Special Topics in Security
ECE 5968

Engin Kirda
ek@ccs.neu.edu

Northeastern University

Duqu

Duqu

From Wikipedia,

For the vers

Duqu is a colle tuxnet worm. The Laboratory of C y and Economics in Hungary discov qu.[3] Duqu got its name from the

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Dear Engin,

Recently we came across a new malware found in the wild that has strong similarities to Stuxnet, inlcuding modular architecture, injection and spreading mechanisms, matching code segments, used keys and constants and code signed with a fraudulent digital signature of a Taiwanese driver manufacturer. The certificate is still valid and the command and control server of the malware is still running, so we may be the first who caught malware.
We did some initial analysis, and wrote a report that we now first share with a limited number of experts.
We attach the report here, or it can be downloaded from our site as
http://www.crysys.hu/publications/files/duqurep.zip
password: etlduqu11

This is the list of parties that we
notified and that received our report today (October 14):

Targeted, Financially-Motivated Attacks

You've Probably Read This: Recent Payment Breaches

- The last years have seen a dramatic escalation in the number of breached Point of Sale (PoS) systems
- Many of these PoS payloads, like Backoff, evaded installed defenses and alarms
- In few cases an early alarm was received, but it was ignored since indistinguishable from the background noise

Targeted, Financially-Motivated Attacks

What is Backoff?

- Malware used in numerous breaches in the last year
- Secret Service estimated 1,000+ U.S. businesses affected
- Targeted to Point of Sale (PoS) systems
- Evades analysis

How are the attackers deploying it?

- Scan for Internet facing Remote Desktop applications
- Brute force login credentials
- Often successfully find administrative credentials
- Use admin credentials to deploy Backoff to remote PoS systems

Carbanak Malware

- Bank robbing, raked in as much as 1 billion $
  - Banks infiltrated, ATMs were taken over
  - Balances adjusted and funds transferred remotely
- Most Carbanak samples exhibit stealthy behavior (90%)
  - 17% display evasive behavior (detecting sandbox)
  - Samples are environmentally-aware
  - Stealthy sandbox is needed that can detect evasions

In Recent Research…

- We looked at a Non-Governmental Organization (NGO)
  - Representing the Uyghur minority in China
  - Many suspicious emails were being sent
  - Many targeted hacking attempts
- Key finding
  - The attacks were surprisingly simple
  - Malware not very sophisticated
  - No unknown vulnerabilities used

GUI Security

Graphical User Interfaces (GUIs)

- De facto standard to interact with most computing devices
  - Desktops, smart phone, computer-based appliances, ...

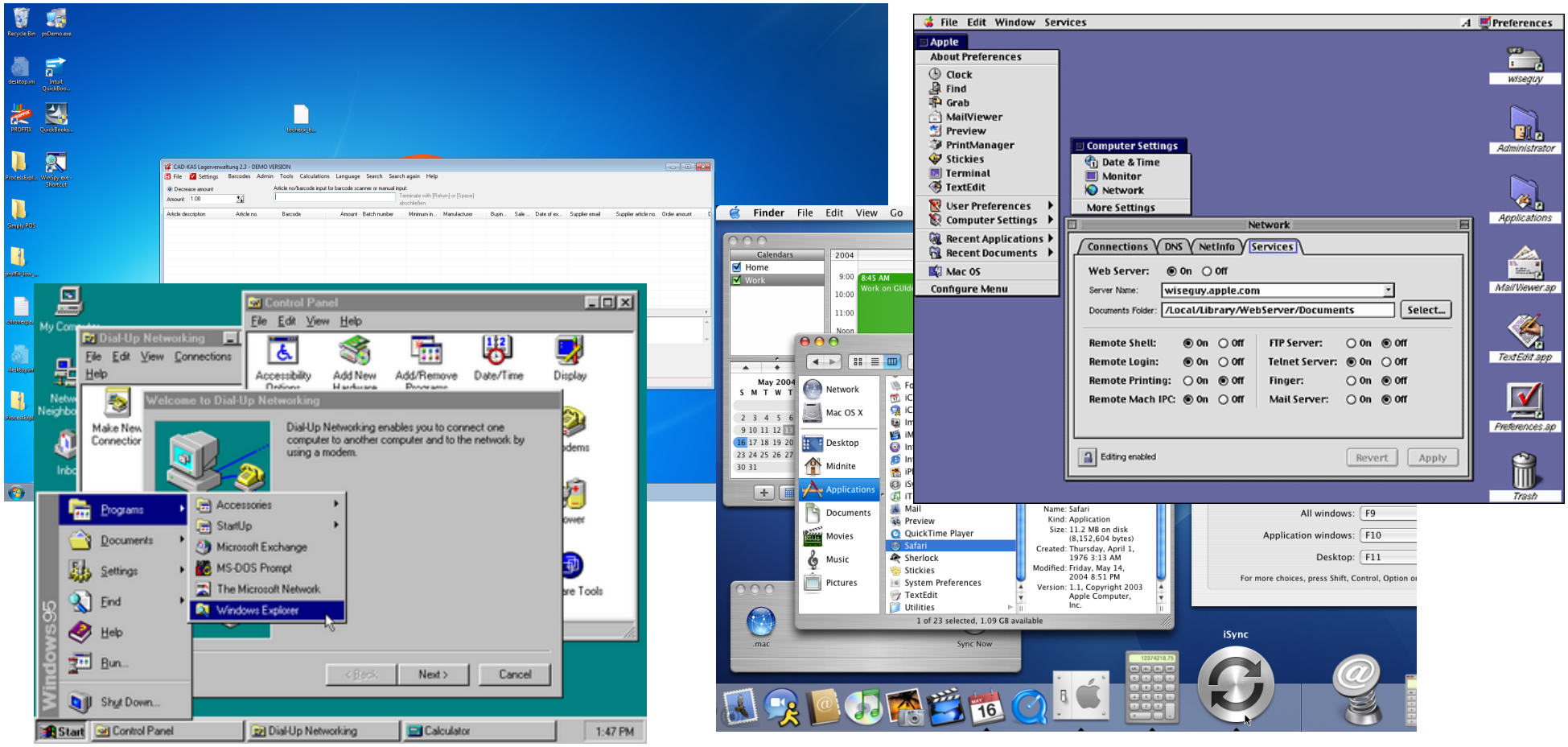
GUI Security History (Shatter Attacks)

