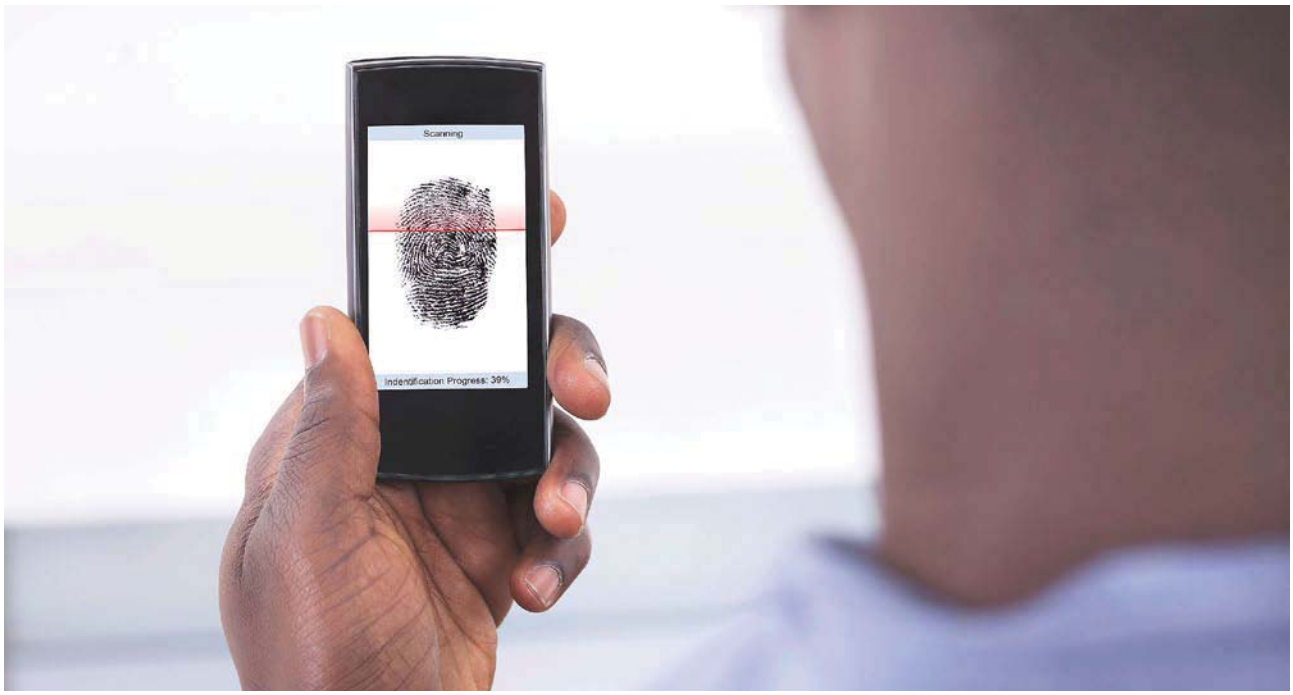
Issue

Killing Passwords: **Strong Authentication** beyond the Password Era

Με το ύψος των ηλεκτρονικών συναλλαγών να υπερβαίνει το ένα τρισεκατομμύριο δολάρια ετησίως και την εμφάνιση του Διαδικτύου των Πραγμάτων (Internet of Things), η ανάγκη για αξιόπιστους και φιλικούς προς τον χρήστη μηχανισμούς αυθεντικοποίησης είναι πιο επιτακτική από ποτέ.

Σήμερα, η πιστοποίηση της ταυτότητας των χρηστών βασίζεται κατά κύριο λόγο στη χρήση κωδικών πρόσβασης (passwords), μια τεχνολογία που αναπτύχθηκε τη δεκαετία του '60. Χάρη στην απλότητα και την ευκολία χρήσης τους, **τα passwords συνεχίζουν να παραμένουν η πιο δημοφιλής μέθοδος αυθεντικοποίησης**, με το 98% των διαδικτυακών υπηρεσιών να τη χρησιμοποιούν, αποκλειστικά, για τον έλεγχο ταυτότητας. Πέρα, όμως, από εξαιρετικά δημοφιλής, η μέθοδος αυτή είναι ιδιαίτερα ανασφαλής, αφού οι χρήστες τείνουν να επιλέγουν ακατάλληλους κωδικούς πρόσβασης, ευμνημόνευτους και συνεπώς, προβλέψιμους. Επιπλέον, οι απαιτήσεις ασφάλειας κρίσιμων υπηρεσιών, όπως αυτών της ηλεκτρονικής τραπεζικής (e-banking), υπερβαίνουν κατά πολύ εκείνες που ικανοποιούνται από τη χρήση απλών συνθηματικών, τα οποία μπορούν εύκολα να κλαπούν ή να παρακαμφθούν. Τέλος, σύμφωνα με μελέτες, το 70% των χρηστών ξεχνούν τον κωδικό τους μία φορά το μήνα, ενώ δοκιμάζουν, κατά μέσο όρο, 2,4 κωδικούς πριν πληκτρολογήσουν το σωστό για να συνδεθούν στην υπηρεσία επιλογής τους.

