OSN Attack
Automated Identity Theft Attacks

John LePage
Department of Electrical & Computer Engineering
Missouri University of Science and Technology

jlpc5@mst.edu
Presentation Overview

Outline

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
Presentation Overview

Outline

- Introduction
- iCloner Overview
- Cloning Attacks
- Testing
- Defense
- Conclusion
Introduction

Social Networks

• There are many social networking sites out there
• LinkedIn
  – Business relationships
  – Over 30 million registered users[1]
• Facebook
  – Relationships based around friendships
  – Over 150 million registered users [2]
  • Growing by 3% per week [3]
  • Over 1 billion uploaded photos[3]
Introduction
Attractive to Attackers

• Why do social media sites draw attackers?
  – There are many users who also have a large contact pool

• Attackers gain access to real information
  – They can easily find out real email addresses
  – Also get detailed information about users

• Also many social media sites do not screen content
  – Easier for malicious programs to get through
Introduction
Ease of Attack

- This presentation will show just how effectively an attacker can gain the trust of someone by using a fake account
Presentation Overview

iCloner Overview

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
iCloner Overview [4]

Introduction

• iCloner is a system for creating fake accounts
  – Collects information on users
  – Automatically creates profiles
  – Automatically sends friend requests
  – Passes CAPTCHAs

iCloner Overview [4]

Crawler Component

• The crawler component
  – Runs through social media sites
  – Collects publicly available information
  – Contact/Friend lists
  – Keeps track of non-public profiles

http://ui-patterns.com/patterns/friend-list
iCloner Overview [4]

Identity matcher

- Attempts to find existing accounts
  - Scans different profiles looking for a match
- Makes an account
  - Either find sites where the profile doesn’t exist yet
  - Or, create duplicate accounts on sites where the profile already exists.
iCloner Overview [4]

Breaking CAPTCHAs

- Usually required in account creation on many sites
  - Completely Automated Public Turing test to tell Computers and Humans Apart

iCloner Overview

Breaking CAPTCHAs

• Facebook CAPTCHAs
  – reCAPTCHAs
  – Contain meaningful words
  – One is already proven to not be able to be read by the system
  – Other has already been correctly identified

• The fact that one of the words already cannot be read greatly increases security
  – User’s contribution greatly increases accuracy
iCloner Overview [4]

Breaking CAPTCHAs

• Breaking reCAPTCHAs
  – First need to try and un-distort the words
  – Then words are extracted using image filters
  – The words are checked against the English Dictionary
  – If the word is not in the Dictionary it is googled
  – If the number of results is above a certain threshold the word is used
  – Otherwise the word google suggests is chosen

https://fakecaptcha.com/
iCloner Overview [4]

Breaking CAPTCHAs

• iCloner was able to correctly answer, on average, 14% of the tested reCAPTCHAs

• Since this is only needed a handful of times an attack is still feasible
  – Creation of the account
  – Sending certain friend requests
Presentation Overview

Outline

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
Cloning Attacks [4]

Overview

- Users are generally not cautious when accepting friend requests
- This is how the attacker gains access to someone’s information
Cloning Attacks [4]

Attack Method

- Attacks typically involve the attacker sending a link to the victim to follow
  - Get site visits
  - Download malicious software

Cloning Attacks [4]

Cross-site Attack

- Users have profiles on one site, but not on others
- Attackers will create an account on these sites
  - Use information from other accounts
- Start to send requests based on the other accounts’ contacts
Presentation Overview

Outline

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
Crawling Experiments

- Tests were performed on the sites StudiVZ and MeinVZ by Bilge, Strufe, Balzarotti, and Kirda
- Each of 16 accounts requested 6,000 web pages per day
  - Broke around 215 CAPTCHAs
- Collected information on roughly 40,000 profiles
Testing

Cloning

• Five accounts were cloned
  – With original owner’s consent
• Contacted 705 people in total
• Acceptance rate of around 60%
  – As high as 90%

• The accounts then sent a link
• Contained a personalized message for the appropriate contact
• Frequency of clicking on the link was around 50%
  – Could lead to potential attacks

Hey, I put some more pictures online. Check them here!: http://193.55.112.123/userspace/pix?user=<account>&guest=<contact>&cred=3252kj5kj25kjk325hk
Ciao, <account first-name>
Presentation Overview

Outline

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
• Provide more information from the sender
  – To help verify authenticity of the request
Defense [4]
Preventing Attacks

- Make CAPTCHAs more difficult to break
  - More overlapping characters
Defense [4]

Preventing Attacks

• Limit the number of times a new CAPTCHA can be requested
  – Otherwise, can just request until there is an easy one to solve
Presentation Overview

Outline

• Introduction
• iCloner Overview
• Cloning Attacks
• Testing
• Defense
• Conclusion
Conclusion

• Very real threat
  – Can affect anyone

• Need to develop more effective strategy to ensure authenticity of accounts
References and Further Reading

• [1] LinkedIn. http://www.linkedin.com,
• [3] Facebook by the Numbers.
End of Foils