότητας. Η συσκευή U2F εξασφαλίζει ότι είχαν εκδοθεί από τη συγκεκριμένη ο Διαχειριστής Κλειδιού για τη συγκεκριμένη υπηρεσία πριν προβεί σε οποιαδήποτε εργασία υπογραφή. Εάν υπάρχει αναντιστοιχία δεν επιστρέφεται καμία υπογραφή.

Ο έλεγχος αυτός προέλευσης του αιτήματος (υπηρεσία/ιστοσελίδα) εξασφαλίζει ότι τα δημόσια κλειδιά και οι διαχειριστές κλειδιού που εκδίδονται από μια συσκευή U2F σε μια συγκεκριμένη ηλεκτρονική υπηρεσία ή ιστοσελίδα δεν μπορεί να χρησιμοποιηθεί από άλλη διαφορετική online υπηρεσία ή ιστοσελίδα (δηλαδή, ένα site με ένα διαφορετικό όνομα για ένα έγκυρο πιστοποιητικό SSL). Αυτή είναι μια κρίσιμη ιδιότητα της ιδιωτικής ζωής - υποθέτοντας ότι ο browser δουλεύει όπως θα έπρεπε, ένα site μπορεί να επαληθεύσει την ταυτότητα με τη συσκευή U2F του χρήστη μόνο με ένα κλειδί, το οποίο έχει εκδοθεί για τη συγκεκριμένη θέση με τη συγκεκριμένη συσκευή U2F.

Αν αυτός ο έλεγχος προέλευσης δεν ήταν παρών, ένα δημόσιο κλειδί και ο διαχειριστής κλειδιού που εκδίδονται από τη συσκευή θα μπορούσε να χρησιμοποιηθεί ως «supercookie», το οποίο θα επέτρεπε πολλαπλές ιστοσελίδες να έρθουν σε συνεννόηση και να επαληθεύσουν και να συσχετίσουν την ταυτότητα του χρήστη.

Διαδιακασία εγγραφής

Η συσκευή συσκευή U2F έχει μια «δοκιμασία φυσικής παρουσίας των χρηστών». Ο χρήστης αγγίζει ένα πλήκτρο (ή αισθητήρας κάποιου είδους) για να ενεργοποιηθεί η συσκευή U2F και αυτό τροφοδοτεί την λειτουργία της συσκευής ως εξής:

Αυθεντικοποίηση για πρώτη φορά

Όταν ο χρήστης προσπαθεί να αυθεντικοποιηθεί για πρώτη φορά σε μια συγκεκριμένη ιστοσελίδα/υπηρεσία (δηλαδή το javascript καλεί να κάνει φέρει μια υπογραφή από τη συσκευή U2F), ο περιηγητής μπορεί να θέσει μια γραμμή πληροφοριών που ρωτά αν ο χρήστης επιθυμεί να επιτρέψει στην υπηρεσία να μιλήσει στη συσκευή U2F. Στην περίπτωση αυτή, ο φυλλομετρητής θα πρέπει επίσης να παρουσιάσει μία επιλογή με την οποία ο χρήστης να επιτρέπει στο πρόγραμμα περιήγησης να θυμηθεί την άδεια και να μην ρωτάει κάθε φορά. Αυτή η ρύθμιση μπορεί να μηδενιστεί (όπως και με άλλες ρυθμίσεις του προγράμματος περιήγησης).

Εγγραφή

Η συσκευή U2F ανταποκρίνεται σε ένα αίτημα και θα δημιουργήσει ένα

ζεύγος κλειδιών μόνο αν έχει ενεργοποιηθεί. Ξεχωριστά, το πρόγραμμα περιήγησης μπορεί να εξασφαλίσει ότι η javascript θα ζητήσει από τη συσκευή U2F να εκδώσει ένα ζεύγος κλειδιών πρόσκλησης το οποίο έχει ως αποτέλεσμα πάντα να φαίνεται στον χρήστη ένα παράθυρο γραμμής πληροφοριών που να ρωτά αν αυτός πράγματι θέλει να επιτρέψει την τρέχουσα τοποθεσία για να δηλωθεί η συγκεκριμένη συσκευή U2F.

Έλεγχος ταυτότητας

Κατά τη διάρκεια του ελέγχου ταυτότητας, ο φυλλομετρητής στέλνει κάποια δεδομένα στη συσκευή U2F που χρειάζονται υπογραφή. Η συσκευή U2F πρέπει να εκτελέσει μία δοκιμασία φυσικής παρουσίας του χρήστη πριν υπογράψει. Αυτό εξασφαλίζει ότι μια υπογραφή μπαίνει μόνο με την άδεια του χρήστη. Εξασφαλίζει επίσης ότι το κακόβουλο λογισμικό δεν μπορεί να τοποθετήσει την υπογραφή, όταν ο χρήστης δεν είναι παρών.

Εν ολίγοις, ο χρήστης θα πρέπει να αγγίξει ένα κουμπί για να εγγραφεί, και μπορεί επίσης να προειδοποιηθεί από το πρόγραμμα περιήγησης. Η εγγραφή είναι μια λειτουργία πολύ υψηλής αξίας - δίνει στην υπηρεσία τη δυνατότητα αυθεντικοποίησης του χρήστη και πρέπει να ληφθεί πολύ σοβαρά υπόψη. Κατά τη διάρκεια του ελέγχου ταυτότητας (ή γενικότερα, κάθε φορά που η ηλεκτρονική υπηρεσία η ιστοσελίδα θα πρέπει να επαληθεύσει τον χρήστη ζητώντας μια υπογραφή), ο χρήστης πρέπει να ενεργοποιήσει τη συσκευή για να αποδείξει την παρουσία του πριν υπάρξει υπογραφή.

Συσκευή U2F

Η πρόσβαση στη συσκευή U2F γίνεται με δύο συναρτήσεις javascript που είναι διαθέσιμες στον φυλλομετρητή (είτε από την online υπηρεσία είτε από τον ιστότοπο). Η μία χρησιμοποιείται για τη δημιουργία του ζεύγους των κλειδιών και η άλλη για να παράξει την υπογραφή.

Εγγραφή – δημιουργία ζεύγους κλειδιών

Ο χρήστης επαληθεύεται από τον ιστότοπο προέλευσης με το όνομα χρήστη και τον κωδικό του ή όποια άλλη επαλήθευση έχει επιλέξει. Έπειτα, η σελίδα εγγραφής καλεί μέσω του φυλλομετρητή τη συνάρτηση για τη δημιουργία του ζεύγους των κλειδιών. Τότε εμφανίζεται μήνυμα (infobar warning) στον χρήστη από τον φυλλομετρητή για να αποδεχθεί και να ξεκινήσει η διαδικασία. Έπειτα, στέλνεται αίτημα δημιουργίας ζεύγους κλειδιών στη συσκευή U2F που είναι συνδεδεμένη στον υπολογιστή.

Η πρώτη συσκευή U2F που είναι συνδεδεμένη στον υπολογιστή η οποία έχει απόδειξη ύπαρξης του χρήστη (πίεση του πλήκτρου πάνω στη συσκευή) απαντάει στο αίτημα. Ο φυλλομετρητής πακετάρει την απάντηση της συσκευής (Διαχειριστή κλειδιών, δημόσιο κλειδί) και το επιστρέφει στην ιστοσελίδα σαν έξοδο της συνάρτησης javascript. Η σελίδα τα προωθεί στον ιστότοπο όπου αποθηκεύονται αυτές οι πληροφορίες καταχωρισμένες στο λογαριασμό του χρήστη, ολοκληρώνοντας έτσι τη διαδικασία.

Αυθεντικοποίηση – δημιουργία υπογραφής

Ο χρήστης ξεκινάει τη διαδικασία αυθεντικοποίησης με το username και τον κωδικό του (ή μόνο το username αν ο ιστότοπος θέλει μόνο επαλήθευση U2F). Ο ιστότοπος προέλευσης καθιστά μια ενδιάμεση σελίδα πιστοποίησης στο οποίο στέλνει το Διαχειριστή Κλειδιού του χρήστη και nonce (ένας τυχαίος αριθμός που χρησιμοποιείται μόνο μία φορά). Αυτό τότε καλεί τη javascript λειτουργία για να δημιουργήσει την υπογραφή. Οι παράμετροι για την κλήση της συνάρτησης είναι ο Διαχειριστής κλειδιών και η nonce.

Όταν η λειτουργία δημουργίας υπογραφής καλείται, το πρόγραμμα περιήγησης μπορεί να δείξει μια γραμμή πληροφοριών που να ζητά την έγκριση του χρήστη.

Μετά την έγκριση του χρήστη, το πρόγραμμα περιήγησης μιλάει σε όλες τις συσκευές U2F συνδεδεμένες στον υπολογιστή.

Η javascript κλήση της συνάρτησης επιστρέφει το αντικείμενο «δεδομένα χρήστη» και την υπογραφή της πρώτης συσκευής που απάντησε. Η ενδιάμεση σελίδα αυθεντικοποίησης στέλνει τα «δεδομένα χρήστη» και τις απαντήσεις της συσκευής U2F στην Αξιόπιστη Οντότητα, το οποίο καθορίζει εάν οποιαδήποτε από τις υπογραφές ταιριάζει με αυτές που περίμενε.

Ανάλογα με την εφαρμογή U2F πολλαπλές συσκευές θα μπορούσαν να απαντήσουν για ένα συγκεκριμένο Διαχειστή Κλειδιών. Για παράδειγμα, θεωρούμε την περίπτωση όπου ο Διαχειριστής Κλειδιών υλοποιείται αποκλειστικά ως ένας δείκτης στη μνήμη on board, η συσκευή U2F (και ως εκ τούτου ένας μικρός ακέραιος αριθμός). Ο χρήστης μπορεί να έχει εγγράψει πολλαπλές συσκευές U2F με έναν συγκεκριμένο λογαριασμό σε συγκεκριμένο ιστότοπο και ορισμένες από αυτές τις συσκευές θα μπορούσαν να χρησιμοποιούν τον ίδιο δείκτη ακέραιο ως Διαχειριστή Κλειδιού για το συγκεκριμένο λογαριασμό για τη συγκεκριμένη προέλευση.

