



**DIMVA 2011**

# Reverse Social Engineering Attacks in Online Social Networks

Danesh Irani, **Marco Balduzzi**  
Davide Balzarotti, Engin Kirda, Calton Pu



# Motivations

---

- ▶ Social Networks have experienced a huge surge in popularity
  - ▶ Facebook has more than 500 Million users:  
<http://www.facebook.com/press/info.php?statistics>
- ▶ The amount of personal information they store requires appropriate security precautions
- ▶ People are not aware of all the possible way in which these info can be abused
- ▶ A simple problem can result in serious consequences for thousands of Social Networks users

# Social Engineering

---



*Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques*

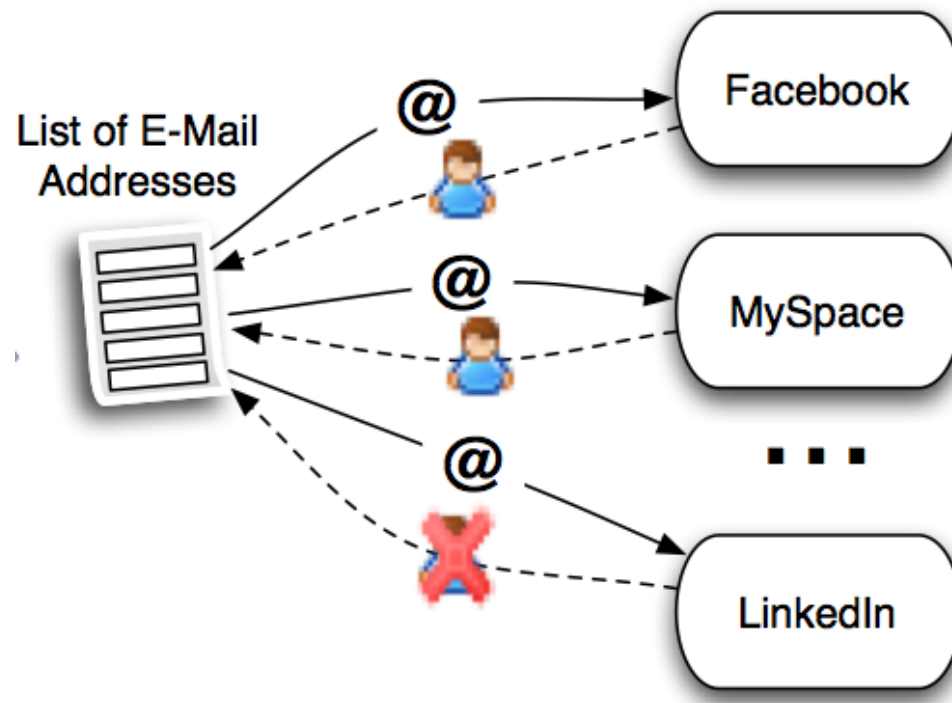
# Reverse Social Engineering Attacks in Social Networks

---

- ▶ Classic Social Engineering: The attacker contacts his victim
- ▶ RSE: The attacker...
  - ▶ 1. feeds his victim with a pretext (baiting)
  - ▶ 2. waits for victim to make the initial approach
- ▶ Victim less suspicious as she makes the initial contact
- ▶ Bypasses current behavioral and filter-based detection
- ▶ Potential to reach millions of users on social networks

# Facebook Initial Experiment

- ▶ Last year (RAID 2010): “Abusing Social Networks for Automated User Profiling”




# Facebook Initial Experiment


- ▶ The account used in that research received a large number of friend requests
- ▶ Hit the limit : 25,000





# Facebook Initial Experiment Results


RECENT ACTIVITY


 Alison is now using Facebook in English (US).


