

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

HY558 – spring 2010

Thanasis Petsas

CSD, Universtity of Crete

# In a nutshell

how easy it would be for a potential attacker to launch automated **crawling and identity theft attacks** against a number of popular social networking sites in order to gain access to a large volume of personal user information

# Social Networks

- a social structure that is made up of nodes representing individuals or organizations
- a relatively new phenomenon on the Internet
- Business relationship-focused
  - XING: 5 million registered users
  - LinkedIn: 30 million registered users
- friendship-focused
  - Facebook: 150 million active users (growth 3%/week)
  - MySpace
  - StudiVZ
  - MeinVZ

# New technology: An attraction of attackers

- as more and more people started using e-mail, unsolicited e-mails (i.e, spam, phishing, those with worm attachments) started increasing in numbers
- about 90% of the incoming e-mail traffic in North America, Europa and Australasia is spam
- As the popularity of social networking sites increase, so does their attractiveness for criminals
- Worms recently target SN sites like Facebook and MySpace
  - Use the friend lists of a victim to spread
  - Although such e-mail attachments may raise more suspicion (by many e-mail users), they are not as well-known on social networking sites
- emails are often scanned for malicious content, whereas SN sites do not usually provide **filtering** → easier for an attacker to launch their campaigns

# Automated identity theft attacks

- **1<sup>st</sup> attack:** They clone an already existing profile in a SN and send friend requests to the contacts of the victim
- **2<sup>nd</sup> attack:** launch an automated, *cross-site profile cloning* attack. Clone the identity of a victim in the site where he is registered, and forge it in a social networking site where he is not registered yet. Then attempt to rebuild the social network of the victim
- They implement their attacks in a prototype system called iCloner (identity Cloner)

# Contributions

- They present 2 automated identity theft attacks: **Profile Cloning** and **cross-site profile cloning**
- there is significant room for improvement to make CAPTCHAs more difficult to break
- present experimental results with real users and show that the attacks they present are feasible in practice in **5** popular social networking sites
- We make suggestions on how social networking sites can improve their security



# Breaking CAPTCHAs

following

finding

SMmm

- CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart
- CAPTCHA algorithm: the ability to generate tests that are at the same time easily solvable by humans, but very hard to solve for a computer application
- should be resistant against Optical Character Recognition (OCR) techniques
- develop a number of CAPTCHA breaking techniques based on a set of open source tools (**ImageMagick** for image filtering, **Tesseract** for the text recognition using OCR)
- and custom-developed scripts (**Python** and **Perl** scripts to partition the CAPTCHAs and to apply manipulations at the pixel level)

# Breaking CAPTCHAs (MeinVZ and StudiVZ)

- Each of them: contains **5 letters**, each letter in a **different font**, with different foreground and background **colors**, often tilted scaled or blurred, and have a simple **grid-based noise**
- They wrote scripts:
  - To detect and remove grid noise
  - Replace background with white pixels
  - Identify connected areas & isolate the letters (in case of overlappings ask the service for a new CAPTCHA)
  - scale all letters to the same size, convert them to B&W
- They use **Tesseract** to recognize the letters for a set of known fonts
- Their tool is able to match all letters correctly 88.7% of the time
- Considering the fact that both MeinVZ and StudiVZ ban the user after three mistakes, they can solve the CAPTCHA with 99.8% probability in one of the three consecutive attempts

# Breaking CAPTCHAs (Facebook reCAPTCHAs)



- Facebook uses reCAPTCHA: a state-of-the-art approach
- Steps
  - Unbend the word back to the original shape (tool extracts the middle line of each word)
  - Translate each pixel column up or down so that the approximating curve becomes a straight line
  - Then an analysis follows similar to the one for the MeinVZ and StudiVZ with Tesseract
  - Then each word is compared with content of [English dictionary](#), and if that fails they submit the word to [Google](#)
- an attacker could use a botnet to have access to thousands of different IPs and distribute the CAPTCHA breaking effort among many hosts

# Profile Cloning Attack

- Users are generally not cautious when accepting friend requests
- The profile cloning attack consists of identifying a victim and creating a new account with his **real name** and **photograph** inside the same social network and automatically contact the friends of the victim
- Names are not unique in SNs
- They didn't add any message to the friend requests in order to evaluate the worst case scenario
- iCloner supports profile cloning attacks on Facebook

# Cross-site Profile Cloning

- Identify victims who are registered in one social network, but not in another, steal their identities and create accounts for them in the network where they are not registered
- it is much easier for an attacker to create forged accounts in social networks **of the same nature**
- the type of information that users provide in their profiles are of similar nature
  - Education
  - previous jobs and current jobs
  - city and country they live in
- iCloner is able to **automatically compare and forge accounts** from XING to LinkedIn