Περαιτέρω, αν και ο χρήστης δεν χρειάζεται κατ' ανάγκη να δει την ενδιάμεση σελίδα εγγραφής, εάν η σωστή συσκευή U2F είναι παρούσα, τότε οι υπογραφές μπορούν να αποκτηθούν και να σταλεί πίσω στον ιστότοπο και ο έλεγχος ταυτότητας να ολοκληρωθεί. Ο χρήστης πρέπει να δει ενδιάμεσες οθόνες μόνο για συνθήκες σφάλματος ("Παρακαλώ εισάγετε μια συσκευή U2F σας», «Θα σας ζητήσει να ενεργοποιήσετε τη συσκευή σας U2F» κ.ά).

Χρήση U2F συσκευής

Χρήση από πολλαπλούς χρήστες

Μια συσκευή U2F δεν έχει το νόημα του ενός χρήστη (το γνωρίζει μόνο για την έκδοση κλειδιών για τον ιστότοπο). Έτσι, ένα άτομο και η σύζυγός του θα μπορούσαν να μοιραστούν μια συσκευή U2F και να το χρησιμοποιούν για τους ατομικούς λογαριασμούς τους στην ίδια προέλευση. Πράγματι, όσο η συσκευή U2F αφορά την υπόθεση των δύο χρηστών, που έχουν λογαριασμούς στην ίδια προέλευση δεν μπορεί να διακριθεί από την υπόθεση του ίδιου του χρήστη που έχει δύο λογαριασμούς σε αυτή την προέλευση.

Η γενική περίπτωση όπου πολλαπλά άτομα μοιράζονται μια ενιαία συσκευή U2F και κάθε πρόσωπο έχει λογαριασμούς σε όποια προέλευση επιλέγει, υποστηρίζεται από το U2F.

Εγγραφή πολλαπλών συσκευών στον ίδιο λογαριασμό

Το U2F δεν περιορίζει το χρήστη να έχει μια μόνο συσκευή που θα εγγραφεί σε ένα συγκεκριμένο λογαριασμό σε ένα συγκεκριμένο χώρο. Έτσι, για παράδειγμα, ένας χρήστης μπορεί να έχει από μια συσκευή U2F μόνιμα συνδεδεμένη σε δύο διαφορετικούς υπολογιστές, όπου κάθε συσκευή U2F είναι εγγεγραμμένη στον ίδιο λογαριασμό σε συγκεκριμένη καταγωγή - επιτρέποντας έτσι να συνδέεται και από τους δύο υπολογιστές με ασφάλεια σε αυτή τη συγκεκριμένη ιστοσελίδα.

Εάν ένας χρήστης έχει εγγράψει πολλαπλές συσκευές U2F σε ένα συγκεκριμένο λογαριασμό, στη συνέχεια, κατά τη διάρκεια ελέγχου ταυτότητας όλοι οι Διαχειριστές Κλειδιών αποστέλλονται από την αρχή μέσω της ενδιάμεσης σελίδας. Η ενδιάμεση σελίδα καλεί τη συνάρτηση javascript δημιουργίας ιστοσελίδας με το πίνακα των Διαχειριστών Κλειδιών και εκείνη με τη σειρά της στέλνει τη συγκεντρωτική απάντηση πίσω στον ιστότοπο. Κάθε συνδεδεμένη συσκευή U2F υπογράφει για τους Διαχειριστές Κλειδιών στον πίνακα που αναγνωρίζει. Η εμπειρία ταυτοποίησης του χρήστη είναι αμετάβλητη.

Ως βελτιστοποίηση, σημειώνεται ότι όταν ένας ιστότοπος εντοπίζει ένα συγκεκριμένο Διαχειριστή Κλειδιού που χρησιμοποιείται με επιτυχία για την επικύρωση από ένα συγκεκριμένο πρόγραμμα περιήγησης, μπορεί να αποθηκεύσει και να θυμάται αυτό το Διαχειριστή Κλειδιού για μελλοντική χρήση θέτοντας ένα cookie στο συγκεκριμένο πρόγραμμα περιήγησης, χρησιμοποιώντας πρώτα αυτόν τον Διαχειριστή Κλειδιού πριν δοκιμάσει κάποιον άλλο.

Αυθεντικότητα U2F συσκευής

Το πρωτόκολλο συσκευής U2F είναι ανοιχτό. Ωστόσο, για την αποτελεσματική ασφάλεια, μια συσκευή U2F πρέπει να οικοδομηθεί με συγκεκριμένα πρότυπα - για παράδειγμα, εάν το κλειδί χειρισμού περιέχει το ιδιωτικό κλειδί, κρυπτογραφείται με κάποια συγκεκριμένη μέθοδο κατασκευαστή,τότε αυτό πρέπει να πιστοποιηθεί, καθώς υλοποιείται, κατά προτίμηση από κάποιον «φορέα πιστοποίησης», όπως FIDO. Επιπλέον, η πραγματική κρυπτογραφική μηχανή (ασφαλές στοιχείο) πρέπει ιδανικά να έχει κάποιες ισχυρές ιδιότητες ασφαλείας.

Ένας τρίτος συμβαλλόμενος πρέπει να είναι σε θέση να προσδιορίσει το είδος της συσκευής που μιλάει μ' ένα ισχυρό τρόπο, ώστε να μπορεί να ελέγχει με τη βάση δεδομένων για να επιβεβαιώσει αν αυτό το είδος της συσκευής έχει τα χαρακτηριστικά πιστοποίησης, τα οποία έχει ορίσει η Αξιόπιστη Οντότητα. Έτσι, για παράδειγμα, ένα site χρηματοπιστωτικών υπηρεσιών μπορούν να επιλέξει να δέχεται μόνο υλικό που υποστηρίζεται από τις συσκευές U2F, ενώ κάποια άλλα site μπορούν να επιτρέψουν συσκευές U2F, που εφαρμόζονται σε λογισμικό.

Κάθε συσκευή U2F έχει ένα κοινόχρηστο ζεύγος κλειδιών επιβεβαίωσης τα οποία είναι αποθηκευμένα στη συσκευή - αυτό το κλειδί είναι κοινό σε ένα μεγάλο αριθμό των μονάδων που παράγεται από τον ίδιο πωλητή (αυτό γίνεται για να μην αναγνωρίζεται μοναδικά η συσκευή U2F). Κάθε δημόσιο κλειδί που παράγεται από τη συσκευή U2F κατά το στάδιο της εγγραφής έχει υπογραφεί με το ιδιωτικό κλειδί βεβαίωσης.

Όταν μια τέτοια υποδομή είναι διαθέσιμη, μία συγκεκριμένη Αξιόπιστη Οντότητα (π.χ. μια τράπεζα) μπορεί να επιλέξει να δέχεται μόνο συσκευές U2F από ορισμένους προμηθευτές που διαθέτουν τις κατάλληλες δημοσιευμένες πιστοποιήσεις. Για να επιβάλει αυτήν την πολιτική, μπορεί να επαληθεύσει ότι το δημόσιο κλειδί από μια συσκευή U2F που παρουσιάστηκε από τον χρήστη είναι από έναν προμηθευτή που εμπιστεύεται.

Η παρουσία του κλειδιού βεβαίωσης εγγυάται μόνο ότι είναι μία καλά δομημένη συσκευή U2F. Ως προς το αν η συσκευή U2F είναι πράγματι ασφαλής, η εγγύηση προέρχεται από τις πιστοποιήσεις στις οποίες Τρίτες Οντότητες επιθεωρούν

την εφαρμογή από τον πωλητή. Εν ολίγοις, η βεβαίωση είναι ένας κωδικός αναγνώρισης των πιστοποιήσεων.

Μια συσκευή U2F η οποία αποθηκεύει τα κλειδιά on board, αντί να εξάγει τα προϊόντα Διαχειριστή Κλειδιών είναι κατ'αρχήν, πιο ασφαλής, δεδομένου ότι δεν είναι ευάλωτη σε τρωτά σημεία στο σχεδιασμό της κρυπτογράφησης των δεδομένων του Διαχειριστή Κλειδιών.

Εξακολουθεί να είναι δυνατή για ένα πωλητή να οικοδομήσει μια U2F συσκευή συμβατή, η οποία δεν έχει πιστοποιηθεί και των οποίων τα κλειδιά βεβαίωσης δεν έχουν δημοσιευθεί σε μια «βάση δεδομένων πιστοποίησης». Ένας τρίτος συμβαλλόμενος θα μπορούσε ακόμα να επιλέξει να αποδεχθεί τέτοιες συσκευές - αλλά θα το πράξει με την πλήρη γνώση ότι το συγκεκριμένο τύπο συσκευής δεν είναι στη βάση δεδομένων πιστοποίησης.

Ανοχή του FIDO U2F σε επιθέσεις

Προστασία από man-in-the-middle

Αν γίνει προσπάθεια επίθεσης man-in-the-middle και κάποιος προσπαθεί να μπει ενδιάμεσα στον χρήστη και στην υπηρεσία κατά τη διάρκεια της διαδικασίας πιστοποίησης, το πρωτόκολλο συσκευή U2F μπορεί να το εντοπίσει τις περισσότερες φορές.