 Alison and Amitabh Lakhota are now friends. · Comment · Like


 Alison and Anthony Jaeger are now friends. · Comment · Like


 Alison and Kenney Rosicka are now friends. · Comment · Like


 Alison and Stig Johannessen are now friends. · Comment · Like


 Alison and Lennox Humphrey are now friends. · Comment · Like


 Alison and Mark Chin are now friends. · Comment · Like


 Alison and Ryan Bathauer are now friends. · Comment · Like


 Alison and David Moore are now friends. · Comment · Like


 Alison and Kareem Trevizo are now friends. · Comment · Like


 Alison and Ruth's Chris Lake Mary are now friends. · Comment · Like


 Alison and Tom Rawlings are now friends. · Comment · Like


 Alison and Chrystian David Saavedra Cuartas are now friends. · Comment · Like


 Alison and Aston Thompson are now friends. · Comment · Like


 Alison and D.i. Omar are now friends. · Comment · Like


 Alison and Patrick Gaunce are now friends. · Comment · Like


 Alison and Edwin Chan are now friends. · Comment · Like


 Alison and Michael Holmes are now friends. · Comment · Like


 Alison and Chippy Maunga are now friends. · Comment · Like


 Alison and Baris Kadioglu are now friends. · Comment · Like


 Alison and Andrea Burnett are now friends. · Comment · Like


 Alison and Timothy Billings are now friends. · Comment · Like


 Alison and Armando Mendoza Arias are now friends. · Comment · Like


 Alison and Harold Arnold are now friends. · Comment · Like


 Alison and Ray Golden are now friends. · Comment · Like


 Alison and Michael Brown are now friends. · Comment · Like

 Alison and Eddie J Grant are now friends. · Comment · Like

 Alison and Martin Tino Moreno are now friends. · Comment · Like

 Alison and Leon van der Walt are now friends. · Comment · Like

 Alison and Giorgio Profeti are now friends. · Comment · Like

 Alison and Tim Page are now friends. · Comment · Like

Voulez-vous enfin perdre du poids? Maigrir de 4 kilos par semaine. Les "Astuces" pour