Τα ανωτέρω προβλήματα δημιούργησαν την **ανάγκη για νέους μηχανισμούς αυθεντικοποίησης, υψηλοτέρων προδιαγραφών, που θα αξιοποιούν τις δυνατότητες των υφιστάμενων τεχνολογιών** και θα επιτυγχάνουν ισορροπία



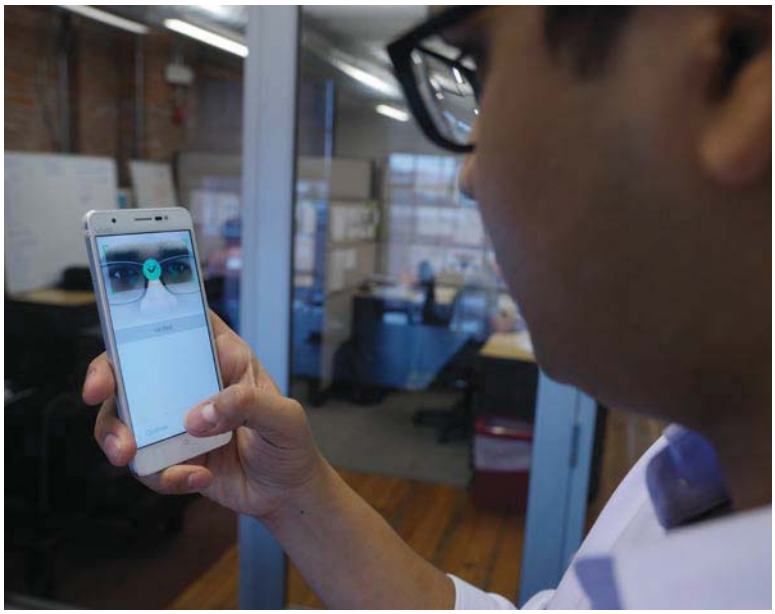
Χρήστος Ξενάκης
Αναπληρωτής Καθηγητής
Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά

Ελένη Βερώνη
Research Associate
Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά

μεταξύ ασφάλειας και ευχρηστίας. Προς αυτή την κατεύθυνση, πολλά πανεπιστήμια και εταιρείες εργάζονται από κοινού για την ανεύρεση εναλλακτικών μεθόδων αυθεντικοποίησης που θα αντικαταστήσουν τους κωδικούς πρόσβασης. Μια λύση αποτελεί η αλλαγή της λογικής πάνω στην οποία βασίζεται ο έλεγχος ταυτότητας ενός χρήστη, με την αντικατάσταση των συνθηματικών που γνωρίζει ο χρήστης, από τα φυσικά χαρακτηριστικά του, όπως το δακτυλικό αποτύπωμα, την ίριδα του ματιού, την αναγνώριση προσώπου, κ.ά. Για την υιοθέτηση των βιομετρικών, όπως ονομάζονται, χαρακτηριστικών, συνετέλεσε καθοριστικά η εξέλιξη και εξάπλωση των έξυπνων κινητών (smartphones), τα οποία διαθέτουν κατάλληλους αισθητήρες για την καταγραφή αυτών, όπως το δακτυλικό αποτύπωμα που χρησιμοποιείται πλέον σε εφαρμογές ηλεκτρονικής τραπεζικής.

Εξέλιξη της βιομετρικής αυθεντικοποίησης, αποτελεί ο **έλεγχος ταυτότητας με βάση τα βιομετρικά χαρακτηριστικά συμπεριφοράς (behavioral biometrics).** Ο τρόπος που περπατάμε, κινούμαστε στην πόλη, μιλάμε ή πληκτρολογούμε μας χαρακτηρίζει μοναδικά σε ικανοποιητικό βαθμό και, συνεπώς, δύναται να χρησιμοποιηθεί αποδοτικά στο πλαίσιο αυθεντικοποίησης. Χαρακτηριστικό παράδειγμα βιομετρικής αυθεντικοποίησης συμπεριφοράς αποτελεί το **Project Abacus της Google** που στοχεύει να εξαλείψει τα passwords από τις συσκευές Android και να τα αντικαταστήσει με τον τρόπο που οι χρήστες αλληλεπιδρούν με τα κινητά τους. Το Abacus δημιούργησε μια μέθοδο αυθεντικοποίησης όπου μέσα από μια ποικιλία δεικτών μέτρησης συνθέτει μια βαθμολογία εμπιστοσύνης (trust score) για το ξεκλείδωμα του κινητού και τη διαβαθμισμένη πρόσβαση σε εφαρμογές, ανάλογα με την κρισιμότητά τους και το επίπεδο ασφάλειας που απαιτούν. Το συγκεκριμένο project είναι σήμερα σε πειραματικό στάδιο.