Ας υποθέσουμε ότι ένας χρήστης έχει καταχωρήσει σωστά μια συσκευή U2F για κάποια υπηρεσία και αργότερα, μία επίθεση man-in-the-middle σε μια διαφορετική υπηρεσία προσπαθεί να υποκλέψει τον ενδιάμεσο έλεγχο ταυτότητας. Σε αυτήν την περίπτωση, η συσκευή U2F του χρήστη δεν θα απαντήσει καν, αφού η προέλευση της υπηρεσίας που είναι καταχωρημένη στον Διαχειριστή Κλειδιού και χρησιμοποιεί η επίθεση, δεν αντιστοιχεί στην προέλευση του Man-in-the-Middle.

Ο φυλλομετρητής επιστρέφει ένα αντικείμενο το οποίο περιέχει πληροφορίες σχετικά με το τι βλέπει ο φυλλομετρητής για την προέλευση, το οποίο χαρακτηρίζεται ως δεδομένα χρηστών. Αυτά τα «δεδομένα χρήστη» περιλαμβάνουν: α) την τυχαία πρόκληση που αποστέλλονται από την προέλευση, β) το όνομα του κεντρικού υπολογιστή προέλευσης φαίνεται από το πρόγραμμα περιήγησης για την ιστοσελίδα που κάνει την κλήση javascript, και γ) αν χρησιμοποιείται η επέκταση ChannelID TLS, channelID, δημόσιο κλειδί της σύνδεσης.

Το πρόγραμμα περιήγησης στέλνει ένα hash αυτού του «δεδομένα πελατών» στη συσκευή U2F. Εκτός από το hash του «δεδομένα πελατών», όπως αναφέρθηκε παραπάνω, ο browser στέλνει το hash της προέλευσης και το κλειδί λαβή ως πρόσθετες εισόδους, στη συσκευή U2F.

Όταν η συσκευή U2F λάβει το hash των δεδομένων του χρήστη, το hash της προέλευσης της υπηρεσίας και του Διαχειριστή κλειδιού, εκτελεί τα ακόλουθα βήματα: Αν είχε πράγματι εκδοθεί αυτό από τον συγκεκριμένο Διαχειριστή κλειδιού για τη συγκεκριμένη υπηρεσία η συσκευή U2F προχωρεί στην έκδοση μια υπογραφής για όλα τα δεδομένα του χρήστη τα οποία στάλθηκαν. Αυτή η υπογραφή επιστρέφεται πίσω σαν μία άλλη τιμή στο σήμα sign του U2F.

Η ιστοσελίδα που έστειλε sign call στη συσκευή U2F στέλνει τις τιμές επιστροφής - τόσο τα «δεδομένα του χρήστη» και την υπογραφή πίσω στο δικτυακό τόπο προέλευσης. Κατά την παραλαβή των «δεδομένων του χρήστη» και της υπογραφής, το πρώτο βήμα της Αξιόπιστης Οντότητας, είναι η σύγκριση και η ταύτιση της υπογραφής με τα δεδομένα. Εφόσον ταιριάξει, η Αξιόπιστη Οντότητα μπορεί να εξετάσει περαιτέρω την ύπαρξη επίθεσης man-in-the-middle με την εξής διαδικασία:

• Αν τα δεδομένα του χρήστη δείξουν μία εσφαλμένη διεύθυνση προέλευσης, τότε όντως συμβαίνει μία τέτοια επίθεση και στην περίπτωση ενός εξελιγμένου MITM που είχε επίσης τη διαμεσολάβηση της καταχώρισης και έτσι πήρε το Διαχειριστή Κλειδιού που εκδίδεται από τη συσκευή U2F για να ταιριάζει με το δικό του όνομα προέλευσης του MITM, καθώς και η MITM προσπαθεί τώρα να εξασφαλίσει ενδιάμεσα μία επικύρωση. Σε μια MITM που διαμεσολαβεί κατά της αυθεντικοποίησης και όχι κατά την εγγραφή θα αποτύχει, δεδομένου ότι η συσκευή U2F θα αρνηθεί να υπογράψει λόγω της αναντιστοιχίας προέλευσης με τον Διαχειριστή Κλειδιού).

• Αν τα δεδομένα του χρήστη δείχνουν μια ChannelID ή προέλευση που χρησιμοποιείται σε ChannelID για τη σύνδεση SSL μπορεί να συμβαίνει το εξής: Όταν το ChannelID σε «δεδομένα χρήστη» δεν ταιριάζει με την ChannelID της προέλευσης που χρησιμοποιείται, μια επίθεση Man-in-the-middle είναι παρούσα και σε εξελιγμένο MITM που διαθέτει ένα πραγματικό ισχύον CERT SSL για την προέλευση και ως εκ τούτου δεν διαφέρει από το πραγματικό.

Μια υπόθεση man-in-the-middle για την οποία η συσκευή U2F δεν προσφέρει προστασία είναι η παρακάτω. Έστω μια online υπηρεσία ή website, που δέχεται απλό κωδικό πρόσβασης, αλλά επιτρέπει στους χρήστες να εγγραφούν μόνοι τους και να εντάξουν ένα U2F. Μια MITM με διαφορετική προέλευση που υπάρχει μεταξύ του χρήστη και του πραγματικού ιστότοπου τη στιγμή της εγγραφής, μπορεί να δηλώσει και να εγγράψει τη συσκευή U2F εικονικά και να μην περάσει αυτή η καταχώριση προς την πραγματική προέλευση αλλά στον εχθρικό ιστότοπο. Αργότερα, για ελέγχους στοιχείων, η MITM μπορεί να δεχθεί τη συσκευή U2F και να κάνει αυθεντικοποίηση με κωδικό πρόσβασης προς τον πραγματικό ιστότοπο.

Υποθέτοντας ότι ο χρήστης δεν παρατηρεί το λάθος (διαφορετική) ιστοτόπου στη διεύθυνση URL, ο χρήστης θα νομίζει ότι έχει συνδεθεί με τον πραγματικό ιστότοπο αλλά στην πραγματικότητα έχει πέσει θύμα επίθεσης man-in-the-middle.

Μετρητής για την ανίχνευση κλωνοποιημένων συσκευών

Το κλειδί διαβεβαίωσης πωλητή είναι μία μέθοδος με την οποία ένας ιστότοπος μπορεί να αξιολογήσει μια συσκευή U2F. Αλλά δεν είναι επιθυμητό να αποτρέψει άλλους πωλητές, ίσως ακόμη και εκείνους που δεν έχουν κανένα ασφαλές στοιχείο, ίσως ακόμη και εφαρμογές λογισμικού. Το πρόβλημα με αυτές τις συσκευές μη ασφαλών στοιχείων βασίζεται, φυσικά, ότι θα μπορούσαν ενδεχομένως να τεθούν σε κίνδυνο και να κλωνοποιηθούν.

Το πρωτόκολλο U2F ενσωματώνει ένα μετρητή χρήσης για να επιτραπεί στον ιστότοπο προέλευσης του αιτήματος να εντοπίσει προβλήματα σε ορισμένες περιπτώσεις. Η συσκευή U2F θυμάται μια καταμέτρηση του αριθμού των πράξεων της υπογραφής που έχει πραγματοποιηθεί - είτε ανά ζεύγος κλειδιών (εάν διαθέτει επαρκή μνήμη) ή συγκεντρωτικά (αν έχει έναν περιορισμό μνήμης) ή ακόμα και κάτι στο ενδιάμεσο (π.χ., κλειδιά που μοιράζονται ένα μετρητή, με λίγο μικρότερη διαρροή της ιδιωτικής ζωής). Η συσκευή U2F στέλνει την πραγματική τιμή του μετρητή πίσω στο πρόγραμμα περιήγησης που το αναμεταδίδει στην προέλευση μετά από κάθε λειτουργία υπογραφής. Η συσκευή U2F συνενώνει επίσης την τιμή του μετρητή πάνω στο hash των δεδομένων του χρήστη πριν από την υπογραφή, έτσι ώστε η προέλευση μπορεί να επαληθεύσει ακράδαντα ότι η τιμή του μετρητή δεν είχε αλλοιωθεί (από το πρόγραμμα περιήγησης).

Ο διακομιστής μπορεί να συγκρίνει την τιμή του μετρητή που η συσκευή U2F απέστειλε και να το συγκρίνει με την τιμή του μετρητή που αντιμετώπισε σε προηγούμενη αλληλεπίδραση με την ίδια συσκευή U2F. Εάν η τιμή μετρητή έχει μετακινηθεί προς τα πίσω, αυτό σηματοδοτεί ότι υπάρχουν περισσότερες από μία συσκευή U2F με το ίδιο ζεύγος κλειδιών για την προέλευση αυτή (δηλαδή, ένας κλώνος της συσκευής U2F έχει δημιουργηθεί σε κάποιο σημείο). Ο μετρητής είναι ένα ισχυρό σήμα της κλωνοποίησης, αλλά δεν μπορεί να ανιχνεύσει την κλωνοποίηση σε κάθε περίπτωση - για παράδειγμα, αν ο κλώνος είναι μόνο ένας ο οποίος

χρησιμοποιείται μετά τη λειτουργία κλωνοποίησης και το πρωτότυπο δεν χρησιμοποιείται ποτέ, αυτή η υπόθεση δεν μπορεί να ανιχνευθεί.