▼ embyte@panda: ~/projects — □ ×

File Modifica Visualizza Terminale Aiuto

adding userID 740268996

adding userID 503801274

adding userID 611605887

adding userID 1396383565

adding userID 1526273025

adding userID 1104221792

adding userID 819593953

adding userID 1611061493

adding userID 1428304705

adding userID 19512192

adding userID 1307418875

adding userID 100000066318035

adding userID 100000055937720

adding userID 1821707518

adding userID 100000059177956

adding userID 1501557741

adding userID 1472203778

adding userID 1101703898

adding userID 543892703

adding userID 1382220005

adding userID 1134840081

adding userID 1459295524

adding userID 1745257731

adding userID 790207499

adding userID 578892825

adding userID 1649894914

adding userID 1535297438

adding userID 669725305

adding userID 1647460077














adding userID 1058588362

adding userID 1523773930

adding userID 100000050357865

adding userID 1559055353

adding userID 508354137

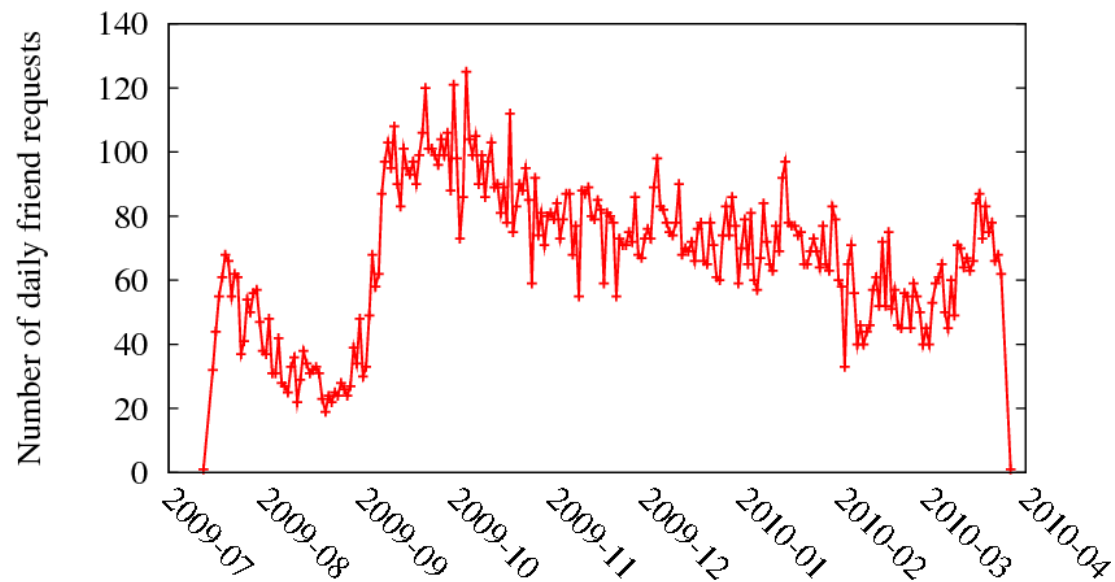
	Sergio Malchiodi Today at 4:00pm	<b>ciao</b> piacere di conoscerti parli italiano o i need write you...
	Naji Mohamed Abdalla Today at 4:00pm	<b>&lt;no subject&gt;</b> hi thk's for accepting my application enjoy ur time regards
	Harry Poulos Today at 3:44pm	<b>&lt;no subject&gt;</b> so, facebook keeps suggesting that we should be friends...
	Duncan D Nulty Today at 3:37am	<b>Facebook - I don't understand it</b> Facebook suggested you as a friend and I'm wondering ...
	Julia Pearlstein Today at 1:31am	<b>facebook weirdness</b> Hi Alison, You don't know me and I don't know you, but y...
	Ro Ward Yesterday at 4:48pm	<b>&lt;no subject&gt;</b> Hey Alison, how are you doing hun. I didn't know what thi...
	Gamaliel Malave Yesterday at 12:16pm	<b>&lt;no subject&gt;</b> Hello Allison. Just wondering if you are my cousing from...
	Ray Goldberg Yesterday at 7:58am	<b>&lt;no subject&gt;</b> Hi. No idea who you are but nice to meet you
	Dale Hunt Yesterday at 1:31am	<b>&lt;no subject&gt;</b> Hi alison, your photo keeps coming up in 'suggested frien...
	Robert Allison Yesterday at 12:51am	<b>hi</b> hi there how are you
	Carlos Gonzalez Gutierrez Mon at 11:28pm	<b>Hi</b> Hi Alison, How are you
	Albert Yin Mon at 6:11am	<b>Suggestions</b> Lol facebook keeps suggesting you as a possible friend. W...
	Dennis Earles Mon at 6:07am	<b>Where are you located?</b>