Παράλληλα με το Abacus, ένα Ευρωπαϊκό ερευνητικό πρόγραμμα βρίσκεται σε εξέλιξη με σημαντική Ελληνική παρουσία, στο οποίο συντονιστής είναι το **Πανεπιστήμιο Πειραιώς** και συγκεκριμένα ο υπογράφων (Αναπλ. Καθηγητής κ. Χρήστος Ξενάκης, Τμήμα Ψηφιακών Συστημάτων). Τίτλος του έργου είναι **«ReCRED: From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control»**, το οποίο χρηματοδοτείται από το Πρόγραμμα Πλαίσιο **Horizon 2020 της Ευρωπαϊκής Ένωσης**. Στο έργο συμμετέχουν συνολικά 12 φορείς, πανεπιστήμια και εταιρείες όπως η Telefonica, Verizon, Cyprus University of Technology, CNIT, Universidad Carlos III de Madrid - IMDEA, UPCOM, EXUS, WEDIA, certSIGN, The Productizers, και Baker & McKenzie, από 8 Ευρωπαϊκές χώρες. Οι στόχοι του ReCRED έχουν αρκετές ομοιότητες με αυτούς του Abacus, αλλά διαφοροποιούνται ως προς τον τρόπο που συλλέγονται, συνδυάζονται και διατηρούνται τα βιομετρικά χαρακτηριστικά των χρηστών. Πιο συγκεκριμένα, το Abacus βασίζεται αποκλειστικά στις πλατφόρμες της Google, η οποία έχει τον πλήρη και αποκλειστικό έλεγχο όλων των δεδομένων αναγνώρισης και ταυτοποίησης των χρηστών. Αντίθετα, το **ReCRED σχεδιάζει και υλοποιεί μια ανοιχτή πλατφόρμα διαχείρισης και πιστοποίησης χρηστών, η οποία συλλέγει μόνο το αποτέλεσμα της βαθμολογίας αυθεντικοποίησης και όχι τα «πρωτογενή» δεδομένα βιομετρικής συμπεριφοράς.**



Βασικές καινοτομίες και πλεονεκτήματα του ReCRED είναι ότι:

α) αποτελεί σχεδιαστική επιλογή η προστασία της ιδιωτικότητας του χρήστη με βάση το Ευρωπαϊκό πλαίσιο,

β) δημιουργείται μια ανοιχτή αρχιτεκτονική, η οποία θα μπορεί να αναπτυχθεί και να χρησιμοποιηθεί από κάθε πάροχο υπηρεσιών, δικτύου, κ.ά. και τέλος,

γ) δίνει τη δυνατότητα σε οργανισμούς που έχουν συνδρομητές (π.χ. online portals, τράπεζες, κτλ.) να παρέχουν νέες υπηρεσίες που σχετίζονται με την αναγνώριση, διαχείριση και ταυτοποίηση χρηστών.

Το ReCRED μεταφέρει όλη την επιβάρυνση μιας διαδικασίας αυθεντικοποίησης από τον χρήστη στην κινητή συσκευή του, χρησιμοποιώντας στο έπακρο τις δυνατότητες που προσφέρουν τα σύγχρονα τηλέφωνα. Έτσι, τα έξυπνα τηλέφωνα εξελίσσονται σε φορείς αυθεντικοποίησης, όπου διαχειρίζονται και αποθηκεύουν, με ασφάλεια, όλους τους λογαριασμούς

Issue

του χρήστη καθώς και την πρόσβαση σε αυτούς, ακολουθώντας σύγχρονα τεχνολογικά πρότυπα που χρησιμοποιούν την ασύμμετρη κρυπτογράφηση (π.χ. FIDO Alliance). Ο χρήστης πιστοποιείται στο κινητό του, τοπικά, χρησιμοποιώντας το **δακτυλικό του αποτύπωμα, την εικόνα του προσώπου του, τον τρόπο βαδίσματος, την κίνησή του στην πόλη, τον τρόπο που πληκτρολογεί στο κινητό του κ.ά.,** και το κινητό μαζί με την πλατφόρμα ReCRED αναλαμβάνει να παρέχει στον χρήστη την πρόσβαση στις υπηρεσίες που επιθυμεί (π.χ. τραπεζικές εφαρμογές, κοινωνικά δίκτυα, κ.ά.). Σε περίπτωση απώλειας ή κλοπής του κινητού τηλεφώνου, όλα τα ευαίσθητα και προσωπικά δεδομένα του χρήστη βρίσκονται είτε κρυπτογραφημένα στη συσκευή είτε σε ένα σημείο αυτής, το οποίο δεν είναι προσπελάσιμο από τρίτους (ακόμα και όταν την έχουν στην κατοχή τους), χρησιμοποιώντας μια νέα τεχνολογία σε επίπεδο υλικού και λογισμικού που ονομάζεται Trusted Execution Environment.