- Shatter Attacks
  - C. Paget (2002), B. Moore (2003)
- Affected platform: Windows NT/2000/XP
- R
- Target: process with admin privileges
  - Code execution → privilege escalation
- Now Windows has User Interface Privilege Isolation (UIPI)
  - Cannot manipulate UI of process that has higher privileges

This issue is about access control problems in the UI

Graphical User Interfaces (GUIs)

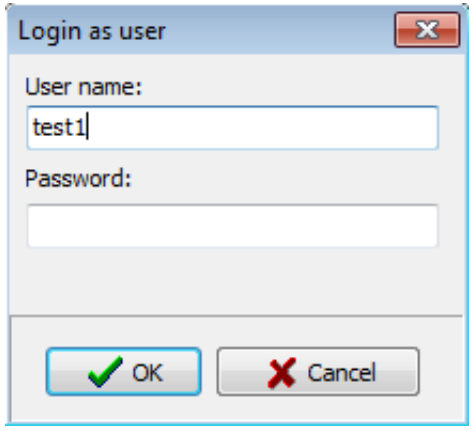
- Windows, Widgets, ...

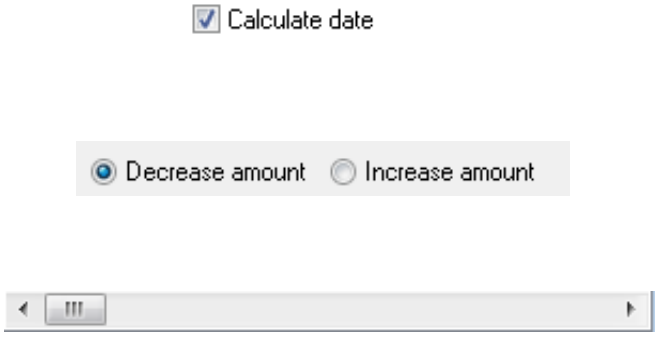


GUIs → Widgets and Windows

- Widget → base UI element
  - Smallest element in a UI framework
  - On MS Windows: widget = window

- Common widgets
  - Window
  - Frame
  - Button
  - Check-box
  - Text edit field
  - Drop down box
  - Slider





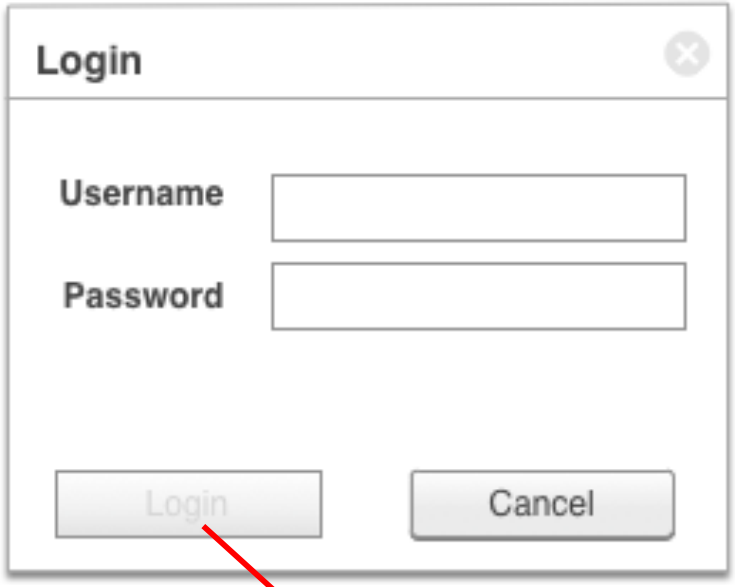
Widget Attributes

- Attributes allow to change widget behavior at runtime
  - Allows user interface to be dynamic
- Common attributes
  - Enabled → enable / disable widget
  - Visibility → show / hide widget
  - Read/Write → allow / disallow changing data stored in widget

```
myButton.enable(false);
```

Widget Attributes

- Attributes allow to change widget behavior at runtime
  - Allows u
- Common attr
  - Enabled
  - Visibility