Κακόβουλο λογισμικό στον χρήστη

Όσο οι συσκευές U2F μπορούν να γίνουν άμεσα προσβάσιμες από το χώρο του χρήστη με το λειτουργικό σύστημα του χρήστη, είναι δυνατόν ένα κακόβουλο λογισμικό να δημιουργήσει ένα ζεύγος κλειδιών χρησιμοποιώντας ένα αίτημα από ψεύτικο ιστότοπο στη συσκευή U2F. Η συσκευή U2F δεν θα είναι σε θέση να ξεχωρίσει το κακόβουλο λογισμικό του χρήστη. Είναι δυνατόν ένα κακόβουλο λογισμικό να αναπαράγει αιτήματα από το μηχάνημα του χρήστη # 1 σε μια συσκευή U2F που συνδέεται στον υπολογιστή του χρήστη # 2 αν το κακόβουλο λογισμικό βρίσκεται και στα δύο μηχανήματα. Προστασία έναντι κακόβουλου λογισμικού γίνεται πιο δυνατή αν η συσκευή U2F είναι ενσωματωμένη μέσα στο λειτουργικό σύστημα OS, σε αντίθεση με τη λειτουργία στον χώρο του χρήστη. Το λειτουργικό σύστημα μπορεί να αποκτήσει αποκλειστική πρόσβαση σε συσκευές U2F και να επιβάλλει τις μεθόδους για τη διασφάλιση της προέλευσης του αιτήματος.

Universal Authentication Framework (UAF) Protocol

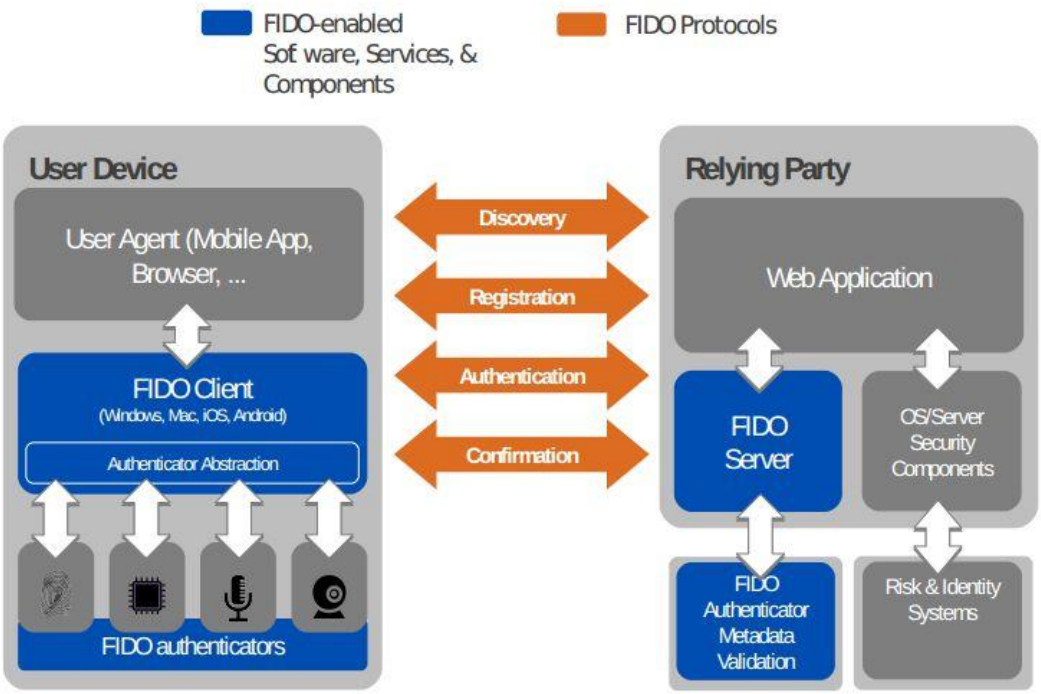
Το πρωτόκολλο UAF επιτρέπει να γίνεται η σύνδεση στις διαδικτυακές υπηρεσίες χωρίς κωδικό και με πολυεπίπεδη ασφάλεια. Ο χρήστης καταχωρεί την συσκευή στην διαδικτυακή υπηρεσία επιλέγοντας έναν μηχανισμό τοπικής αυθεντικοποίησης.

Όταν εγγράφεται ο χρήστης δεν χρειάζεται να καταχωρίσει τον κωδικό του όταν αυθεντικοποιείται από εκείνη την συσκευή, αλλά απλά ξαναχρησιμοποιεί τον τοπικό μηχανισμό αυθεντικοποίησης, όποτε απαιτείται.

Στόχοι του UAF

Το UAF προσφέρει τα εξής:

- Υποστηρίζει εφαρμογές των αξιόπιστων οντοτήτων και τα περιβάλλοντα ανάπτυξής τους.
- Ικανοποιούνται οι ανάγκες τόσο των τελικών χρηστών όσο και των Συμβαλλόμενων Οντοτήτων.
- Δίνεται ιδιαίτερη έμφαση στην εμπειρία του τελικού χρήστη.
- Είναι cross-platform ισχυρό πρωτόκολλο ελέγχου ταυτότητας.
- Προσφέρει ένα ενιαίο cross-platform authenticator API.
- Διαθέτει απλούς μηχανισμούς για την ένταξη της Συμβαλλόμενης Οντότητας.



FIDO UAF Client

Ο πελάτης FIDO UAF είναι υπεύθυνος για:

• Αλληλεπίδραση με συγκεκριμένους FIDO UAF ελεγκτές ταυτότητας χρησιμοποιώντας το επίπεδο του FIDO UAF Authenticator Abstraction μέσω του FIDO UAF Authenticator API.

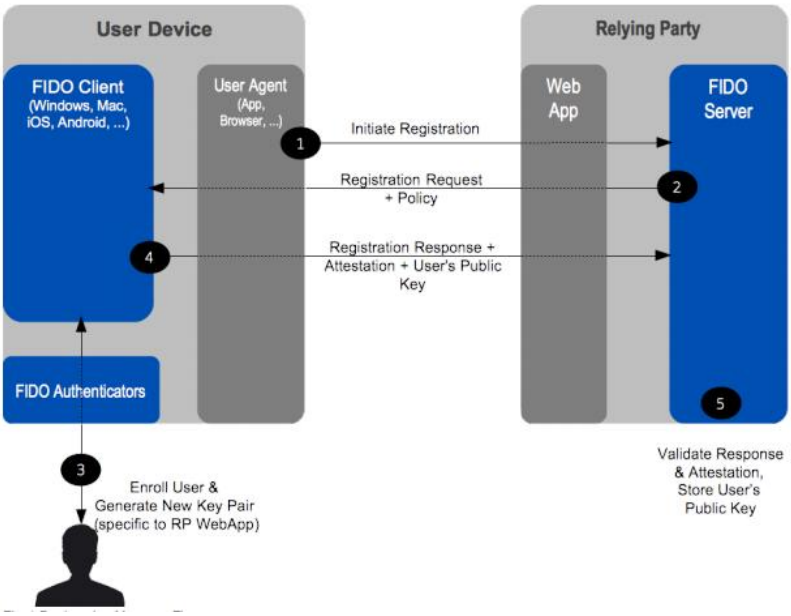
• Αλληλεπίδραση με έναν «πράκτορα χρήστη» στη συσκευή (π.χ. ένα κινητό app, το πρόγραμμα περιήγησης) χρησιμοποιώντας συγκεκριμένη διεπαφή για να επικοινωνήσει με το FIDO UAF Server. Για παράδειγμα, ένα FIDO plugin για συγκεκριμένο πρόγραμμα περιήγησης θα χρησιμοποιήσει τις υφιστάμενες διεπαφές του προγράμματος περιήγησης plugin. Μία εφαρμογή κινητού μπορεί να χρησιμοποιήσει ένα συγκεκριμένο FIDO-SDK. Ο πράκτορας χρήστη είναι τότε υπεύθυνος για την επικοινωνία μηνυμάτων FIDO UAF με ένα διακομιστή FIDO UAF της Συμβαλλόμενης Οντότητας.

Η αρχιτεκτονική FIDO UAF εξασφαλίζει ότι το λογισμικό FIDO που χρησιμοποιείται από τον χρήστη μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα τύπων συστημάτων, λειτουργικών συστημάτων και προγραμμάτων περιήγησης στο Web. Ενώ το λογισμικό FIDO πελάτη είναι συνήθως για συγκεκριμένη πλατφόρμα, οι

αλληλεπιδράσεις μεταξύ των διαφόρων λειτουργιών εξασφαλίζουν μια συνεπή εμπειρία χρήστη από πλατφόρμα σε πλατφόρμα.

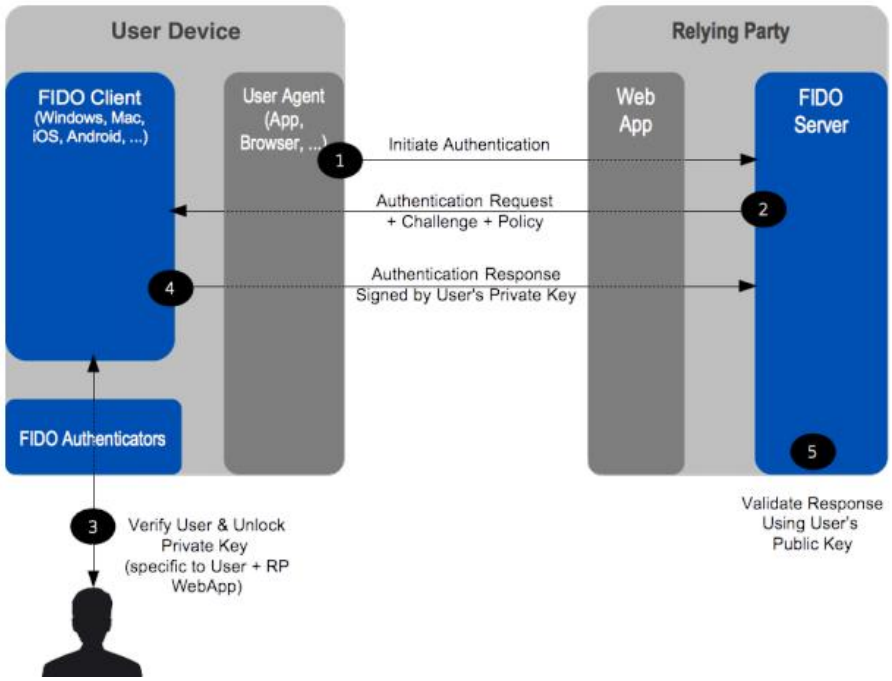
Εγγραφή αυθεντικοποιητή

Μία Αξιόπιστη Συμβαλλόμενη Οντότητα μπορεί να ανιχνεύσει με διαφάνεια, όταν ο χρήστης αρχίζει να συνεργάζεται μαζί του. Σε αυτή την αρχική φάση εισαγωγής, η ιστοσελίδα θα ζητήσει από το χρήστη άδεια για να ανιχνευθεί κάθε FIDO UAF Authenticator, δίνοντας τις επιλογές στον χρηστή όσον αφορά την εγγραφή με τον δικτυακό τόπο ή όχι



