



Τεχνολογικό
Πανεπιστήμιο
Κύπρου

Σχολή Μηχανικής και
Τεχνολογίας

Πτυχιακή εργασία

**User-friendly application for anonymous access
to online services**

Κωνσταντίνος Μάμαντος

Λεμεσός, Ιούνιος 2021

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

User-friendly application for anonymous access to online services

Κωνσταντίνος Μάμαντος

Επιβλέπων Καθηγητής

Δρ. Μιχάλης Σιριβιανός

Πνευματικά δικαιώματα

Copyright © Κωνσταντίνος Μάμαντος, 2021

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Τεχνολογικού Πανεπιστημίου Κύπρου δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον Δρ Μιχάλη Σιριβιανό για την εμπιστοσύνη που μου έδειξε αναθέτοντας μου αυτή την πτυχιακή εργασία. Επίσης θα ήθελα να ευχαριστήσω τον κύριο Μάρκο Χαραλάμπους, μέλος της ερευνητικής ομάδας του κ Σιριβιανού για τον όλο συντονισμό, τις εισηγήσεις και τις οδηγίες του για την διεκπεραίωση ολόκληρης της εργασίας.

ΠΕΡΙΛΗΨΗ

Οι υφιστάμενοι τρόποι αυθεντικοποίησης στο διαδίκτυο παρουσιάζουν σοβαρές αδυναμίες. Πρώτα απ' όλα βασίζονται στον παραδοσιακό τρόπο του κωδικού πρόσβασης, μειώνοντας την ασφάλεια και την ευκολία χρήσης του τελικού χρήστη. Κατά δεύτερον, η έλλειψη αυθεντικοποίησης βάσει χαρακτηριστικών δεν επιτρέπει τη διατήρηση της ανώνυμης πρόσβασης στις υπηρεσίες. Κατά τρίτον, οι χρήστες έχουν πολλούς διαδικτυακούς λογαριασμούς που συχνά αντανακλούν ξεχωριστές πτυχές ταυτότητας. Αυτό καθιστά δύσκολη την απόδειξη συνδυασμών των χαρακτηριστικών ταυτότητας στους χρήστες. Ο κύριος σκοπός της παρούσας πτυχιακής είναι να υλοποιηθεί μια φιλική προς τον χρήστη εφαρμογή για την πλατφόρμα του "INCOGNITO" που θα επιτρέψει στους χρήστες να κατανοήσουν με ευκολία τι χρειάζεται για να έχουν πρόσβαση στις διαδικτυακές υπηρεσίες σχετικά με την ιδιωτικότητα και την απόδειξη συγκεκριμένων χαρακτηριστικών της ταυτότητας τους ή ολόκληρη την ταυτότητα τους. Επιπλέον η πλατφόρμα του INCOGNITO χρησιμοποιεί προχωρημένο λογισμικό σε κινητές εφαρμογές για να μετατρέψει διαδικτυακές και φυσικές αποδείξεις ταυτότητας σε επικυρωμένες και κρυπτογραφικά ισχυρές αποδείξεις των ταυτοτήτων που μπορούν να χρησιμοποιηθούν για να πάρουν πρόσβαση σε διαδικτυακές υπηρεσίες. Επίσης, η πλατφόρμα του "INCOGNITO" συνδέεται με φυσικούς και διαδικτυακούς Identity Providers για να αποκτήσει τα χαρακτηριστικά της ταυτότητας.

Λέξεις κλειδιά: Διαδικτυακές Υπηρεσίες, Εξουσιοδότηση Αυθεντικοποίηση, κρυπτογράφηση, βιομετρικά

ABSTRACT

Current authentication methods on the Web have severe weaknesses. First, services massively rely on the traditional password paradigm, reducing the end-users security and usability. Second, the lack of attribute-based authentication does not allow anonymity-preserving access to services. Third, users have multiple online accounts that often reflect distinct identity aspects. This makes proving combinations of identity attributes hard on the users. This thesis's primary purpose is to implement a user-friendly application for the "INCOGNITO" platform that will allow users to easily understand what is needed to access online services concerning their privacy and prove specific attributes of their identity or their whole identity. Moreover, the "INCOGNITO" platform uses advanced software on mobile devices to convert online and physical identity proofs into validated and cryptographically strong proofs of identities that can then be used to get access to Online Services. Also, the "INCOGNITO" platform connects with Physical and Online Identity Providers in order to acquire identity attributes.

Keywords: Web services, authorization, authentication, encryption, biometrics