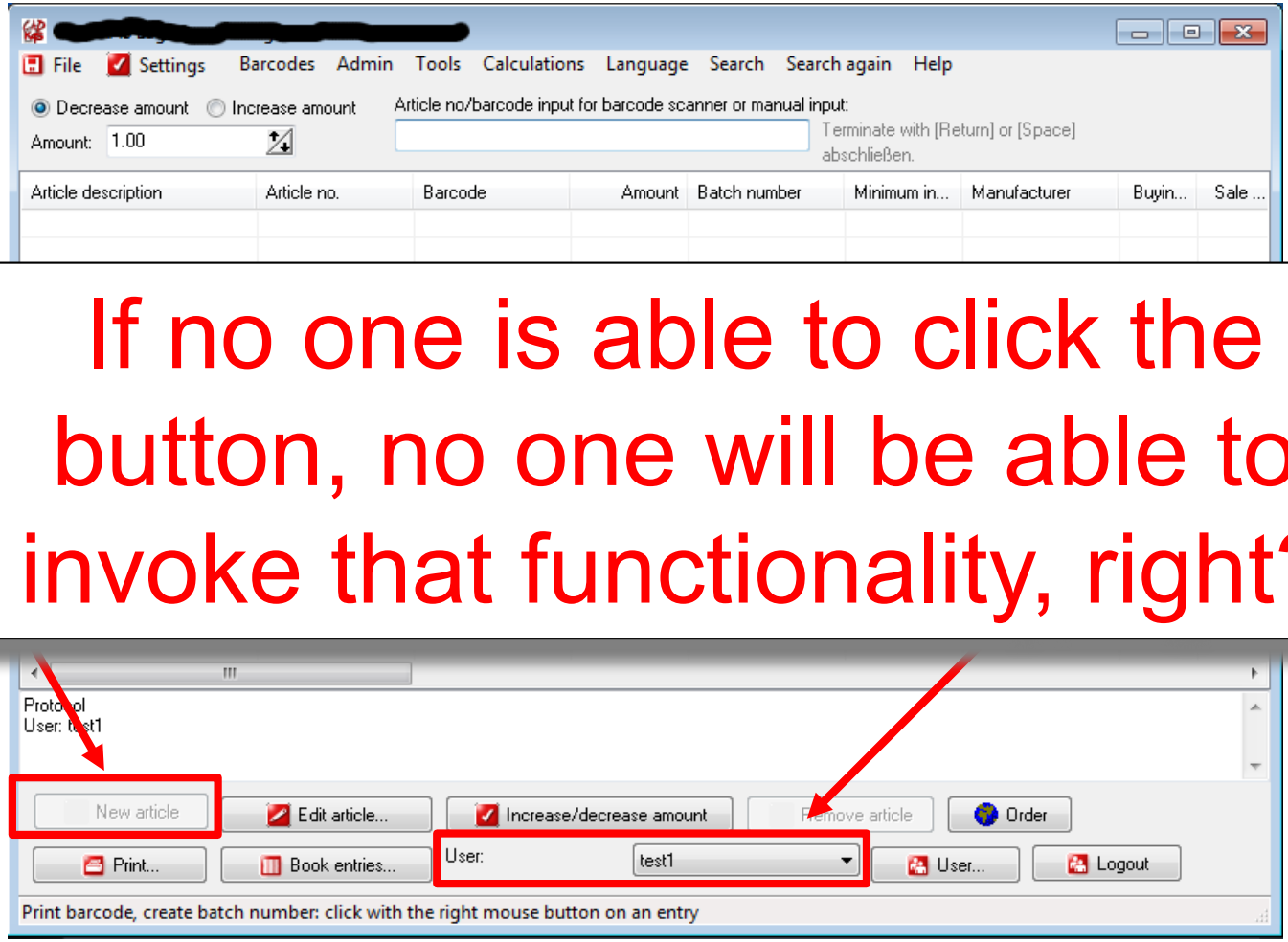
Login button disabled → indicates username required

Access Control

- Basic security requirement
- Common in any kind of enterprise application
- E
- D
  - Create / Add data
  - View data
  - Modify data
  - Execute privileged functionality

Implementing access control using GUI elements is tempting

Access Control in the GUI



Disal

If no one is able to click the button, no one will be able to invoke that functionality, right?

User

The Answer is: No.

In fact, it's a bad idea and can lead to problems

Access Control in the GUI

- Widgets *can* be manipulated (e.g., using a tool such as WinSpy++)
  - Feature of UI frameworks (i.e., object orientation)
  - There is no need to modify application binary
- Manipulate widget → bypass GUI-based access control
- Interestingly, to date, this is a problem that no one has discussed in literature

Demo: WinSpy++ on Windows

Social Networks

Social Networks

- Social networks
  - massive growth and rise in popularity
  - people provide significant amount of private/sensitive information
  - security and privacy threats not well-understood
  - often, protection offered by social network providers lacking

Social Network Security Issues

- Data privacy
  - blackmail
  - identity theft
  - personalized spear-phishing
  - targeted advertisement
- New venue to reach large number of potential victims
  - spam
  - malware / worms
  - links that point to sites with browser exploits (drive-by downloads)

Social Network Security Issues

- Rogue applications
  - developed and under control of third parties
  - access to profile information and those of friends
- Support for regular crime
  - absence notes for burglary opportunities
  - monitor victim's spending habits
- Crawlers
  - obtain large amount of data against will of social networks

Social Network Security Issues

- Data privacy
  - blackmail
  - identity theft
  - personalized spear-phishing
  - targeted advertisement

- New venue to reach large number of potential victims
  - spam
  - malware / worms
  - links that point to sites with browser exploits (drive-by downloads)

Data Privacy

- W
  -

Breaking news

Search

Firing dispatcher for Facebook drug joke was right, Wisconsin council claims

NewsCore | May 25, 2010 12:11am

A CITY council in Wisconsin defended its decision to fire a Police and Fire Department dispatcher who joked about drug addiction on her Facebook page.

Dana Kuchler, a 21-year veteran of the West Allis' Dispatch Department, joked that she was addicted to "Vicodin, Adderall, quality marijuana, MD 20/20 Grape and (absinthe)" on the social networking site.

She was fired from her job for the remarks and appealed to an arbitrator, claiming the Facebook post was a joke. She pointed out she had written "ha" in it and urine and hair samples tested negative for drugs.

The arbitrator said she should be entitled to go back to work after a 30-day suspension, but the City of West Allis complained that was not appropriate.

"Making stupid jokes on Facebook where the line between public and private communications is admittedly blurred, calls into question that good judgment and common sense of the grievant and her resulting ability to perform her job," the City argued.

Related Coverage

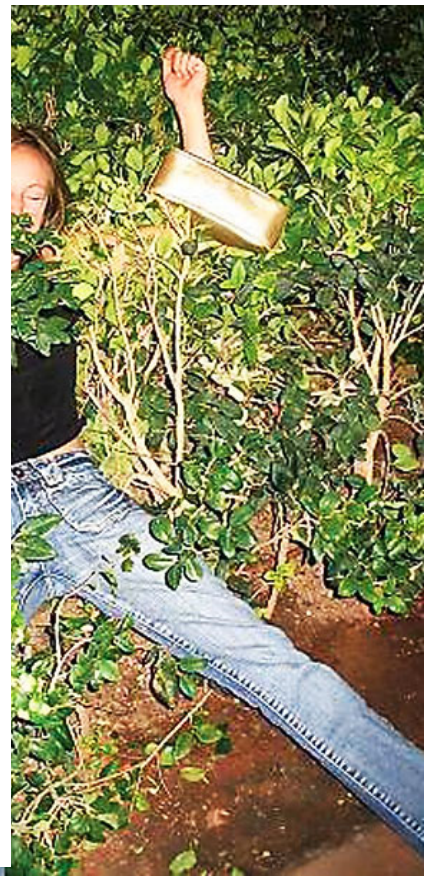
Facebook issues warning after killing
Daily Telegraph, 7 days ago

Murder prompts Facebook revolt
Courier Mail, 8 days ago

Teacher wrote 'loser' on child's

It added that Kuchler's post "mocks and is blatantly inconsistent with the mission of the Police Department that employs her."