# Facebook Initial Experiment Results

---

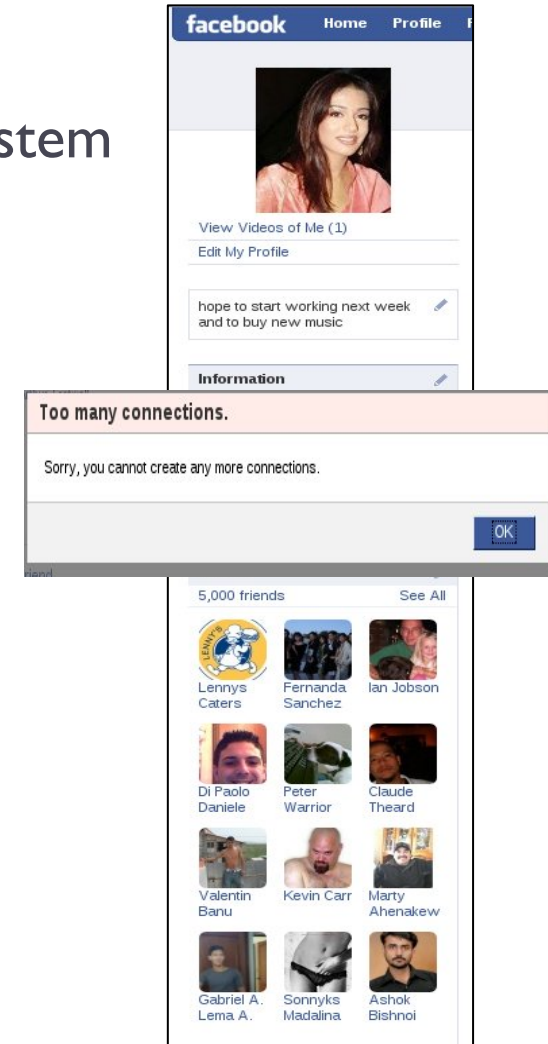
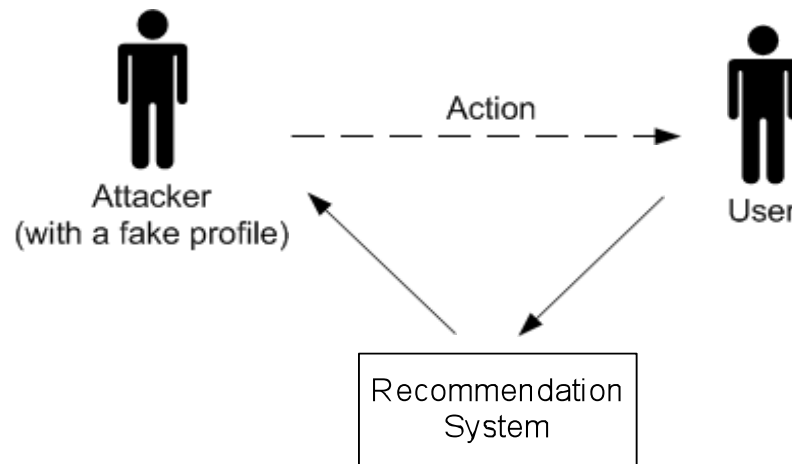
- ▶ About 500,000 email queried
- ▶ 3.3% friend connect rate in 3 months
- ▶ Cascading effect based on reputation
- ▶ 0.37% average friend connect rate per month





# 3 Types of Real-World RSE Attacks

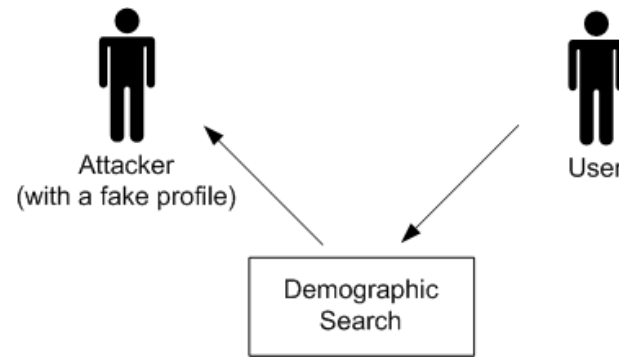
- ▶ Recommendation-Based
  - ▶ Mediated attack where Recommendation System performs baiting



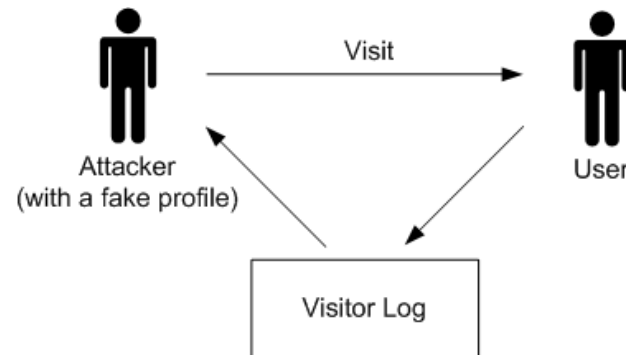
# 3 Types of Real-World RSE Attacks

---

## ► Demographic-Based – Mediated



## ► Visitor Tracking-Based – Direct








# Experiment

- ▶ RSE attack on Facebook, Badoo and Friendster

<i>Type of Attack</i>	Facebook	Badoo	Friendster
<i>Recommendation-Based</i>	✓✕	-	-
<i>Demographic- Based</i>	✓	✓✕	✓
<i>Visitor Tracking-Based</i>	-	✓	✓✕

- ▶ Determine characteristics which make profiles effective

Social Network	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Age	23	23	23	35	23
Sex	Male	Female	Female	Female	Female
Location	New York	New York	Paris	New York	New York
Picture*					

