

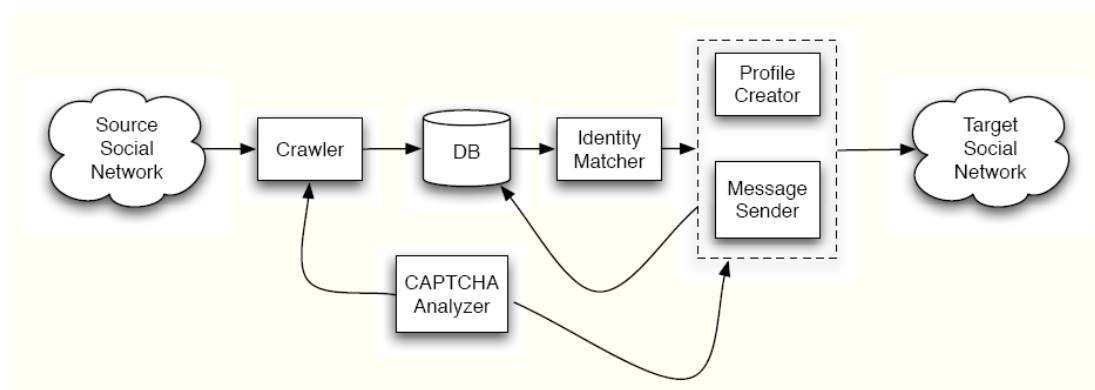
All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks

Το paper παρουσιάζει πόσο εύκολα θα μπορούσε ένας πιθανός attacker να κάνει αυτοματοποιημένο crawling και επιθέσεις «Κλοπής Ταυτότητας» (Identity theft) εναντίον σε έναν αριθμό από διάσημα social networking sites με απώτερο σκοπό να αποκτήσει πρόσβαση σε ένα μεγάλο όγκο προσωπικών και ευαίσθητων δεδομένων των χρηστών.

Τα δύο είδη επιθέσεων που προτείνουν οι συγγραφείς είναι:

1. Η κλωνοποίηση ενός ήδη υπάρχοντος profile σε ένα Social Network και η αποστολή friend requests σε όλες τις επαφές του με σκοπό τη απόκτηση όσο το δυνατόν περισσότερης πληροφορίας.
2. Μια αυτοματοποιημένη *cross-site profile cloning* επίθεση, όπου εδώ ο attacker προσπαθεί να κάνει clone ένα profile ενός χρήστη, ο οποίος είναι ήδη εγγεγραμμένος σε ένα social network, και να το δημιουργήσει σε ένα άλλο social network όπου ο χρήστης δεν είναι εγγεγραμμένος εκεί ακόμα. Μετά, αυτό που προσπαθεί να κάνει είναι να ξανακτίσει το social network του θύματος.

Υλοποιούν τις επιθέσεις τους σε ένα prototype system που το ονομάζουν *iCloner* (Identity Cloner) και η αρχιτεκτονική του παρουσιάζεται παρακάτω:



Το σύστημα αποτελείται από 4 βασικά components:

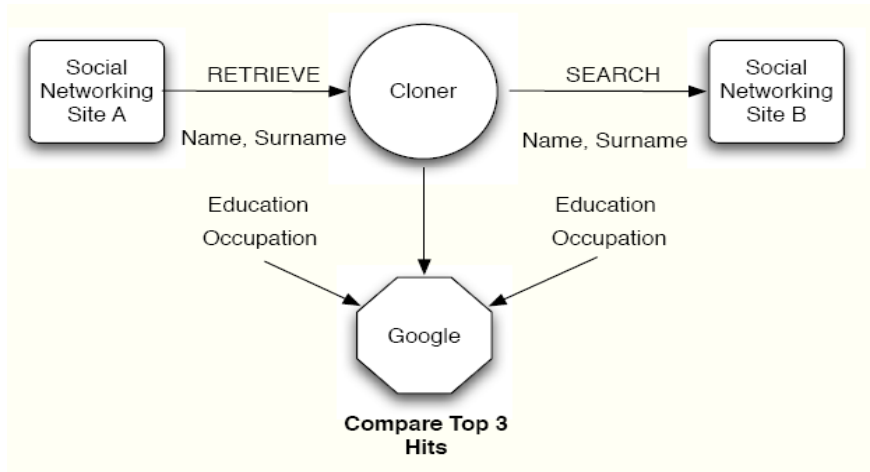
- Τον crawler, ο οποίος είναι υπεύθυνος να κάνει crawl ένα networking site και να συλλέγει πληροφορίες που τα profile τους είναι public. Είναι ικανός να κάνει crawl

στα StudiVZ, MeinVZ, Facebook και XING και να συλλέγει πληροφορίες από contact lists και profiles, αν αυτά είναι publically προσβάσιμα. Επίσης κρατάει πληροφορία για τα user profiles από τα οποία δεν μπόρεσε να αντλήσει πληροφορία λόγω των περιοριστικών access settings που έχουν).