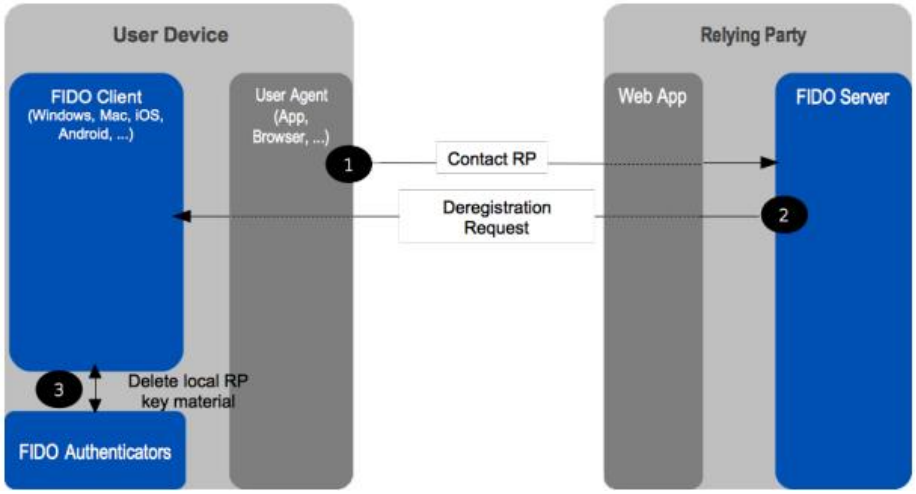
Αυθεντικοποίηση

Μετά την εγγραφή, το FIDO UAF Authenticator στη συνέχεια θα χρησιμοποιηθεί κάθε φορά που ο χρήστης ελέγχει την ταυτότητα στο δικτυακό τόπο. Ο δικτυακός τόπος μπορεί να εφαρμόσει διάφορες στρατηγικές για εναλλακτικές περιπτώσεις που αυθεντικοποιήτης FIDO δεν είναι παρόν. Αυτά μπορεί να κυμαίνεται από συμβατικά επιτρεπόμενη είσοδο με μειωμένα προνόμια μέχρι και απαγορεύοντας την είσοδο.



Απεγγραφή αυθεντικοποιητή

Υπάρχουν κάποιες περιπτώσεις όπου ένας Τρίτος Συμβαλλόμενος μπορεί να χρειαστεί να καταργήσει τα διαπιστευτήρια UAF που σχετίζονται με ένα συγκεκριμένο λογαριασμό χρήστη. Για παράδειγμα, ο λογαριασμός χρήστη ακυρώνεται ή διαγράφεται, ο χρήστης έχει χάσει ή του έχουν κλέψει FIDO Authenticator. Στις περιπτώσεις αυτές, η Αξιόπιστη Οντότητα μπορεί να ζητήσει από τον αυθεντικοποιητή FIDO για να διαγράψει τα κλειδιά ταυτότητας που συνδέονται με το λογαριασμό του χρήστη



FIDO UAF Server

Ένας διακομιστής FIDO UAF υλοποιεί την πλευρά του διακομιστή των πρωτοκόλλων FIDO UAF και είναι υπεύθυνο για:

• Σε συνεργασία με το web server της Συμβαλλόμενης Οντότητας να επικοινωνούν τα μηνύματα FIDO UAF μέσω ενός πράκτορα χρήστη της συσκευής.

• Επικύρωση των διαβεβαιώσεων του FIDO UAF αυθεντικοποιητή έναντι των μεταδεδομένων του διαμορφωμένου αυθεντικοποιητή, εξασφαλίζοντας ότι μόνο έμπιστοι ελεγκτές ταυτότητας θα καταχωριστούν για χρήση.

• Διαχείριση της σύνδεσης των εγγεγραμμένων FIDO UAF ελεγκτών ταυτότητας στους λογαριασμούς των χρηστών στο Τρίτου Συμβαλλόμενου.

• Αξιολόγηση της ταυτοποίησης του χρήστη και την απάντηση της επιβεβαίωσης της συναλλαγής για τον προσδιορισμό της ισχύος τους.

Ο διακομιστής FIDO UAF έχει σχεδιαστεί για να αναπτυχθεί ως ένας διακομιστής εσωτερικής εγκατάστασης στη Συμβαλλόμενη Οντότητα ή να ανατεθεί σε Τρίτη οντότητα παροχής υπηρεσιών FIDO.

FIDO UAF Protocols

Τα πρωτόκολλα FIDO UAF μεταφέρουν μηνύματα FIDO UAF μεταξύ των συσκευών των χρηστών και των Συμβαλλόμενων Αξιόπιστων Οντοτήτων. Υπάρχουν μηνύματα για:

• Εγγραφή Αυθεντικοποιητή: Το πρωτόκολλο καταχώρησης FIDO UAF επιτρέπει σε Τρίτους Συμβαλλόμενους να:

- Ανακαλύψουν τους διαθέσιμους στο σύστημα ή στη συσκευή του χρήστη FIDO UAF ελεγκτές ταυτότητας. Θα επιστρέψει τα χαρακτηριστικά τους επιτρέποντας να λάβουν χώρα έτσι οι αποφάσεις πολιτικής και η επιβολή.
- Επιβεβαιώνει τους ισχυρισμούς των ελεγκτών ταυτότητας FIDO UAF για να διασφαλιστεί ότι η υπηρεσία ελέγχου ταυτότητας είναι αυθεντική και αξιόπιστη. Η επαλήθευση συμβαίνει με τη χρήση της διαβεβαίωσης των πιστοποιητικών δημόσιου κλειδιού που διανέμεται μέσω των μεταδεδομένων του αυθεντικοποιητή.

• Καταχώρηση του αυθεντικοποιητή στην υπηρεσία ελέγχου ταυτότητας και σύνδεση με το λογαριασμό του χρήστη στην Αξιόπιστη Συμβαλλόμενη Οντότητα. Μόλις επικυρωθεί μια βεβαίωση authenticator, ο Τρίτος Συμβαλλόμενος μπορεί να προσφέρει ένα μοναδικό ασφαλές αναγνωριστικό που είναι ειδικά για αυτόν και την FIDO UAF ταυτότητα. Αυτό το αναγνωριστικό μπορεί να χρησιμοποιηθεί σε μελλοντικές αλληλεπιδράσεις μεταξύ του ζεύγους {RP, Authenticator} και δεν είναι γνωστό σε οποιεσδήποτε άλλες συσκευές.

• Επαλήθευση χρήστη: Η αυθεντικοποίηση βασίζεται σε κρυπτογραφικά πρωτόκολλα ελέγχου ταυτότητας που ανταποκρίνονται σε πρόκληση και διευκολύνει την επιλογή των χρηστών σχετικά με το ποιοι FIDO UAF ελεγκτές ταυτότητας απασχολούνται σε περίπτωση ταυτοποίησης.

• Επιβεβαίωση Ασφαλής Συναλλαγής: Εάν η Υπηρεσία ελέγχου ταυτότητας χρήστη περιλαμβάνει τη δυνατότητα να το πράξουν, ο Αξιόπιστος Τρίτος Συμβαλλόμενος μπορεί να παρουσιάσει στον χρήστη ένα ασφαλές μήνυμα επιβεβαίωσης. Το περιεχόμενο του μηνύματος προσδιορίζεται από την Αξιόπιστη Οντότητα και θα μπορούσε να χρησιμοποιηθεί σε διάφορα πλαίσια, όπως επιβεβαίωση μιας χρηματοοικονομικής συναλλαγής, συμφωνία χρήστη, ή απελευθέρωση των φακέλων ασθενών.

• Απεγγραφή Αυθεντικοποιητή: Η διαγραφή απαιτείται συνήθως όταν ο λογαριασμός χρήστη έχει αφαιρεθεί από την Αξιόπιστη Οντότητα. Ο Τρίτος Συμβαλλόμενος μπορεί να προκαλέσει τη διαγραφή ζητώντας από την Υπηρεσία ελέγχου ταυτότητας να διαγράψει τη πιστοποίηση με το σχετικό UAF και το λογαριασμό χρήστη.

FIDO UAF Authenticator Abstraction Layer

Το στρώμα FIDO UAF Authenticator Abastraction παρέχει ένα ενιαίο API για τους χρήστες FIDO επιτρέποντας τη χρήση του προγράμματος ελέγχου ταυτότητας που βασίζεται σε υπηρεσίες κρυπτογράφησης. Παρέχει ένα ομοιόμορφο κατώτερο στρώμα "authenticator plugin" API διευκολύνοντας την ανάπτυξη των multi-vendor FIDO UAF ελεγκτών ταυτότητας και των απαιτούμενων οδηγών τους.