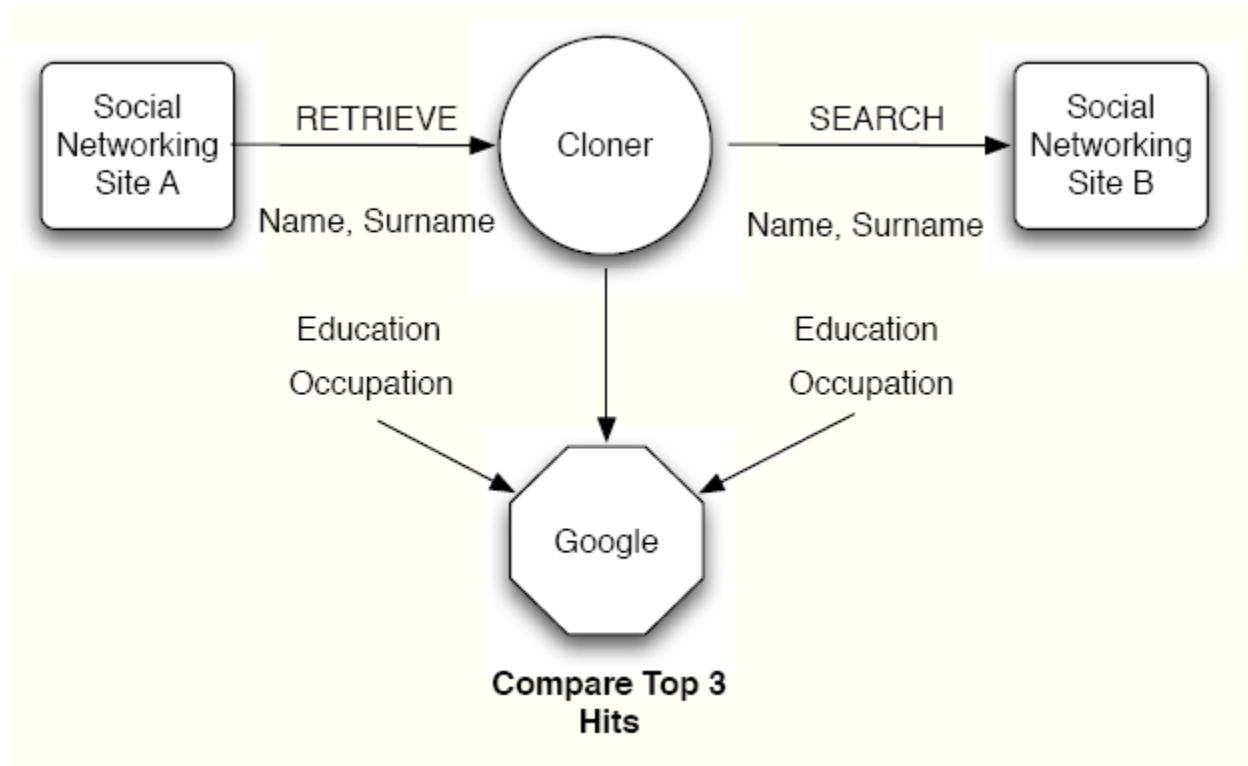
# Cross-site Profile Cloning

- after the stolen identity has been created, they have to **identify the friends of the victim** in the original network and check which of them are registered in the target network
- Not so simple: a simple search for a name may return multiple accounts
- Simple scoring system

Matching Fields	Score
Education	2 points
Company	2 points
City & Country	1 point

- If the total score is at least 3 → the 2 profiles belong to the same person

# Determine if information is identical



- Some users may enter different names for the same type of information e.g. “TU Wien” & “Vienna University of Technology”

# Crawling Experiments

- They created 16 user accounts in StudiVZ and MeinVz
- To keep a low profile they implement slow delays for each page request
- Each crawler instance requested and parsed 6000 pages/day and encountered on average 215 CAPTCHAs to break
- Total: 40.000 profiles/day
- They stopped the experiment after they had crawled more than **5 million** public user profiles with contact information and more than **1.2 million** profiles with complete user information

# Crawling Experiments

- They used similar experimental setup for XING
- XING does not contain CAPTCHA, instead **disable** accounts that are generating high number of requests
- each account was able to crawl around 2000 profiles before it get disabled
- They crawled **118,000** profiles in total, before they stopped the experiment

# Profile Cloning Experiments

- Using iCloner, they duplicate 5 user profiles (D1,... , D5) in **facebook** with same name and picture
- Then iCloner sent requests to all contacts for each victim (705 users in total)
- They create 1 fictitious profile for each forged profile (F1, ... , F5) with random names and pictures
- Measure the effectiveness of profile cloning in these two cases