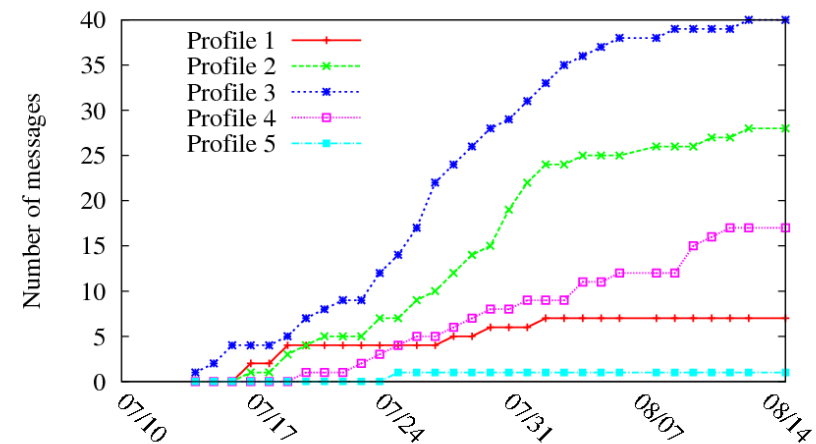
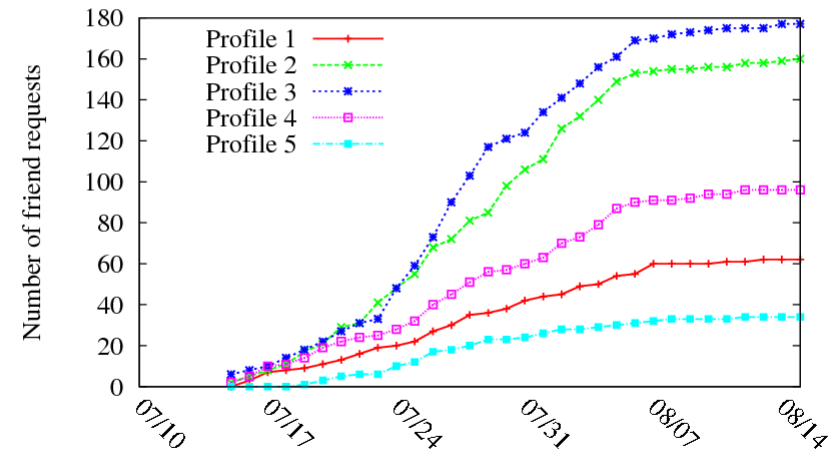
# Ethical and Legal Considerations

---

- ▶ We consulted with the legal department of our institution (comparable to the Institute Review Board (IRB) in the US) and our handling and privacy precautions were deemed appropriate and consistent with the European legal position.
- ▶ When the data was analyzed, identifiers (e.g., names) were anonymized, and only aggregate analysis of the collected data was performed.

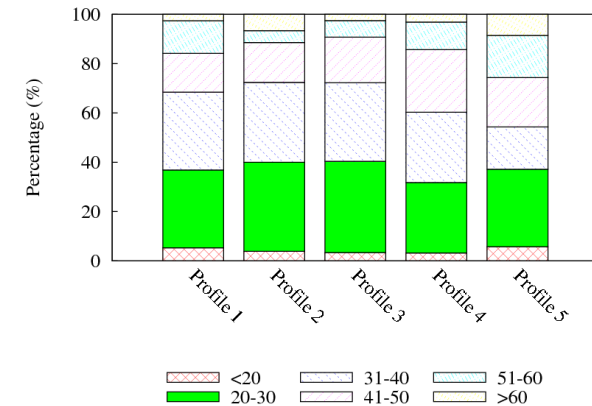
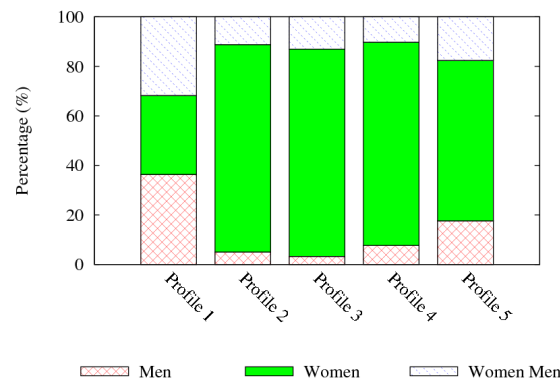
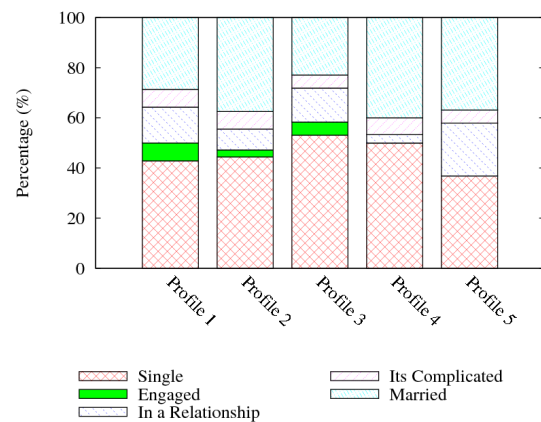
# Recommendation Based (Facebook)