[redacted]ler, the West Allis Police Chief wrote that Kuchler's Facebook posting "destroyed the city's trust and confidence in (her) ability and integrity" as a dispatcher and was "an embarrassment to the city."



Data Privacy

- Wealth of sensitive and private information
  - not everything on Facebook is cool
  - so, how do social networks protect this data?

Facebook's Gone

By Ryan Singel ✉ May 7, 2010 | 6:5

Facebook has gone rogue, dru
Zuckerberg's dreams of world
rest of the web ecosystem reco
replace it with something open

Facebook used to be a place t
thoughts with friends and family
stupid games that let you prete
don or a homesteader. It becar
connect with your friends, long-
members. Even if you didn't rea
them.

Facebook announces 'simplified' privacy settings

Press conference follows tumultuous month for social network

By Helen A.S. Popkin
msnbc.com
updated 5:31 p.m. PT, Wed., May 26, 2010

The Facebook public image offensive continued today with a press conference at the social network's Palo Alto headquarters announcing its new "simplified" privacy settings.

The event is a marked departure from Facebook's general method of announcing changes via relatively subtle blog posts and notices on the site. The news conference, announced yesterday, came as a surprise to industry analysts who expected privacy setting changes to come in the next few weeks, not days.

Video

Launch

Zuckerberg on Facebook's privacy changes
Facebook CEO Mark Zuckerberg speaks with CNBC's Julia Boorstin.

Data Privacy

- Wealth of sensitive and private information
  - not everything on Facebook is cool
  - so, how do social networks protect this data
- Wait! You need to
- True, but …
  - open profiles
  - fake profiles
  - profile cloning
  - link addicts

TopLinked.com Home Page
TopLinked.com Account

TopLinked.com Top 50 List
TopLinked.com Top Supporters
TopLinked.com Invite Me List

Add Yourself to the Invite Me List
Add Yourself to the Top Supporter List

About TopLinked.com
Happy Members
Contact TopLinked.com

TopLinked is a Trademark of TopLinked.com.
Copyright 2006-2010. All Rights Reserved.

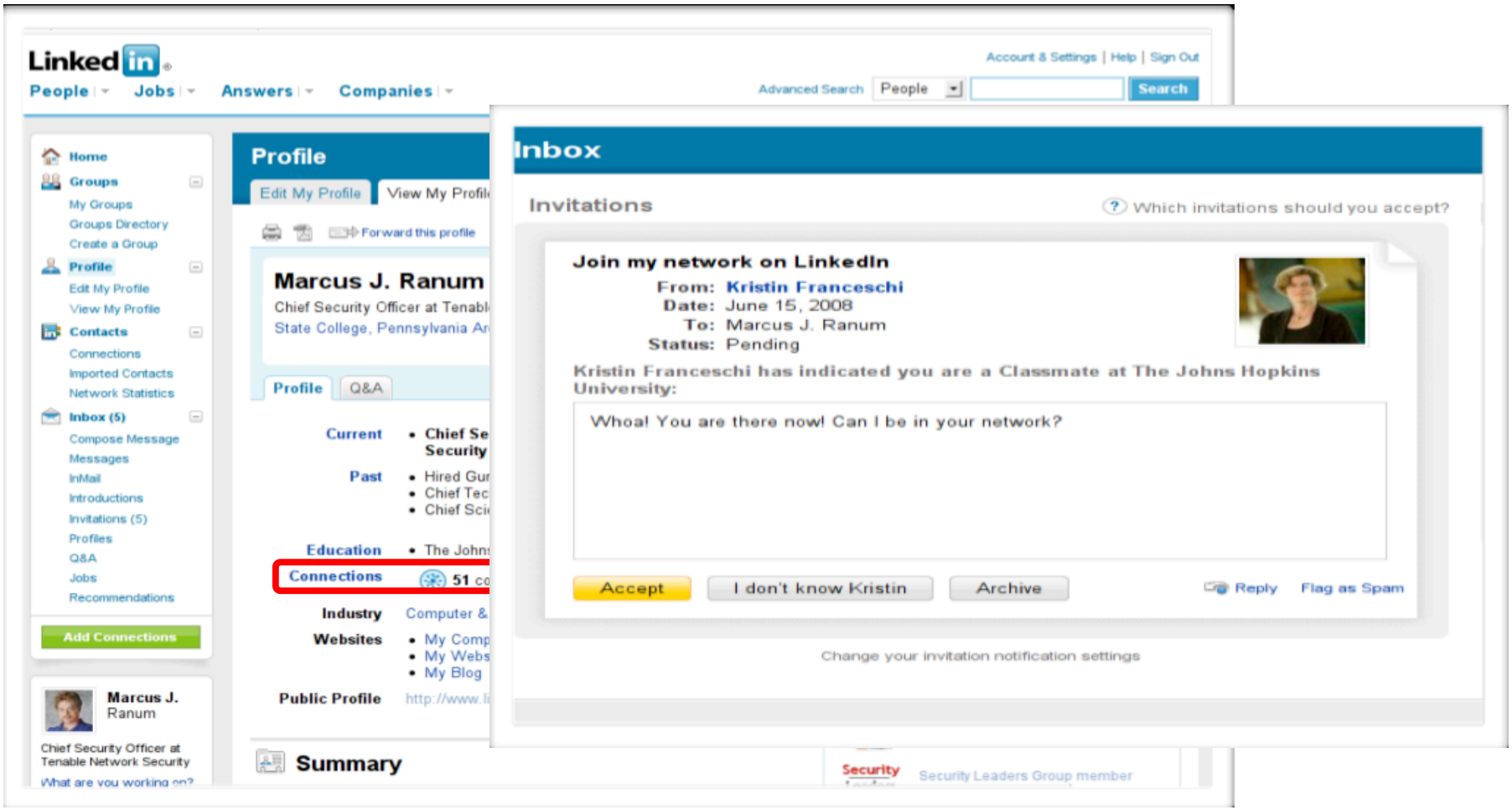
The TopLinked 50

The Top 50 most connected people on LinkedIn!

