ΠΡΟΣ

1) **Ολα τα μέλη ΔΕΠ του Τμήματος Επιστήμης Υπολογιστών**
2) **Τους εκπροσώπους των Μεταπτυχιακών φοιτητών του Τμήματος Επιστήμης Υπολογιστών**
3) **Την Επταμελή Εξεταστική Επιτροπή**
4) **Ολα τα μέλη της Πανεπιστημιακής Κοινότητας**

Πρόσκληση σε Δημόσια Παρουσίαση της Διδακτορικής Διατριβής του

κ. Πολάκης Ιάσων - Στυλιανός

Την Πέμπτη, 20 Φεβρουαρίου 2014 και ώρα 16:00 στην αίθουσα " Σ. Ορφανουδάκης" του Ινστιτούτου Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας (ΙΤΕ) το Ηράκλειο, θα γίνει η δημόσια παρουσίαση και υποστήριξη της Διδακτορικής Διατριβής του υποψηφίου διδάκτορος του Τμήματος Επιστήμης Υπολογιστών κ. Πολάκη Ιάσων – Στυλιανός με θέμα:

"Υπηρεσίες κοινωνικής δικτύωσης από την σκοπιά του επιτιθέμενου: καινοτόμες τεχνικές επιθέσεων και αμυντικοί μηχανισμοί"

" Online Social Networks from a Malicious Perspective: novel attack techniques and defense mechanisms"

ΠΕΡΙΛΗΨΗ

Οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν τις πιο δημοφιλείς ψηφιακές υπηρεσίες, καταλαμβάνοντας την πλειοψηφία του χρόνου που ξοδεύουν οι χρήστες στο Διαδίκτυο. Αυτές οι υπηρεσίες έχουν εξελιχθεί σημαντικά απο την μορφή που κατείχε η πρώτη γενιά τους, και προσφέρουν μια εκτενής συλλογή λειτουργιών όπως αλληλεπίδραση μεταξύ χρηστών, ανταλλαγή περιεχομένου, διαδικτυακά παιχνίδια και υπηρεσίες καθολικής σύνδεσης (single sign on). Αυτές οι υπηρεσίες έχουν πολύ σημαντική επίδραση στο Διαδίκτυο, και έχουν μεταβάλλει αμετάκλητα την έννοια της ιδιωτικότητας στην ψηφιακή εποχή. Ένα φυσικό επακόλουθο της δημοτικότητας τους είναι και η στοχοποίηση τους απο κακόβουλους χρήστες με σκοπό το κέρδος.

Η τεράστια συλλογή προσωπικών δεδομένων και ενδιαφερόντων των χρηστών που έχουν συλλέξει αυτές οι υπηρεσίες, καθώς και η εμπιστοσύνη που δείχνουν οι χρήστες στα μηνύματα που λαμβάνουν απο άλλους χρήστες αυτών των υπηρεσιών, καταστούν τις υπηρεσίες κοικωνικής δικτύωσης ιδανικό εφαλτήριο για την μετάδοση κερδοφόρων εξατομικευμένων επιθέσεων. Οι επιθέσεις σε αυτά τα δίκτυα μπορούν να βασιστούν στην πραγματογνωμοσύνη επιθέσεων απο πιο.παραδοσιακά μέσα

(π.χ., spam στο ηλεκτρονικό ταχυδρομείο), και να ενσωματώσουν νέες τεχνικές για την δημιουργία σύνθετων και πολύπλοκων επιθέσεων. Η διαρκής εξέλιξη αυτών των υπηρεσιών και η συνεχής ενσωμάτωση νέων λειτουργιών εισάγει νέες ευπάθειες (vulnerabilities) που μπορούν να εκμεταλλευθούν οι επιτιθέμενοι.

Η έρευνα για την ασφάλεια σε υπηρεσίες κοινωνικής δικτύωσης επιβάλλει μια επιθετική προσέγγιση όπου οι ερευνητές "αναλαμβάνουν το ρόλο" του επιτιθέμενου όταν εξερευνούν τα αμυντικά μέσα αυτών των υπηρεσιών. Η "κλειστή" (proprietary) φύση τους περιορίζει την εκτέλεση τους στα ελεγχόμενα πλαίσια ενος εργαστηρίου, και απαιτεί μια black-box προσέγγιση καθώς οι εσωτερικοί μηχανισμοί τους είναι άγνωστοι. Αυτό έχει ως αποτέλεσμα οι ερευνητές να πρέπει να αλληλεπιδρούν με τις πραγματικές υπηρεσίες και τους χρήστες τους. Μόνο τότε μπορούν να προβλέψουν τεχνικές που μπορεί να υιοθετήσουν μελλοντικά οι επιτιθέμενοι, και να αναπτύξουν αποτελεσματικές αμυντικές τεχνικές που θα εμποδίσουν τις πραγματικές επιθέσεις.