- ▶ 50,000 profiles queried per attack profile
  - ▶ Profiles 2 and 3 (girls) most successful
  - ▶ Profile 5 least effective
- ▶ 94% of messages sent after friend requests
- ▶ Most common 3-grams: “suggested you as” or “suggest I add”
- ▶ The baiting works



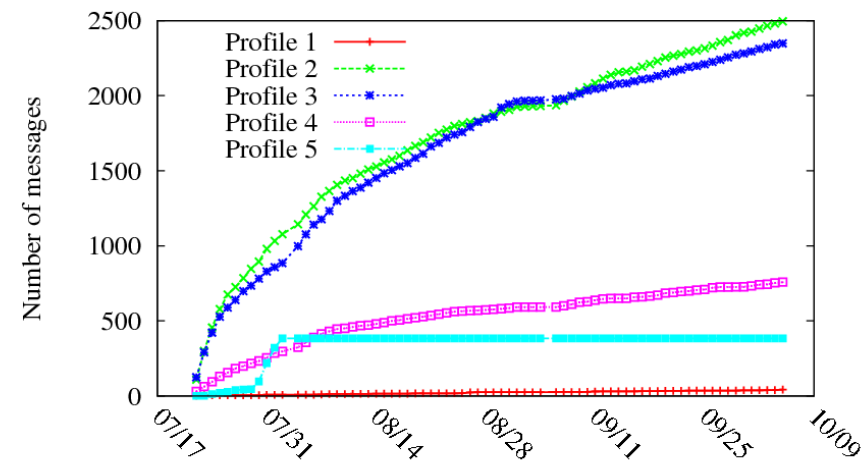
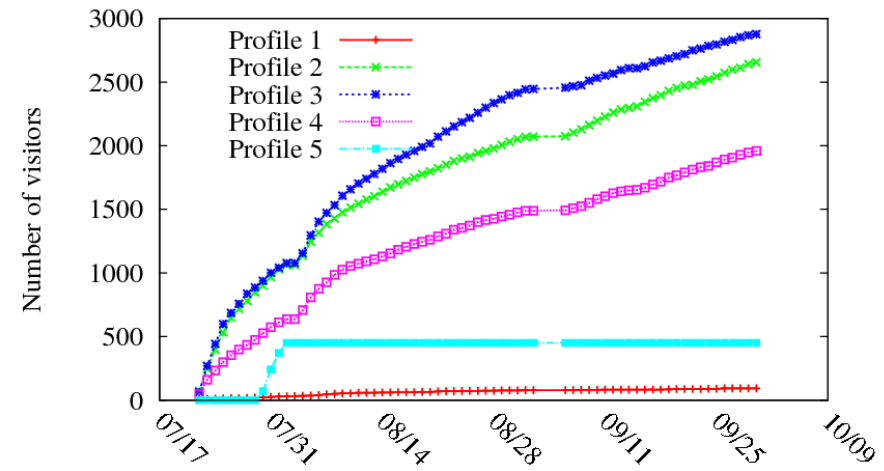
# Recommendation Based (Facebook)