Note: Not all of the people listed below are active TopLinked Members - so please make sure they have TopLinked.com listed on their profile before extending a connection invitation to them.

Rank	Name (linked to profile)	Connections
1	Ron Bates	44,000+
2	Kenneth Warner Weinberg	41,000+
3	Andrew 'Flip' Filipowski	41,000+
4	Steven Burda	38,000+
5	Richard Atkind	32,000+
6	Wei Guan	32,000+
7	Marc Freedman	30,000+
8	William (Bill) Howell	30,000+
9	Stacy Donovan Zapar	30,000+
10	John L. Evans	30,000+
11	Joe Weinsteiger	30,000+
12	Gerald Haman	30,000+
13	Jan Karel Kleijn	30,000+
14	Pier Paolo Mucelli	30,000+
15	Malcolm Ian Geoffrey Lawrence	30,000+
16	Jan Mulder	30,000+
17	Peter R. Luiks	30,000+
18	Ed Nusbaum	29,000+
19	Jayesh Sampat	29,000+
20	Rawley Martos	29,000+
21	Joe Gillespie	29,000+
22	Shally Steckerl	29,000+

Fake Profile (Ranum Experiment)

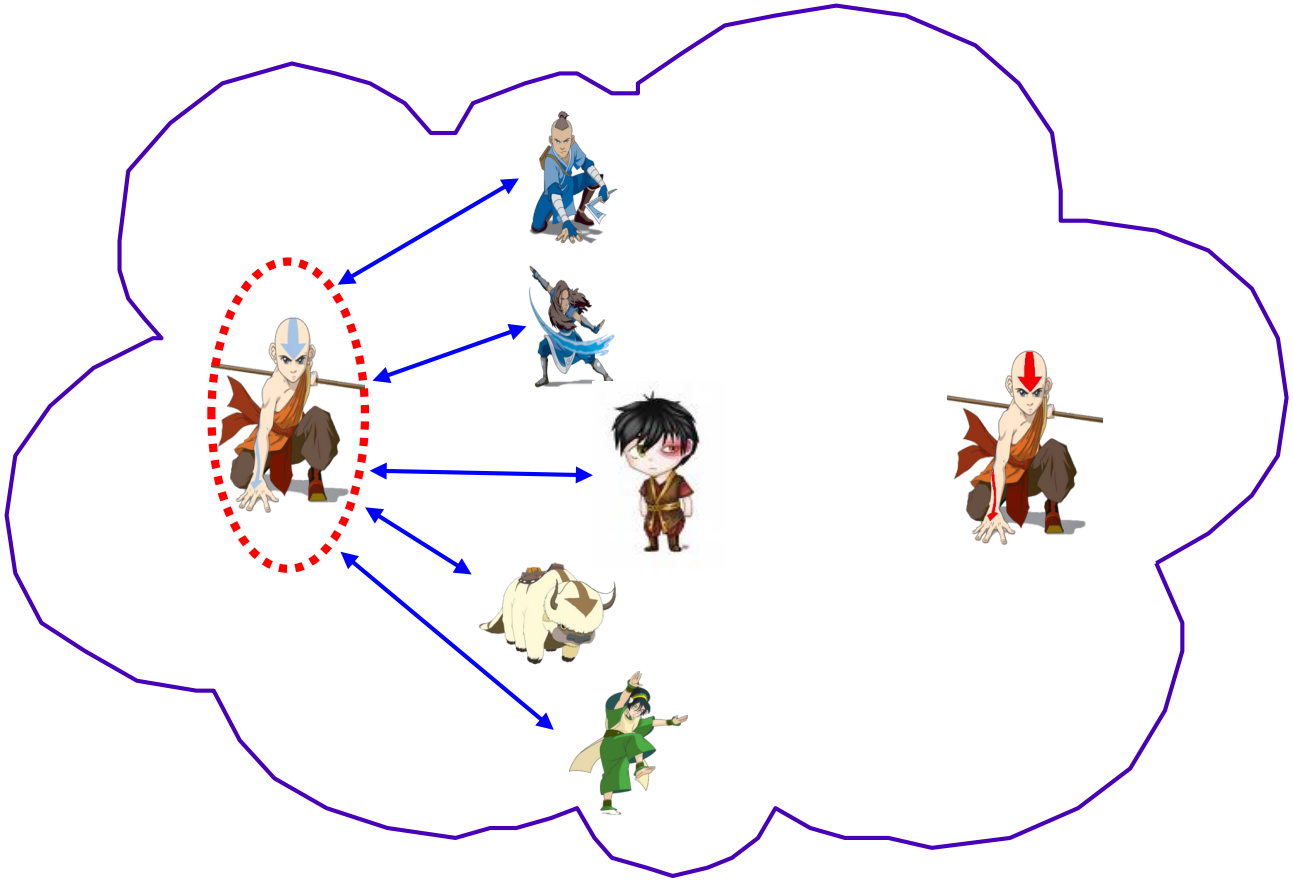


Source: Shawn Moyer and Nathan Hamiel (BlackHat Talk)