FIDO UAF Authenticator

Ένας αυθεντικοποιητής FIDO UAF είναι μία ασφαλής οντότητα, που συνδέεται με ή στεγάζονται μέσα σε συσκευές χρηστών FIDO, που μπορούν να δημιουργήσουν κλειδί που σχετίζεται με Τρίτους Συμβαλλόμενους. Το κλειδί μπορεί στη συνέχεια να χρησιμοποιηθεί για να συμμετάσχουν σε FIDO UAF πρωτόκολλα ισχυρού έλεγχου ταυτότητας. Για παράδειγμα, ένας αυθεντικοποιητής FIDO UAF μπορεί να δώσει μια απάντηση σε ένα κρυπτογραφικό πρόκληση χρησιμοποιώντας το κλειδί ταυτοποιώντας το στην Τρίτη Οντότητα.

Προκειμένου να επιτευχθεί ο στόχος της απλούστευσης της ολοκλήρωσης των δυνατότητων ελέγχου ταυτότητας, ένας αυθεντικοποιητής FIDO UAF θα είναι σε θέση να βεβαιώσει τον συγκεκριμένο τύπο (π.χ., βιομετρικό) και τις ικανότητές του (π.χ., με την υποστήριξη αλγόριθμων κρυπτογράφησης), καθώς και την προέλευσή του. Αυτό παρέχει εμπιστοσύνη στον Τρίτο Συμβαλλόμενο ότι ο χρήστης προς ταυτοποίηση είναι πράγματι ο χρήστης που αρχικά έχει καταχωρηθεί με την ιστοσελίδα.

Γνησιότητα FIDO UAF Αυθεντικοποιητή

Στο πλαίσιο FIDO UAF πρέπει να υπάρχει διαβεβαίωση πώς οι ελεγκτές ταυτότητας (αυθεντικοποιήτες) είναι αυθεντικοί κατά την εγγραφή σε μία Αξιόπιστη Συμβαλλόμενη Οντότητα, δηλαδή ότι τα κλειδιά που παράγουν και/ ή ορισμένες μετρήσεις που αναφέρουν, προέρχονται από γνήσιες συσκευές με πιστοποιημένα χαρακτηριστικά.

Μια υπογραφή βεβαίωσης, μεταφέρεται με ένα μήνυμα πρωτόκολλου καταχώρησης FIDO UAF για να επικυρωθεί από το FIDO UAF Server. Οι αυθεντικοποιητές FIDO UAF δημιουργούν ιδιωτικά κλειδιά που χρησιμοποιούνται για να δημιουργήσουν τις υπογραφές και το FIDO UAF διακομιστή επικυρώνει την υπογραφή χρησιμοποιώντας τη βεβαίωση από το πιστοποιητικό δημόσιου κλειδιού που βρίσκεται στα μεταδεδομένα του αυθεντικοποιητή. Τα μεταδεδομένα των πιστοποιητικών μοιράζονται με τους FIDO UAF Διακομιστές εκτός ζώνης.

Ασφάλεια πρωτοκόλου UAF

Το πρωτόκολλο FIDO UAF υποστηρίζει μια ποικιλία διαφορετικών ελεγκτών ταυτότητας FIDO. Παρόλο που η ασφάλεια των εν λόγω ελεγκτών ταυτότητας ποικίλει, το πρωτόκολλο UAF και ο διακομιστής FIDO θα πρέπει να παρέχουν ένα πολύ υψηλό επίπεδο ασφάλειας - τουλάχιστον σε εννοιολογικό επίπεδο. Στην πραγματικότητα, θα μπορούσαν να απαιτούν FIDO Authenticator με ένα υψηλό επίπεδο ασφάλειας, ώστε να επωφεληθεί πλήρως από την δύναμη ασφαλείας UAF.

Σε ορισμένα περιβάλλοντα η συνολική ασφάλεια της ρητής πιστοποίησης (όπως προβλέπεται από το FIDO) είναι λιγότερο σημαντική, δεδομένου ότι θα μπορούσε να συμπληρωθεί με ένα υψηλό βαθμό πιστοποίησης ή αν η εφαρμογή δεν απαιτεί ακόμη και ένα υψηλό επίπεδο αντοχής ταυτότητας.

Οι στόχοι ασφαλείας του FIDO UAF είναι οι κάτωθι:

- Strong Authentication **[SG-1]:** Αυθεντικοποίηση ενός χρήστη ή / και μιας συσκευής από Τρίτη Συμβαλλόμενη Οντότητα με υψηλή (κρυπτογραφική) δύναμη.
- Credential Guessing Resilience **[SG-2]**: Παροχή ισχυρής προστασίας ενάντια σε ωτακουστές, π.χ. να είναι ανθεκτικό σε φυσική παρατήρηση, ανθεκτικό σε στοχευόμενες πλαστοπροσωπίες, ανθεκτική σε στραγγαλισμό.
- Credential Disclosure Resilience **[SG-3]**: Να είναι ανθεκτικό σε επιθέσεις phishing και σε πραγματικό χρόνο επίθεσης phishing, συμπεριλαμβανομένης της ανθεκτικότητας σε απευθείας σύνδεση επιθέσεις από τους αντιπάλους που είναι σε θέση να χειριστούν ενεργά την κυκλοφορία του δικτύου.
- Μη-συνδεσιμότητα **[SG-4]**: Προστασία της συνομιλίας έτσι ώστε κάθε δύο εξαρτώμενα μέρη να μην μπορεί να συνδεθεί η συζήτηση με ένα χρήστη (δηλαδή να είναι unlinkable).
- Verifier Leak Resilience **[SG-5]**: Να είναι ανθεκτικό σε διαρροές από τα άλλα μέρη που βασίζεται.
- Authenticator Leak Resilience **[SG-6]:** Να είναι ανθεκτικό σε διαρροές από άλλους ελεγκτές ταυτότητας FIDO. Δηλαδή, τίποτα που ένας συγκεκριμένος FIDO Authenticator θα μπορούσε ενδεχομένως να διαρρεύσει να μπορεί να χρησιμοποιηθεί από έναν εισβολέα για να μιμηθεί οποιοδήποτε άλλο χρήστη σε οποιαδήποτε Τρίτη Συμβαλλόμενη Οντότητα.
- Συναίνεση χρήστη **[SG-7]:** Ρητή συναίνεση χρήστη.

- Limited PII **[SG-8]**: Περιορισμός ποσότητας των προσωπικών πληροφοριών που μπορεί να χαρακτηρίσουν μοναδικά ένα χρήστη (PII) να εκτίθενται στην Τρίτη Συμβαλλόμενη Οντότητα.
- Attestable Properties **[SG-9]**: Τρίτοι Συμβαλλόμενοι θα πρέπει να είναι σε θέση να ελέγξουν του μοντέλου / τύπου FIDO Authenticator (προκειμένου για τον υπολογισμό του ρίσκου που εμπεριέχει).
- Αντίσταση DoS **[SG-10]**: Να είναι ανθεκτικό σε επιθέσεις άρνησης παροχής υπηρεσίας. Δηλαδή να αποτρέπει τους εισβολείς από την εισαγωγή μη έγκυρων πληροφοριών εγγραφής για ένα νόμιμο χρήστη για την επόμενη φάση της σύνδεσης. Στη συνέχεια, ο νόμιμος χρήστης δεν θα είναι σε θέση να συνδεθεί με επιτυχία πια.
- Αντίσταση Πλαστογραφίας **[SG-11]**: Να είναι ανθεκτικό στην πλαστογράφηση (Επιθέσεις Μίμηση). Δηλαδή να αποτρέψει τους εισβολείς από το να επιχειρήσουν να τροποποιήσουν υποκεκλαμμένες συνομιλίες.
- Αντίσταση Παράλληλης Συνεδρία **[SG-12]** ς: Να είναι ανθεκτικό σε επιθέσεις Παράλληλης Συνεδρίας. Χωρίς να γνωρίζει τα διαπιστευτήρια του χρήστη, ένας εισβολέας μπορεί να μεταμφιεστεί ως ο νόμιμος χρήστης, δημιουργώντας ένα έγκυρο μήνυμα ελέγχου ταυτότητας από κάποια eavesdropped επικοινωνία μεταξύ του χρήστη και του διακομιστή.
- Αντίσταση Προώθησης **[SG-13]**: Να είναι ανθεκτικό σε επιθέσεις αναπαραγωγής και προώθησης. Έχοντας υποκλαπεί προηγούμενες συνομιλίες, ένας εισβολέας μπορεί να μιμηθεί το νόμιμο χρήστη για τον έλεγχο ταυτότητας στο σύστημα. Ο εισβολέας μπορεί να επαναλάβει ή να διαβιβάσει τα μηνύματα που υποκλάπησαν.
- Μη αποποίηση1 **[SG-14]**: Παροχή ισχυρής κρυπτογραφικής μη άρνηση για ασφαλείς συναλλαγές.
- Λειτουργία εντός των όριων ασφαλείας περιβάλλοντος λειτουργίας **[SG-15].**

[1] Ο μόνος στόχος ασφαλείας του FIDO που ισχύει και για το U2F.

Παρακάτω φαίνεται ο πίνακας συσχέτισης των στόχων του FIDO και των μέτρων που λαμβάνονται.