- ▶ Majority of victims attracted: Single Young users who expressed interest in “Women”
- ▶ Profile 1 received a large number of requests from users expressing interest in “Men”
- ▶ Profile 5 attracted largest number of requests from older users



# Demographic Based (Badoo)

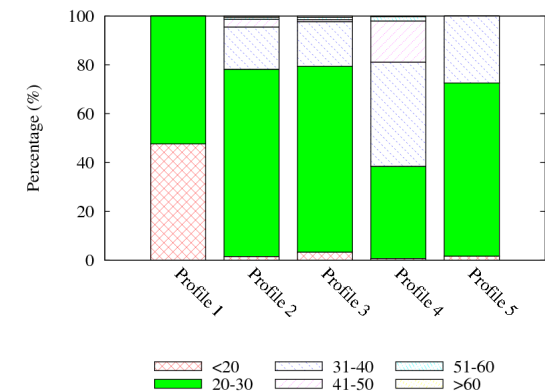
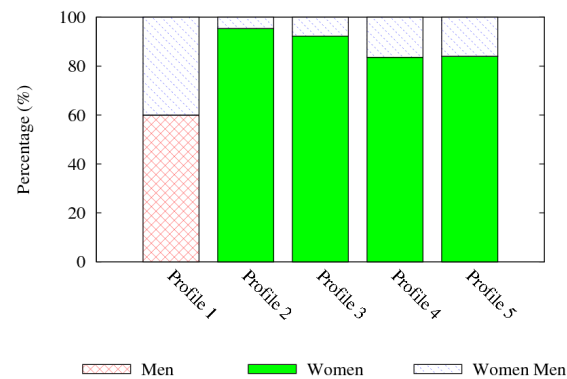
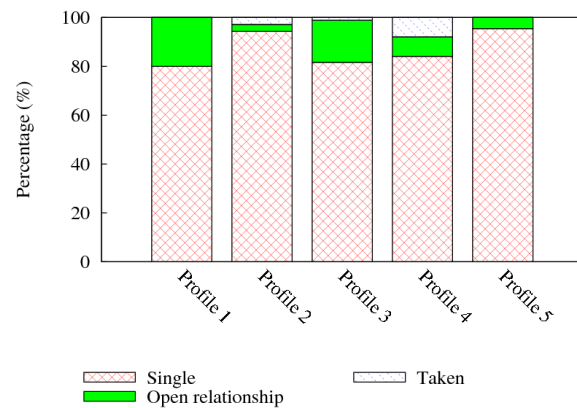
- ▶ Created the fake profiles and occasionally updated to remain in search
  - ▶ Profile 5 was removed
  - ▶ Profiles 2 and 3 most successful again
  - ▶ Profile 5 not using actual photo was disabled
- ▶ 50% of visitors messaged Profile 2 and 3 (44% avg.)
- ▶ Most common 3-grams: “how are you”, “get to know”, and “would you like”
- ▶ Face-to-face relation