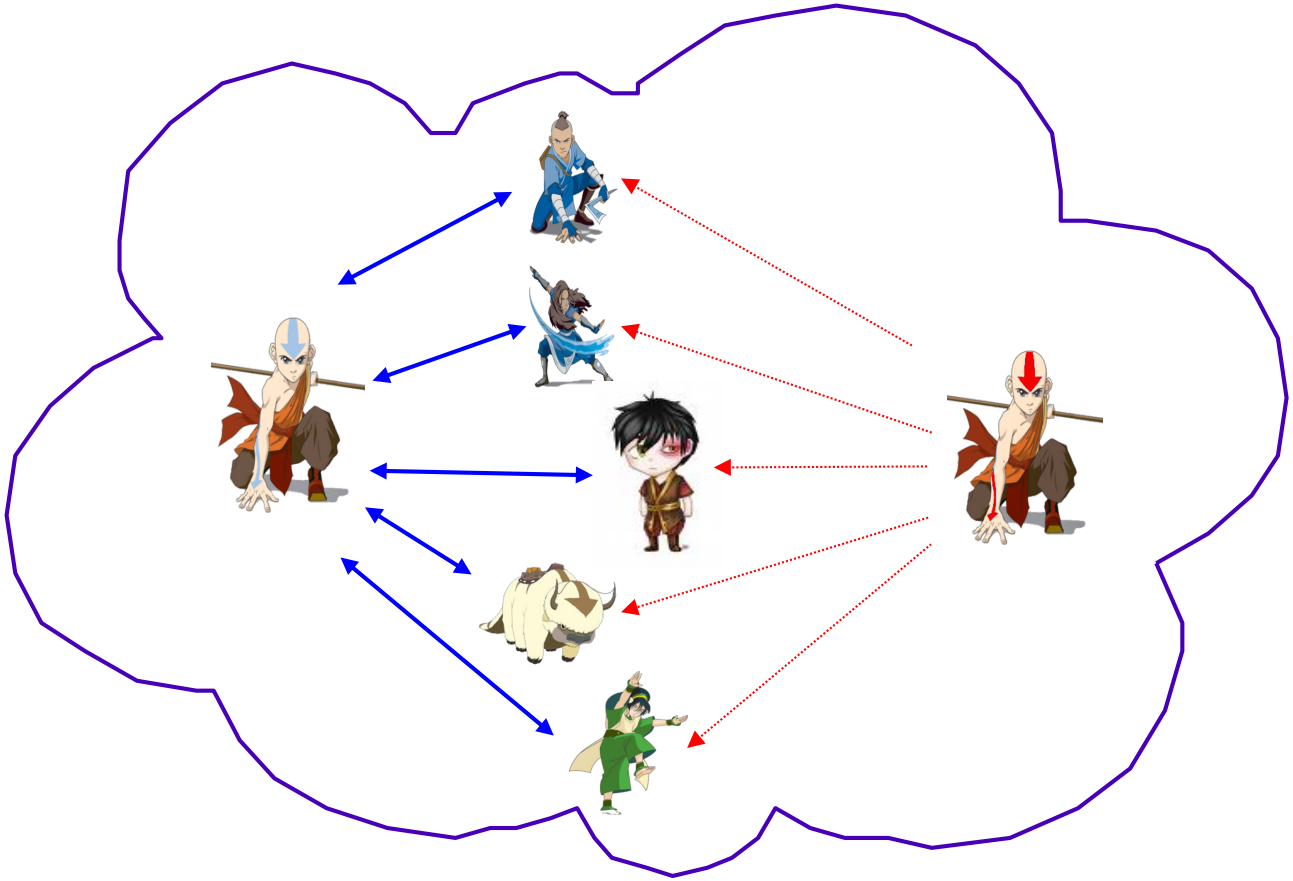
Automated Profile Cloning

- The attack consists of:
  - Identifying a victim
  - Creating a new account with her real name and profile photo
    - This information is typically visible to all registered users
  - Sending friend requests to the users in the victim's contact list