Εκτός από την εξέλιξη των έξυπνων κινητών τηλεφώνων σε φορείς ταυτοποίησης και παροχής πρόσβασης, τα οποία «ανοίγουν» για λογαριασμό του χρήστη όλες τις πόρτες στις οποίες έχει τη δυνατότητα να εισέλθει στον ηλεκτρονικό κόσμο, το ReCRED παρέχει δύο επιπλέον καινοτομίες:

α) την ολοκληρωμένη διαχείριση ηλεκτρονικών λογαριασμών και ταυτοτήτων ενός χρήστη, και

β) την έκδοση ανώνυμων πιστοποιητικών που διασφαλίζουν συγκεκριμένες ιδιότητες του χρήστη, εξασφαλίζοντας παράλληλα την ανωνυμία του.

Σε ό,τι αφορά στην πρώτη, είναι γνωστό ότι η πλειοψηφία των χρηστών του Διαδικτύου σήμερα διαθέτει πολλές εγγραφές σε πλειάδα online εφαρμογών όπως λογαριασμούς email (π.χ. Gmail, Yahoo, κτλ.), κοινωνικά δίκτυα (π.χ. Facebook, Twitter, LinkedIn, κτλ.), τραπεζικές εφαρμογές, εταιρικές εφαρμογές κ.ά. Το ReCRED δίνει τη δυνατότητα παροχής πρόσβασης σε όλες αυτές τις εφαρμογές και διαχείρισης των λογαριασμών τους από ένα μοναδικό σημείο, ανεξάρτητα από τον τρόπο αναγνώρισης και πιστοποίησης που χρησιμοποιεί η κάθε μία, κάνοντας χρήση ακόμα και του αριθμού του κινητού τηλεφώνου του χρήστη. Έτσι, παρέχεται ευχρηστία και ευελιξία στους χρήστες των υπηρεσιών, χωρίς, όμως, να παραβιάζεται ή να υποβαθμίζεται κατ' ελάχιστον το επίπεδο ασφάλειας και προστασίας των ευαίσθητων δεδομένων που απαιτούνται. Ταυτόχρονα, δίνεται η δυνατότητα σε χρήστες που το επιθυμούν να συνδέσουν την ηλεκτρονική τους με την φυσική τους ταυτότητα, προκειμένου να εκτελέσουν αγοραπωλησίες μέσα από ηλεκτρονικές πλατφόρμες όπως το eBay.

Τα ανώνυμα πιστοποιητικά από την άλλη πλευρά, δύναται να δηλώσουν με επαληθεύσιμο τρόπο κάθε ιδιότητα που επιθυμεί ένας χρήστης (π.χ. φύλο, ενήλικας, φοιτητής, συνταξιούχος, κ.ά.), χωρίς την αποκάλυψη κανενός άλλου προσωπικού ή ευαίσθητου στοιχείου της ταυτότητάς του. Εκδίδονται από έμπιστες αρχές που έχουν στην κατοχή τους τέτοια στοιχεία (π.χ. δημόσιες υπηρεσίες, τηλεπικοινωνιακούς παρόχους, τραπεζικά ιδρύματα, πλατφόρμα ReCRED, κ.ά.) και υποβάλλονται κρυπτογραφημένα από τους χρήστες μέσω των κινητών τηλεφώνων σε online υπηρεσίες, και όχι μόνο, που απαιτούν συγκεκριμένες ιδιότητες όπως την έκδοση εκπτωτικών εισιτηρίων, την παροχή κοινωνικών επιδομάτων κλπ. Με τον τρόπο αυτό εξασφαλίζεται, αποδεδειγμένα, η απόλυτη ανωνυμία και προστασία των προσωπικών - ευαίσθητων δεδομένων για τους χρήστες, αλλά ταυτόχρονα, και η τήρηση των κανόνων με αδιαμφισβήτητο τρόπο.

ReCRED

Το ερευνητικό έργο ReCRED αναμένεται να ολοκληρωθεί τον Απρίλιο του 2018, αλλά από το καλοκαίρι του 2017 θα ξεκινήσουν μεγάλης κλίμακας πιλοτικές δοκιμές. **Για περισσότερες πληροφορίες επισκεφτείτε τον ιστότοπο www.recred.eu ή αποστείλατε μήνυμα στο xenakis@unipi.gr.**