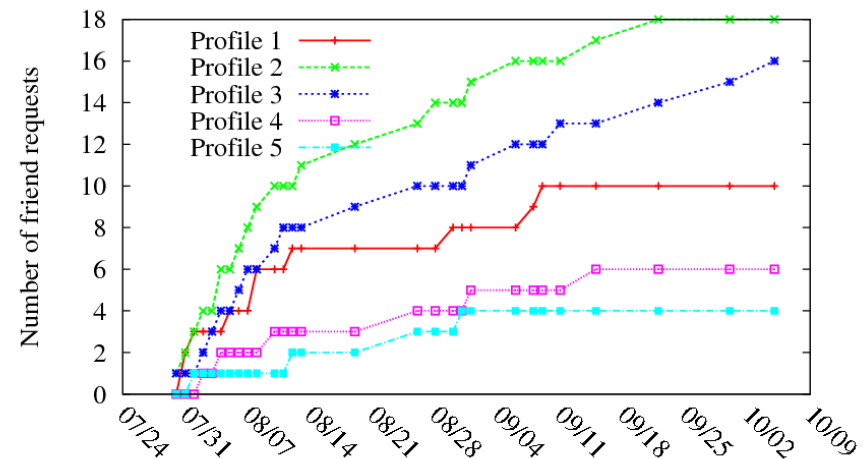
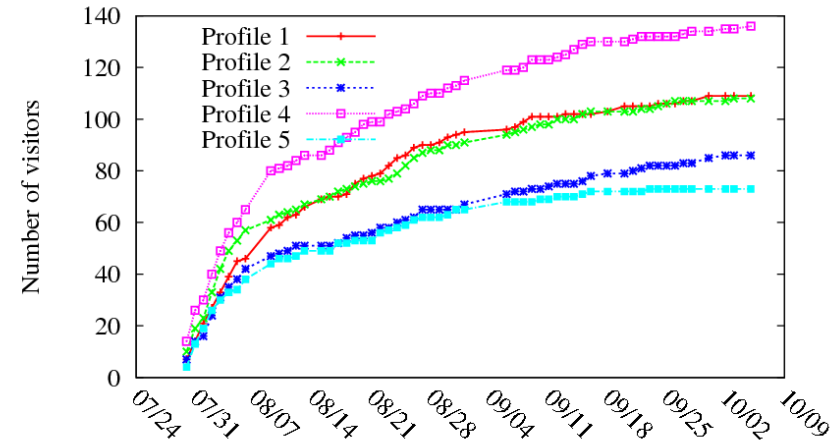
# Demographic Based (Badoo)

- ▶ Most users who expressed interest were “Single”.
- ▶ Attracted users interested in their gender and approximate age group.
  - ▶ Profile 1 received large interest from younger profiles. Profile 4 from older profiles.



## Visitor Based (Friendster)

- ▶ 42,000 users visited per attack profile
  - ▶ Number of users visited attack profiles back, consistent with Facebook
  - ▶ 0.25% to 1.2% per month
- ▶ Number of following friend requests or messages low in comparison
- ▶ Demographics similar to Facebook



# Lessons Learned

---

- ▶ **Pretexting** – critical for RSE attacks
  - ▶ Excuse needed to “break the ice”
  - ▶ Recommendation systems (e.g. Facebook) provide strongest pretext
  - ▶ The Visitor Based attack was not effective (e.g. Friendster)
- ▶ **Profile effectiveness**
  - ▶ Attractive female profiles are highly successful
  - ▶ Can be tuned to demographics of target victim(s) (e.g. Badoo)

# Countermeasures

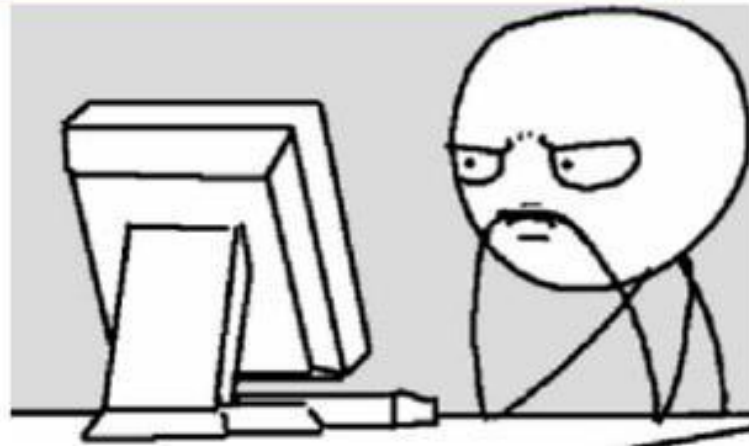
---

- ▶ Perform recommendations based on very strong links
  - ▶ Ensure at least a few friends in common (or within n-degrees of separation)
- ▶ Adapt behavioural techniques to RSE techniques
  - ▶ Check accounts only performing a single action
  - ▶ Ensure bi-directional activity (i.e. profile also searches and adds users)
- ▶ CAPTCHAs for incoming friend requests

# Questions



Everything is going  
According to plan.



failbook.com