- Τον Identity Matcher, ο οποίος αναλύει τα data που προέκυψαν απ' τον crawler και αποθηκεύτηκαν στη database και ψάχνει να βρει profiles σε διαφορετικά social networks που ανήκουν στο ίδιο άτομο.
- Τον profile creator, που χρησιμοποιεί τη πληροφορία που παράγει ο Identity Matcher για να δημιουργήσει accounts σε social networks όπου τα θύματα δεν έχουν κάνει εγγραφή, ή να κάνει duplicate ένα ήδη υπάρχον profile μέσα στο ίδιο network.
- Και τον Message Sender, ο οποίος κάνει login στα created accounts που δημιούργησε ο Profile Creator, και αυτόματα στέλνει friend requests σε όλους όσους είναι γνωστό ότι είναι φίλοι με το victim.

Επειδή σε κάποια social networking sites μπορεί να χρειάζεται η επίλυση κάποιων CAPTCHA, π.χ. όταν κάποιος πάει να δημιουργήσει ένα καινούργιο account, να στείλει ένα friend request, ή μερικές φορές όταν πάει να κάνει access ένα profile, οι συγγραφείς έκαναν ανάλυση των CAPTCHA που χρησιμοποιούνται από το StudiVZ, MeinVZ και το Facebook και σχεδίασαν (χρησιμοποιώντας open source tools) τεχνικές έτσι ώστε να σπάνε αυτά τα CAPTCHA με success rate που καθιστά τις αυτόματες επιθέσεις τους πραγματοποιήσιμες. Οι αλγόριθμοι αυτοί είναι ενσωματωμένοι στον extra component του iClone, τον CAPTCHA analyzer.

Αν ψάξει κανείς σε ένα social network για ένα profile πολλές φορές τα αποτελέσματα της αναζήτησης είναι πολύ περισσότερα του ενός, για να διαπιστώσουν οι συγγραφείς ότι ένα account δεν υπάρχει σε ένα social network, ή 2 accounts είναι ακριβώς τα ίδια σε 2 social networks, εκτός από το profile name σύγκριναν και άλλα πεδία και κρατούσαν ένα score. Αν στο τέλος αυτό το score ήταν μεγαλύτερο από ένα threshold, τότε τα 2 accounts ανήκουν στο ίδιο άτομο. Επίσης, για να συγκρίνουν τα values ενός πεδίου για 2 profiles, ένα απλό string matching δεν αρκούσε οπότε δημιούργησαν ένα query που περιείχε και τα 2 terms μαζί και έκαναν search στο Google. Αν τα top 3 αποτελέσματα περιείχαν και τους 2 όρους, τότε οι τιμές του συγκεκριμένου πεδίου και στα 2 profiles ήταν ίδιες.



Αρχικά έκαναν κάποια πειράματα για να αξιολογήσουν τον crawler τους. Δημιούργησαν 16 accounts στα StudiVZ και meinVZ και 16 για το XING και συγκέντρωσαν έναν μεγάλο αριθμό από profiles από κάθε social network. Μετά πραγματοποίησαν το πρώτο είδος επίθεσης κάνοντας duplicate 5 profiles που υπήρχαν ήδη στο facebook και με ίδιο όνομα και εικόνα και έστειλαν friend requests σε όλους τους φίλους του θύματος. Επίσης έκανα το ίδιο και για άλλα 5 profiles που με random ονόματα και εικόνες για να μελετήσουν την αποδοτικότητα του profile cloning σε αυτές τις 2 περιπτώσεις. Παρατηρούν ότι το acceptance rate των requests που έγιναν από τα duplicate profiles είναι μεγαλύτερο από το αντίστοιχο των αυθαίρετων profiles, άρα καταλήγουν στο συμπέρασμα ότι η επίθεση που περιγράφουν όντως είναι αποτελεσματική. Δοκιμάζουν επίσης να στείλουν και κάποιο suspicious μήνυμα με ένα URL στο body του, στους friends των 2 set από profiles χωρίς να αλληλεπικαλύπτονται και διαπιστώνουν ότι και στις 2 περιπτώσεις το click rate ήταν το ίδιο. Τέλος, πραγματοποιούν και το δεύτερο είδος επίθεσης δημιουργώντας 5 XING accounts στο LinkedIn και στέλνουν friend requests σε όλους του friends του κάθε account. Λίγο περισσότερα από τα μισά friend requests έγιναν δεκτά, οπότε αυτό το ποσοστό είναι αρκετό για να ισχυριστούν ότι και το δεύτερο είδος επίθεσης που προτείνουν είναι αποτελεσματικό.

Σαν τρόπους αντιμετώπισης σε τέτοιου είδους επιθέσεις προτείνουν οι Social Network Providers:

- να προσφέρουν περισσότερη πληροφορία για το authentication των friend request που δέχονται οι χρήστες τους (π.χ. από ποια χώρα ήρθε το request με βάση την IP address του μηχανήματος, την ημερομηνία δημιουργίας του profile).
- Να κάνουν τα CAPTCHA πιο ανθεκτικά σε OCR τεχνικές.
- Να προσθέσουν rate limit στον αριθμό των διαφορετικών CAPTCHA που μπορούν να εμφανίζονται στο χρήστη ανά μονάδα χρόνου. Π.χ. λίγες εικόνες ανά λεπτό.
- Να υιοθετήσουν, ή να βελτιώσουν behavior-based anomaly detection τεχνικές για να ανιχνεύουν και να κάνουν block crawling και άλλου είδους ύποπτη δραστηριότητα όπως π.χ. η αποστολή από εκατοντάδες friend requests σε μικρό χρονικό διάστημα.