Στόχος Ασφαλείας	Μέτρα που λαμβάνονται
[SG-1] Strong User Authentication	• Key Protection • Channel Binding • Trusted Facet List • Signature Counter
[SG-2] Credential Guessing Resilience	• Key Protection • Cryptographically Secure Verifier Database
[SG-3] Credential Disclosure Resilience	• Key Protection • Authenticator Certification • Signature Counter
[SG-4] Unlinkability	• Unique Authentication Keys • Authenticator Class Attestation
[SG-5] Verifier Leak Resilience	• Unique Authentication Keys • Cryptographically Secure Verifier Database
[SG-6] Authenticator Leak Resilience	• Authenticator Certification • Signature Counter
[SG-7] User Consent	• Key Protection • User Consent • Secure Channel with Server Authentication • Transaction Confirmation
[SG-8] Limited PII	Unique Authentication Keys
[SG-9] Attestable Properties	• Authenticator Class Attestation • Authenticator Status Checking • Authenticator Certification
[SG-10] DoS Resistance	Protocol Nonces
[SG-11] Forgery Resistance	• Secure Channel with Server Authentication • Protocol Nonces • Round Trip Integrity • Channel Binding
[SG-12] Parallel Session Resistance	• Secure Channel with Server Authentication

	• Protocol Nonces • Round Trip Integrity • Channel Binding
[SG-13] Forwarding Resistance	• Secure Channel with Server Authentication • Protocol Nonces • Round Trip Integrity • Channel Binding
[SG-14] Transaction Non-Repudiation	• Key Protection • Unique Authentication Keys • Protocol Nonces • Authenticator Certification • Transaction Confirmation • Round Trip Integrity • Channel Binding
[SG-15] Respect for Operating Environment Security Boundaries	• Key Handle Access Token • Trusted Facet List

Χρήση TLS για προστασία επικοινωνίας

Προκειμένου να προστατευθεί η επικοινωνία δεδομένων μεταξύ FIDO UAF πελάτη και διακομιστή FIDO ένα προστατευμένο κανάλι TLS πρέπει να εγκαθιδρυθεί από τον FIDO UAF Πελάτη (ή User Agent) και την Αξιόπιστη Οντότητα για όλα τα στοιχεία του πρωτοκόλλου.

Το τελικό σημείο του server της σύνδεσης TLS πρέπει να βρίσκεται στην Συμβαλλόμενη Οντότητα. Το τελικό σημείο του πελάτη της σύνδεσης TLS πρέπει να είναι είτε ο FIDO UAF Client ή το User Agent.

Το τελικό σημείο TLS πελάτη και διακομιστή πρέπει να χρησιμοποιεί TLS v1.2 ή νεότερη έκδοση και πρέπει να χρησιμοποιείται μόνο αν το TLS v1.1 TLS v1.2 ή νεότερη έκδοση δεν είναι διαθέσιμη. Οι «Anon» και «null» TLS κρυπτο-σουίτες δεν επιτρέπονται και πρέπει να απορριφθούν. Οι ανασφαλείς κρυπτο-αλγοριθμοί TLS (π.χ. MD5, RC4, SHA1) θα πρέπει να αποφεύγονται.

TLS Binding

Τα ο UAF βασίζεται σε έλεγχο ταυτότητας διακομιστή TLS για τη σύνδεση με τα κλειδιά ελέγχου ταυτότητας AppIDs. Υπάρχουν αρκετές απειλές όπως είναι οι εξής:

- Οι επιτιθέμενοι θα μπορούσαν να πάρουν με δόλο ένα πιστοποιητικό διακομιστή TLS για το ίδιο αναγνωριστικό εφαρμογής ως στηριζόμενη κόμμα και θα μπορούσαν να είναι σε θέση να χειριστούν το σύστημα DNS.
- Οι επιτιθέμενοι θα μπορούσαν να είναι σε θέση να κλέψει διακομιστή TLS ιδιωτικό κλειδί του Τρίτου Συμβαλλόμενου και το πιστοποιητικό και θα μπορούσαν να είναι σε θέση να χειριστούν το σύστημα DNS.

Και υπάρχουν απαιτήσεις λειτουργικότητας:

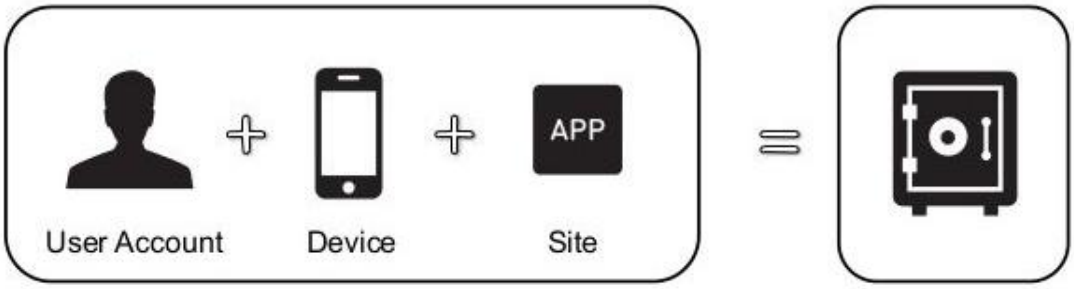
- Οι συναλλαγές UAF μπορεί να εκτείνονται σε πολλαπλές συνεδρίες TLS.
- Τα κέντρα δεδομένων θα μπορούσε να χρησιμοποιήσει SSL συμπυκνωτές.
- Τα κέντρα δεδομένων θα μπορούσε να εφαρμόσει εξισορρόπησης φόρτου για TLS παραμέτρους που χρησιμοποιούν διαφορετικά πιστοποιητικά TLS.

Αν ο πελάτης λειτουργεί πίσω από proxy έμπιστο (σε αυτό τον πελάτη) που λειτουργεί ως TLS άνθρωπος-in-the-middle, ο πελάτης θα δει ένα διαφορετικό πιστοποιητικό από τη μία από αυτό που ο διακομιστής χρησιμοποιεί. Αυτό είναι πραγματικά αρκετά κοινό για την εταιρικά ή στρατιωτικά δίκτυα με μια στάση υψηλής ασφάλειας που θέλουν να ελέγχουν όλες τις εισερχόμενες και εξερχόμενες κινήσεις.

Αν ο διακομιστής FIDO παίρνει μόνο μια τιμή κατακερματισμού, δεν υπάρχει τρόπος να το διακρίνει από μια επίθεση. Αν η αποστολή ολόκληρου του πιστοποιητικού είναι αποδεκτή από την άποψη της απόδοσης, ο διακομιστής μπορεί να το εξετάσει και να προσδιορίσει αν είναι ένα πιστοποιητικό για ένα έγκυρο όνομα από έναν μη τυπικό εκδότη (πιθανόν διοικητικά αξιόπιστο) ή ένα πιστοποιητικό για διαφορετικό όνομα (το οποίο σχεδόν βέβαια υποδηλώνει μια επίθεση προώθησης).

Ασφάλεια FIDO

Εννοιολογικά, το FIDO περιλαμβάνει μια συνομιλία μεταξύ ενός υπολογιστικού περιβάλλοντος που ελέγχεται από ένα Τρίτο Συμβαλλόμενο και εκείνο που ελέγχεται από τον χρήστη που θα πιστοποιηθεί. Περιβάλλον του Τρίτου Συμβαλλόμενου αποτελείται τουλάχιστον από ένα web server και server-side τμήματα μιας εφαρμογής web, συν ένα διακομιστή FIDO. Ο FIDO Server έχει ένα κομμάτι εμπιστοσύνης, που περιέχει τις (δημόσιες) άγκυρες εμπιστοσύνης για την βεβαίωση των αυθεντικοποιητών FIDO.



Το περιβάλλον του χρήστη, αναφέρεται ως η συσκευή του χρήστη FIDO, αποτελείται από ένα ή περισσότερους ελεγκτές ταυτότητας FIDO, ένα κομμάτι του λογισμικού που ονομάζεται FIDO Client που είναι το τελικό σημείο για UAF και συνομιλίες U2F, και το λογισμικό agent του χρήστη. Ο agent του χρήστη μπορεί να είναι ένα πρόγραμμα περιήγησης που φιλοξενεί μια διαδικτυακή εφαρμογή που εξέδωσε ο Τρίτος Έμπιστος Συμβαλλόμενος, ή μπορεί να είναι μια αυτόνομη εφαρμογή που εξέδωσε. Σε κάθε περίπτωση, ο πελάτης FIDO μπορεί πράγματι να εφαρμοστεί σε ολόκληρη ή εν μέρει, εντός των ορίων του πράκτορα χρήστη.

Η κατηγοριοποίηση των επιθέσεων σύμφωνα με το FIDO είναι η εξής:

1. Αυτοματοποιημένες επιθέσεις που επικεντρώθηκαν σε εξαρτώμενα μέρη, τα οποία επηρεάζουν τον χρήστη, αλλά δεν μπορεί να εμποδιστεί από το χρήστη.

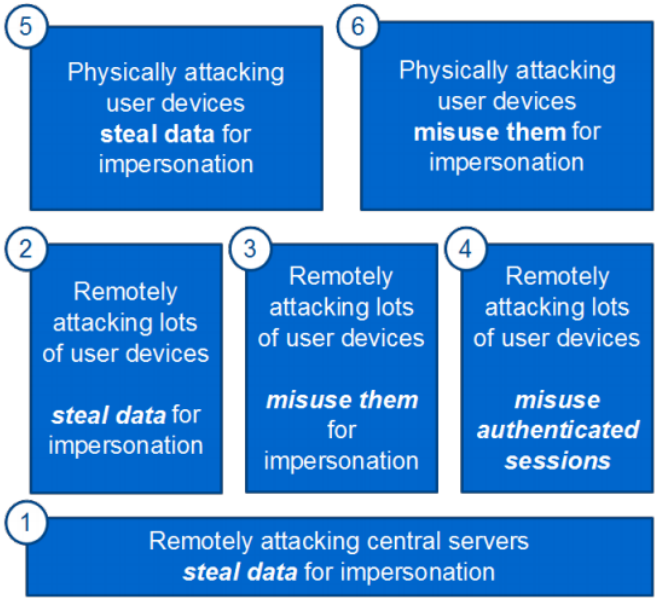
2. Αυτοματοποιημένες επιθέσεις που πραγματοποιούνται μια φορά και μπορεί να οδηγήσει στην ικανότητα να μιμηθεί τον χρήστη σε συνεχή βάση, χωρίς τη συμμετοχή του ή τη συσκευή του άμεσα.