# Profile Cloning Experiments

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>

- How much trust users would have in messages that they would receive from their new contacts
- They created a simple non-personal message containing a suspicious link
- First they sent the link to the users that had accepted the requests from their fictitious accounts
- And then they sent it to contacts of the forged accounts, that hadn't received it yet

# Profile Cloning Evaluation

Fraction of accepted contact requests

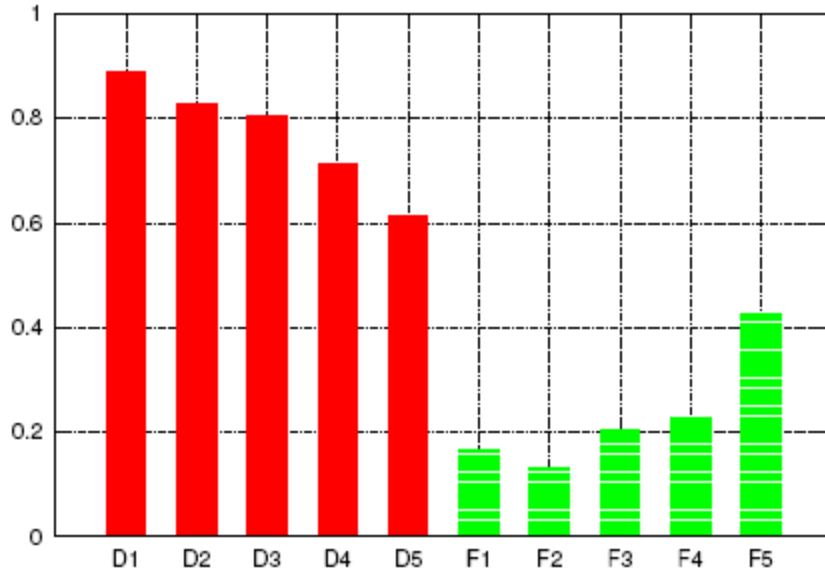


Figure 3: The fraction of accepted contact requests (D1..D5 are the forged profiles, and F1..F5 are the fictitious profiles)

Fraction of clicked spam links

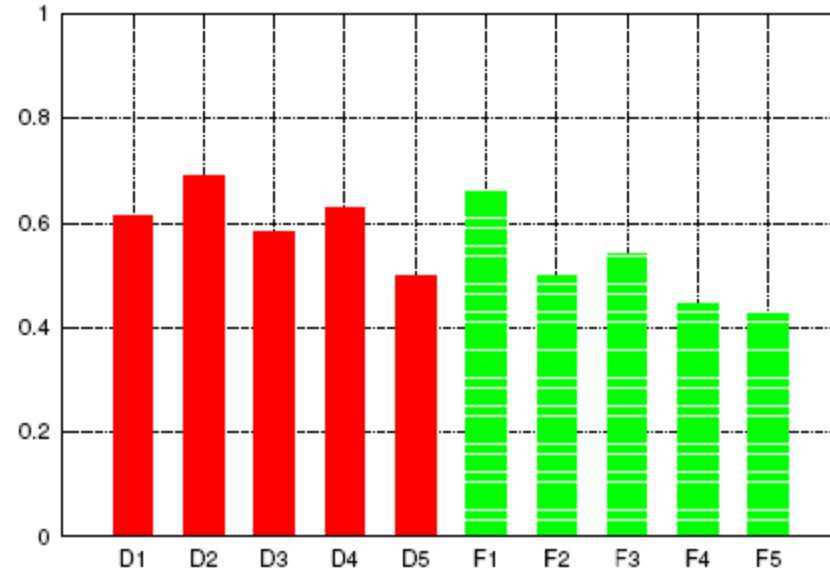
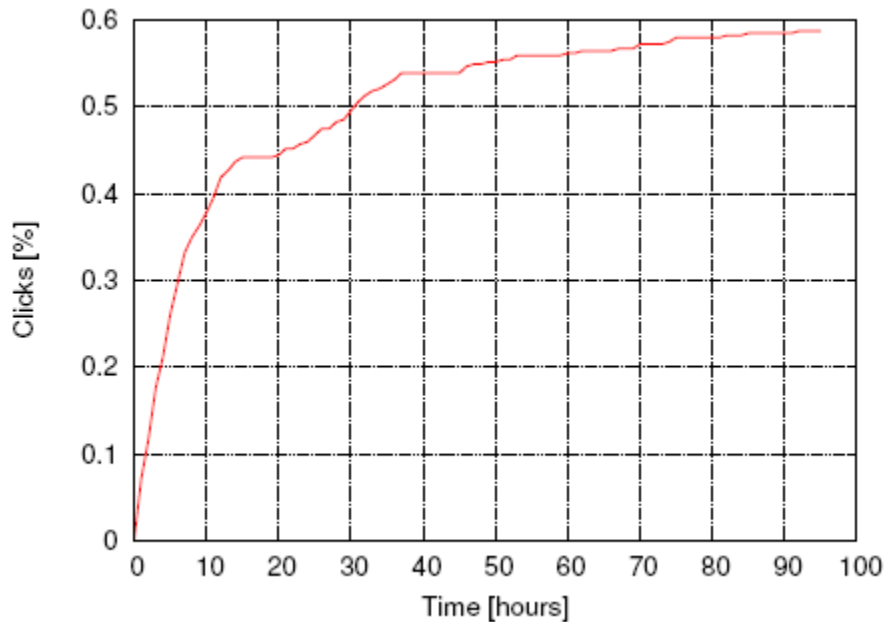
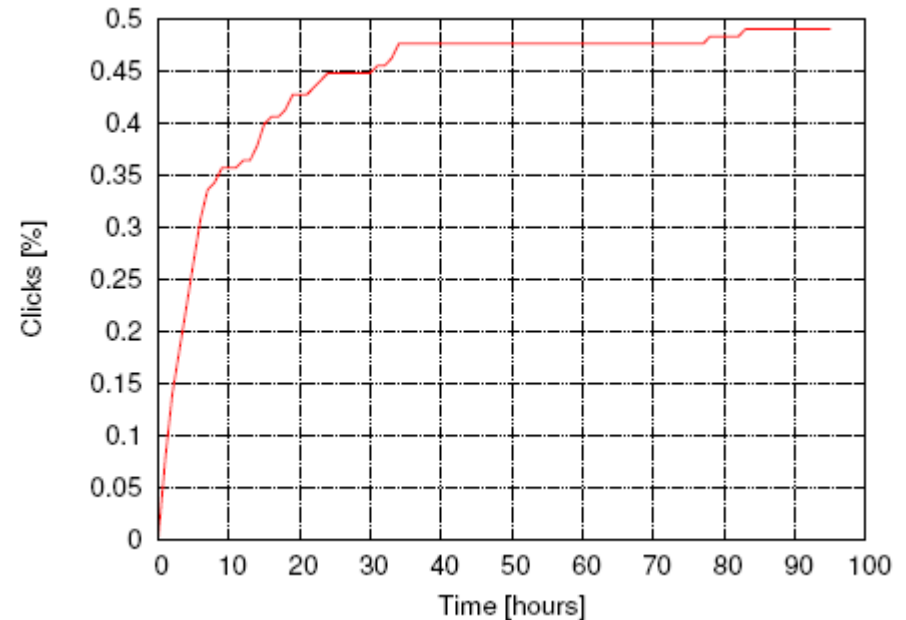