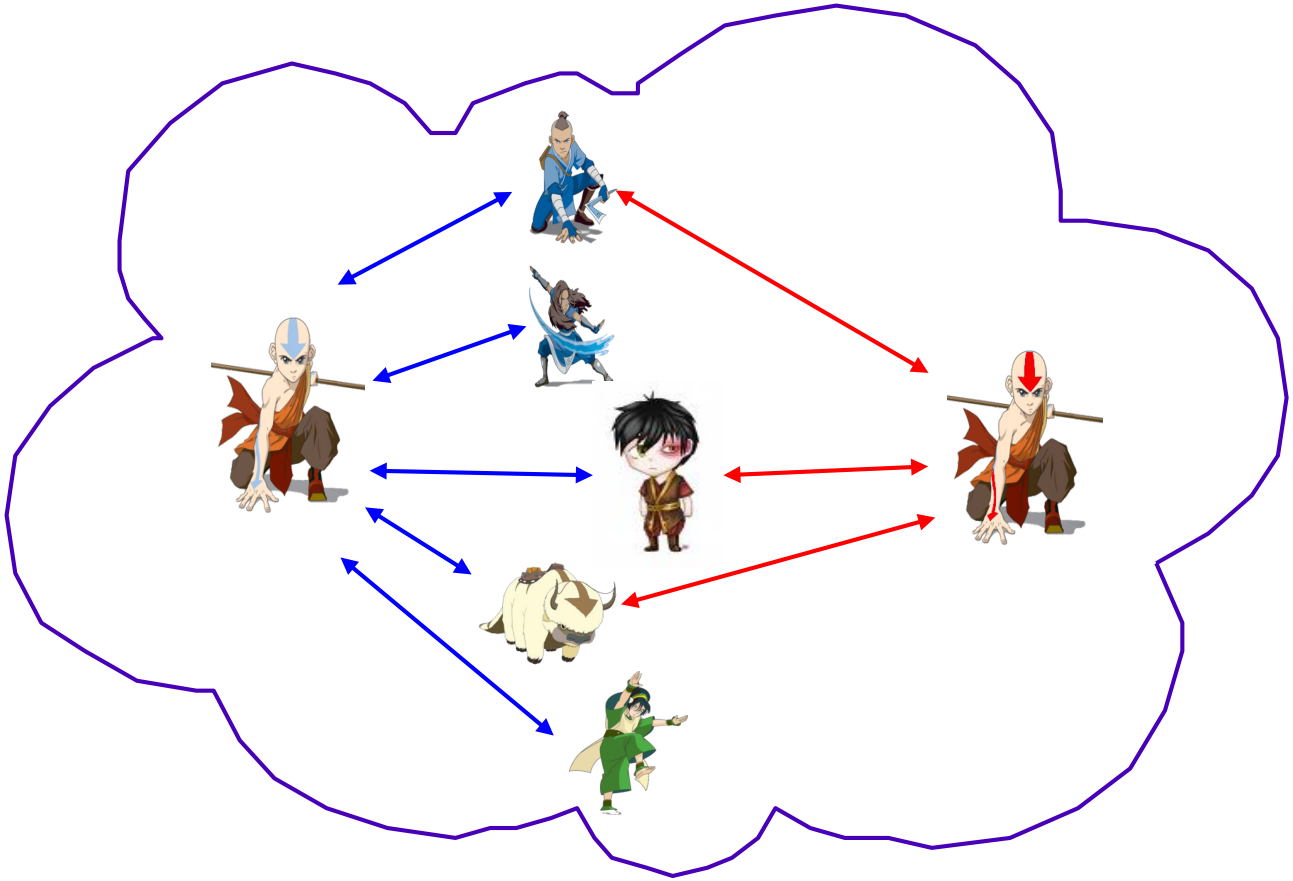
Profile Cloning



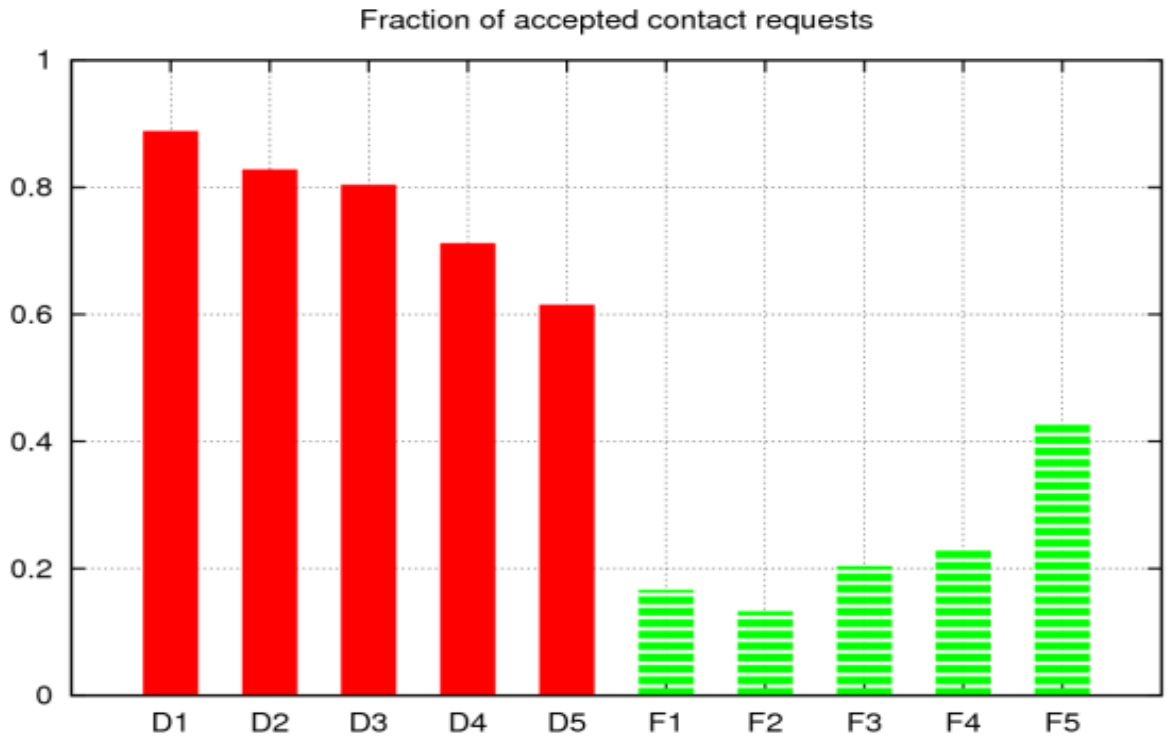
Profile Cloning



Profile Cloning



Profile Cloning



And Apparently, It Was Real…

SCIENCE FAIR 2011

nature news

nature news home | news archive | specials | opinion | features | news blog | nature jo

comments on this story

Stories by subject

- Technology
- Science in culture
- Cell and molecular biology
- Lab life

Published online 23 April 2009 | *Nature* **458**, 1089 (2009) | doi:10.1038/news.2009.398

News

Fake Facebook pages spin web of deceit

Stem-cell scientists are caught up in fictional friend network — but no-one knows why.