Σε αυτή την εργασία επιδεικνύουμε οτι με την χρήση λειτουργιών απο διάφορες ηλεκτρονικές υπηρεσίες με τρόπους για τους οποίους δεν έχουν σχεδιαστεί, μπορούμε να "χτίσουμε" και να εξαπολύσουμε καινοτόμες επιθέσεις που είναι αποτελεσματικές αλλά και πρακτικές με τις ισχύουσες συνθήκες. Τα αποτελέσματα απο τα πειράματα μας αποκαλύπτουν τον ευπαθή σχεδιασμό των υπάρχοντων αμυντικών μηχανισμών που χρησιμοποιούν οι υπηρεσίες κοινωνικής δικτύωσης, και την αδυναμία τους να προστατέψουν τα κεφάλαια τους απο τους επιτιθέμενους. Τα χαρακτηριστικά των.επιθέσεων μας και τα πειραματικά αποτελέσματα μας, καθοδηγούν τον σχδιασμό και την υλοποίηση καινοτόμων αμυντικών μηχανισμών.

Προσδιορίζουμε τα εξής στοιχεία ως κεφάλαια για τις υπηρεσίες κοινωνικής δικτύωσης που πρέπει να προστατεύονται απο κακόβουλους χρήστες: (i) οι πληροφορίες των χρηστών, (ii) οι λογαριασμοί (accounts) των χρηστών και (iii) οι ενέργειες των χρηστών. Αναλαμβάνουμε τον ρόλο του επιτιθέμενου και εξαπολύουμε επιθέσεις που παρακάμπτουν τους αμυντικούς μηχανισμούς (αν υπάρχουν) που έχουν ως σκοπό να προστατεύουν αυτά τα κεφάλαια. Πρώτα εξερευνούμε διάφορες τεχνικές για συλλογή και συσχετισμό.προσωπικών δεδομένων χρηστών που μπορούν να χρησιμοποιηθούν για εξατομικευμένες επιθέσεις. Στη συνέχεια, επιδεικνύουμε την αποτελεσματικότητα των επιθέσεων ενάντια σε μηχανισμούς πιστοποίησης χρηστών που χρησιμοποιούν φωτογραφίες. Τέλος, διεξάγουμε εκτενή πειράματα για να εξερευνήσουμε τους αμυντικούς μηχανισμούς υπηρεσιών κοινωνικής δικτύωσης για την ανίχνευση ενεργειών απο κακόβουλους χρήστες.που κάνουν χρήση λειτουργιών που βασίζονται στην γεωγραφική θέση του χρήστη. Σε κάθε περίπτωση βασιζόμενοι στα πειραματικά μας αποτελέσματα, σχεδιάζουμε μηχανισμούς για την μείωση ή πρόληψη (αν είναι εφικτό) των επιθέσεων μας.

Επόπτης: Καθηγητής Ευάγγελος Π. Μαρκάτος

ABSTRACT

Social networking services have become the most popular digital services, occupying the majority of the time users spend online. These services have greatly evolved from the first generation of social networks, and offer an expansive set of functionality

ranging from user interaction and content sharing, to online gaming and single sign-on services. These services have inadvertently and irrevocably affected the World Wide Web, and forever altered the notion of privacy in the digital era. A natural consequence of their popularity was to also draw the attention of the Internet miscreants that target users for profit.

The vast amounts of personal information and interests that users divulge in these services, along with the high amount of trust users implicitly show to communication received within such networks, has rendered online social networks the ideal springboard for deploying highly- profitable personalized attacks. Attacks in social networks can build upon the expertise of more traditional attack vectors (e.g., email spam) and also incorporate novel techniques for creating complex and intricate attacks. The ever-evolving nature of these networks and the continuous incorporation of novel functionality introduce new design vulnerabilities, which can be exploited by adversaries.

Security research in social networks mandates that researchers assume the role of the adversary when exploring the security aspects of these services. Their proprietary nature restricts their deployment in the controlled environment of a laboratory, and may require a black-box testing approach, as their internal mechanisms are often unknown. As such, researchers must interact with the actual services and their users. Only then will they be able to "anticipate" techniques that adversaries may employ in the future, and develop effective defense mechanisms that will hinder the actual attacks.

In this dissertation we demonstrate that by misusing functionality found in various online services and social networks, we can build and deploy novel attacks that are effective while remaining practical. The results of our experiments reveal the vulnerable design of existing defense mechanisms employed by social networks and their inability to protect their assets from adversaries. The characteristics of our attack techniques and the outcome of our experiments guide the design and implementation of new defense mechanisms.

Specifically, we identify the following resources as the "assets" of social networking services, which should be protected against adversaries: (i) user information, (ii) user accounts and (iii) user actions. We assume the role of the attacker and deploy attacks that bypass any mechanisms (if any) deployed for protecting each type of asset. First, we explore various techniques for harvesting and correlating (personal) user information that can be and used for crafting personalized attacks. Next, we demonstrate the effectiveness of automated attacks again photo-based authentication mechanisms designed to hinder adversaries from compromising user accounts. Finally, we conduct extensive experiments to explore the defense mechanisms deployed by social networks to detect and remove actions by malicious users in regards to location-based functionality. In each case, based on the insight gained from our experiments we design mechanisms for mitigating or (if possible) preventing our attacks.

Supervisor: Professor Evangelos P. Markatos