Figure 4: Click through rate for messages sent by forged profiles (D1,..,D5), and fictitious profiles (F1,..,F5)

# Click delays of the receivers



CDF of clicks over time for forged accounts



CDF of clicks over time for fictitious accounts

about 45% of the users clicked the link in the first 20 hours

# Cross-site Profile Cloning Experiments

- success of this attack depends on the number of users and their contacts that **have a profile in both** the source and the target social network
- They crawled 30.000 XING profiles and found 3.700 (12%) of them also in LinkedIn
- XING has 6 million registered users → upper bound to number of contacts an attacker can have: 700.000
- They clone 5 XING accounts to LinkedIn and iCloner identified 78 out of 443 (17,6%) contacts also registered in LinkedIn
- Then iCloner sent contact requests to these accounts

# Cross-site Profile Cloning Evaluation

Profiles	LP	SR
X1	18.2%	50.0%
X2	14.5%	66.6%
X3	22.8%	51.6%
X4	14.5%	100.0%
X5	15.6%	46.4%
Total	17.6%	56.4%

Table 1: Percentage of XING profiles found in LinkedIn (LP) and the success rate (SR) of the contact requests

56 % (in total 44) of the contact requests were accepted

# Suggestion for improvements in Social Network site security

- Provide more information to the receiver on the authenticity of a contact request
  - Where was issued (country information based on IP)
  - Profile creation date
- Make CAPTCHA more difficult to break
  - The attackers main objective is to separate each symbol and to detect it using OCR
  - Rendering the image so as some symbols overlapping each other
  - Render additional paths of randomly connected lines spanning over many symbols

# Suggestion for improvements in Social Network site security

- **Rate limit** the number of CAPTCHAs that are displayed to a user with a threshold value of a few images/minute
- Adopt (or improve) behavior-based anomaly detection techniques to **detect and block** crawling and other suspicious activities

# Conclusion

- Social networking sites have been increasingly popular
- Unfortunately, when a new technology starts to attract a large number of users, criminals are attracted as well
- They present and evaluate 2 identity theft attacks
- Their results show that not all SN sites are well-protected against automated crawling and access
- Moreover, most users in SN sites are not cautious when accepting friend requests or clicking on links that are sent to them

Question ?