3. Αυτοματοποιημένες επιθέσεις που αφορούν τον χρήστη ή συσκευή του για κάθε επιτυχημένη πλαστοπροσωπία.

4. Αυτοματοποιημένες επιθέσεις στις συνεδρίες που επικυρώνονται από το χρήστη.

5. Μη αυτοματοποιημένες επιθέσεις στο χρήστη ή τη συσκευή του που εκτελούνται μία φορά και μπορεί να οδηγήσει στην ικανότητα να μιμηθεί τον χρήστη σε μια συνεχή βάση, χωρίς τη συμμετοχή του ή τη συσκευή του άμεσα.

6. Μη αυτοματοποιημένες επιθέσεις στο χρήστη ή συσκευή του, η οποία περιλαμβάνει τη συσκευή ή χρήστη του για κάθε επιτυχημένη πλαστοπροσωπία.



Συμπερασματικά, φαίνεται ότι το FIDO τηρεί υψηλά πρότυπα ασφάλειας. Παρακάτω φαίνονται τα σημαντικότερα χαρακτηριστικά του.

Χαρακτηριστικά	Πλεονεκτήματα Ασφαλείας
Μοναδικό κλειδί για κάθε χρήστη/συσκευή/ιστότοπο	Τμηματοποίηση ρίσκου
Υψηλή εντροπία ασύμμετρων κλειδιών αντί για κωδικούς	Προστασία ενάντια σε επιθέσεις dictionary και brute force
Τα μυστικά δεν αποκαλύπτονται στον χρήστη	Προστασία ενάντια σε phishing, key logging, shoulder surfing

Πλεονεκτήματα FIDO

Από τα παραπάνω είναι προφανές ότι FIDO είναι ένα εξαιρετικό εργαλείο. Προσφέρει τόσο πλεονεκτήματα στους χρήστες, στις διαδικτυακές υπηρεσίες αλλά και στις εταιρίες.

Τα οφέλη για τους χρήστες είναι ότι είναι ιδιαίτερο απλό στην χρήση του. Απαιτεί από τον χρήστη είτε να μεταφέρει ένα USB είτε απλά να χρησιμοποιήσει τα βιομετρικά του χαρακτηριστικά. Δεν χρειάζεται πλέον να αγχώνεται για την πολυπλοκότητα των κωδικών ούτε αν θα το ξεχάσει ή του τον κλέψουν. Άρα είναι ασφαλέστερη η χρήση του διαδικτύου και των υπηρεσιών που προσφέρονται.

Για τους παρόχους διαδικτυακών υπηρεσιών τους δίνει τη δυνατότητα με μία πολύ εύκολα εγκαταστήσιμη και συντηρίσιμη τεχνολογία να προσφέρουν ασφαλείς υπηρεσίες. Τους προσφέρει υψηλή ασφάλεια βασισμένη σε δημόσια κλειδιά. Δημιουργεί εμπιστοσύνη στους χρήστες ωθώντας τους όλο και περισσότερο στην χρήση διαδικτυακών υπηρεσίων. Το κόστος μειώνεται για τις υπηρεσίες αφού ο χρήστης φέρνει τη δική του συσκευή για την αυθεντικοποίηση. Τέλος, ένα από τα πιο βασικά πλεονεκτήματα του FIDO για τις υπηρεσίες είναι η δυνατότητά του να λειτουργήσει σε πολλαπλές πλατφόρμες και να υποστηρίξει πλήθος μεθόδων αυθεντικοποίησης.

Συμπεράσματα

Στη εποχή μας, η αυθεντικοποίηση είναι η θεμέλιος λίθος όλων των υπηρεσιών καθώς σχεδόν όλη η ζωή μας περνάει μέσα από το διαδίκτυο και τις υπηρεσίες που προσφέρονται. Οπότε είναι προφανές ότι είναι απαραίτητη ένα σύστημα για να εξασφαλίζει ότι ο χρήστης είναι αυτός που δηλώνει και υπάρχει και στον φυσικό κόσμο. Το πρότυπο FiDO έρχεται να προσφέρει αυτή την ασφάλεια και εμπιστοσύνη.

Το πρότυπο FiDO προσφέρει δύο τρόπους αυθεντικοποίησης. Ο ένας χρησιμοποιεί μία συσκευή USB, ένα security token, για την αυθεντικοποίηση του χρήστη και είναι το πρότυπο U2F. Επίσης, προσφέρει ένα άλλο πρότυπο που εκμεταλλεύεται τα βιομετρικά χαρακτηριστικά, το UAF.

Το FiDO εξασφαλίζει ότι καμία εφαρμογή δεν έχει τον ίδιο κωδικό με οποιαδήποτε άλλη. Δεν μπορεί να αντιγραφεί αυτός ο κωδικός. Ένας κακόβουλος θα έπρεπε να υποκλέψει τον κωδικό του χρήστη για μία συγκεκριμένη εφαρμογή και μετά να κλέψει (στον φυσικό κόσμο) το USB security token. Δεν βασίζεται μόνο στη συσκευή U2F αλλά και στο password(σε περίπτωση κλοπής) Στην περίπτωση του UAF θα έπρεπε να βρει τρόπο να παρακάμψει το συγκεκριμένο σετ βιομετρικών χαρακτηριστικών που χρησιμοποιείται. Αλλά τα βιομετρικά στοιχεία δεν μπορούν να αντιγραφούν εύκολα.

Είναι προφανές ότι υπάρχει διαφάνεια της διαδικασίας καθώς ο χρήστης ενημερώνεται σε κάθε βήμα με παράθυρο ειδοποίησης και επιτρέπει ο ίδιος τη συνέχεια της διαδικασίας. Δεν απαιτεί ιδιαίτερο χειρισμό από πλευράς του χρήστη καθώς χρησιμοποιεί τα ίδια του τα χαρακτηριστικά ή ένα απλό USB security token. Ένα ακόμα πλεονέκτημα του FiDO είναι ότι μπορεί να λειτουργήσει σε πολλαπλές πλατφόρμες χωρίς καμία επιπλέον προσθήκη ή αλλαγή.

Αυτά τα δύο πρότυπα του FIDO μπορούν να έχουν ευρεία χρήση. Μπορούν να χρησιμοποιηθούν σε εταιρικά περιβάλλοντα αλλά και σε στρατιωτικά. Ο χρήστης εμπιστευόμενος το πρότυπο αυτό θα αρχίσει να χρησιμοποιεί ολοένα και περισσότερο υπηρεσίες ηλεκτρονικών αγορών και των αντίστοιχων ιστοτόπων που τις προσφέρουν.

Σαν εταιρεία παροχής υπηρεσιών με χρήση FIDO μπορεί να δράσει και το κράτος όπου χρήστης θα είναι ο πολίτης. Θα του προσφέρει υπηρεσίες ηλεκτρονικά που είναι ιδιαίτερα χρονοβόρες και δεν απαιτούν την φυσική του παρουσία. Επίσης, μπορεί να λειτουργήσει και διακρατικά είτε από την πλευρά κρατών της Ευρωπαϊκής Ένωσης για ανταλλαγή πληροφοριών είτε για να προσφέρουν στον πολίτη τη δυνατότητα διεκπεραίωσης υπηρεσιών από άλλη χώρα στην οποία βρίσκεται ή είναι πολίτης.

Στο άλλο σκέλος αυτό το πρότυπο να χρησιμοποιηθεί από στρατιωτικές εφαρμογές για μετάδοση πληροφοριών ή πρόσβαση σε ιδιαίτερα διαβαθμισμένες υπηρεσίες.

Το τελικό συμπέρασμα είναι ότι το FiDO μπορεί να προσφέρει εμπιστοσύνη και αίσθημα ασφάλειας του χρήστη σε παροχή ηλεκτρονικών υπηρεσιών, είτε αυτές οι υπηρεσίες αφορούν ηλεκτρονικό εμπόριο είτε παροχή ηλεκτρονικών δημόσιων υπηρεσιών.

Βιβλιογραφία

[1] FIDO U2F Architectural Overview.

[2]FIDO U2F Javascript API.

[3]FIDO U2F Implementation Considerations.

[4]FIDO UAF Architectural Overview.

[5]FIDO UAF Protocol Specification.

[6]FIDO Security Reference.

[7]Biometrics, https://en.wikipedia.org/wiki/Biometrics.

[8]Facial recognition system, https://en.wikipedia.org/wiki/Facial_recognition_system.

[9]Fingerprint , https://en.wikipedia.org/wiki/Fingerprint.

[10]Retinal Scan, https://en.wikipedia.org/wiki/Retinal_scan.

[11]Iris Recognition, https://en.wikipedia.org/wiki/Iris_recognition.

[12]Palm print, https://en.wikipedia.org/wiki/Palm_print.

[13]Hand Geometry, https://en.wikipedia.org/wiki/Hand_geometry.

[14]Biometric Security Advantages and Disadvantages, http://www.slideshare.net/prabhjeet946/biometric-security-advantages-and-disadvantages#.

[15]The defence forensics and biometrics agency – Biometrics 101, http://www.biometrics.dod.mil/References/Tutorial/Default.aspx.

[16]Password free authentication- Figuring out FIDO, http://searchsecurity.techtarget.com/feature/Password-free-authentication-Figuring-out-FIDO.

[17]IEEE Fingerprints Recognition, http://nemertes.lis.upatras.gr/jspui/bitstream/10889/1402/1/EEE_Fingerprints_Recognition_final.pdf

[18]Biometrics Offers Advantages and Controversies,

http://www.rand.org/natsec_area/products/biometrics.html.

[19]What Is Near-Field Communication?, http://gizmodo.com/5707321/what-is-near-field-communication.

[20]OUR PLANS FOR YUBIKEY NEO & U2F,
https://www.yubico.com/2014/09/yubikey-neo-u2f/.