Lucas Laursen

In September 2008, *Forbes* science editor Matthew Herper and

Reverse Social Engineering

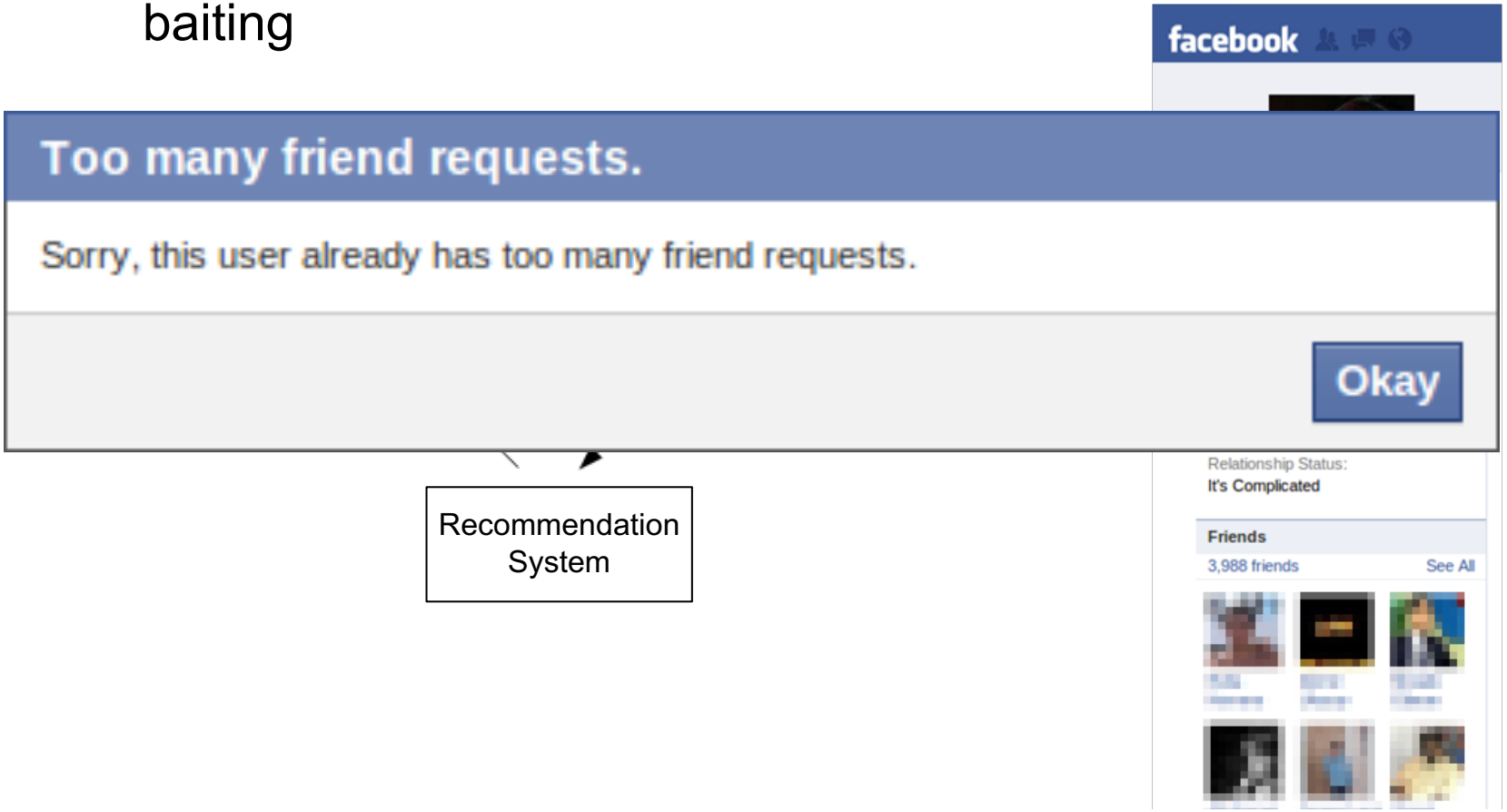
- Attack well-known by hackers in the past
  - Instead of calling victims, you make victim call you
  - e.g., you post an admin phone number

Reverse Social Engineering Attacks

- Attacks rely on a form of “baiting” to stimulate victim’s curiosity
  - Potential to reach millions of users on social networks
  - Bypasses current behavioral and filter-based detection
- Attacker waits for victim to make the initial approach
  - Victim less suspicious as she makes the initial contact
  - Higher probability of success for a follow-up attack
- Types:
  - Direct – Baiting is visible to targeted user
  - Mediated – Baiting is performed by an intermediate approach

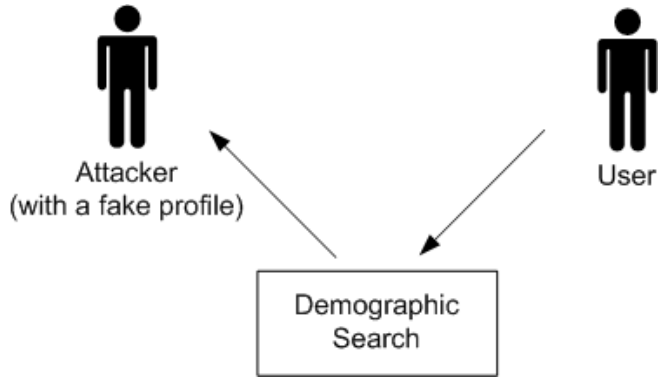
Example of Real-World RSE Attack

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

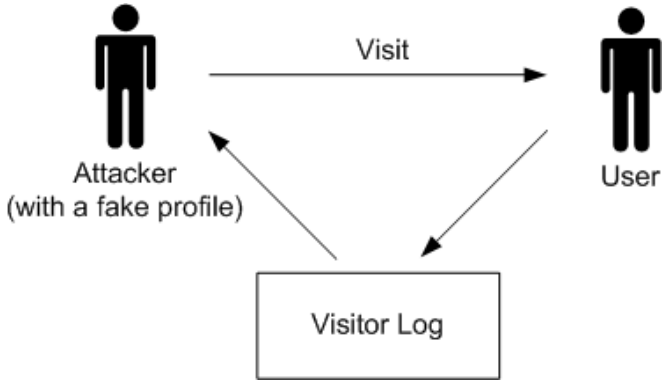


More Real-World RSE Attacks

- Demographic-Based – Mediated



- Visitor Tracking-Based – Direct



Measuring Effects – Creating Attack Profiles

- Determine characteristics which make profiles effective
  - 5 profiles with different characteristics

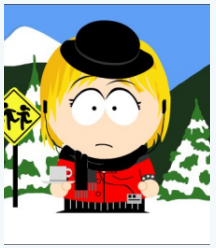
Social Network	Profile 1	Profile 2	Profile 3	Profile 4	Profile 5
Age	23	23	23	35	23
Sex	Male	Female	Female	Female	Female
Location	New York	New York	Paris	New York	New York
Picture*					

Table 1: Summary of key characteristics of profiles used.

Measuring Effects – Data

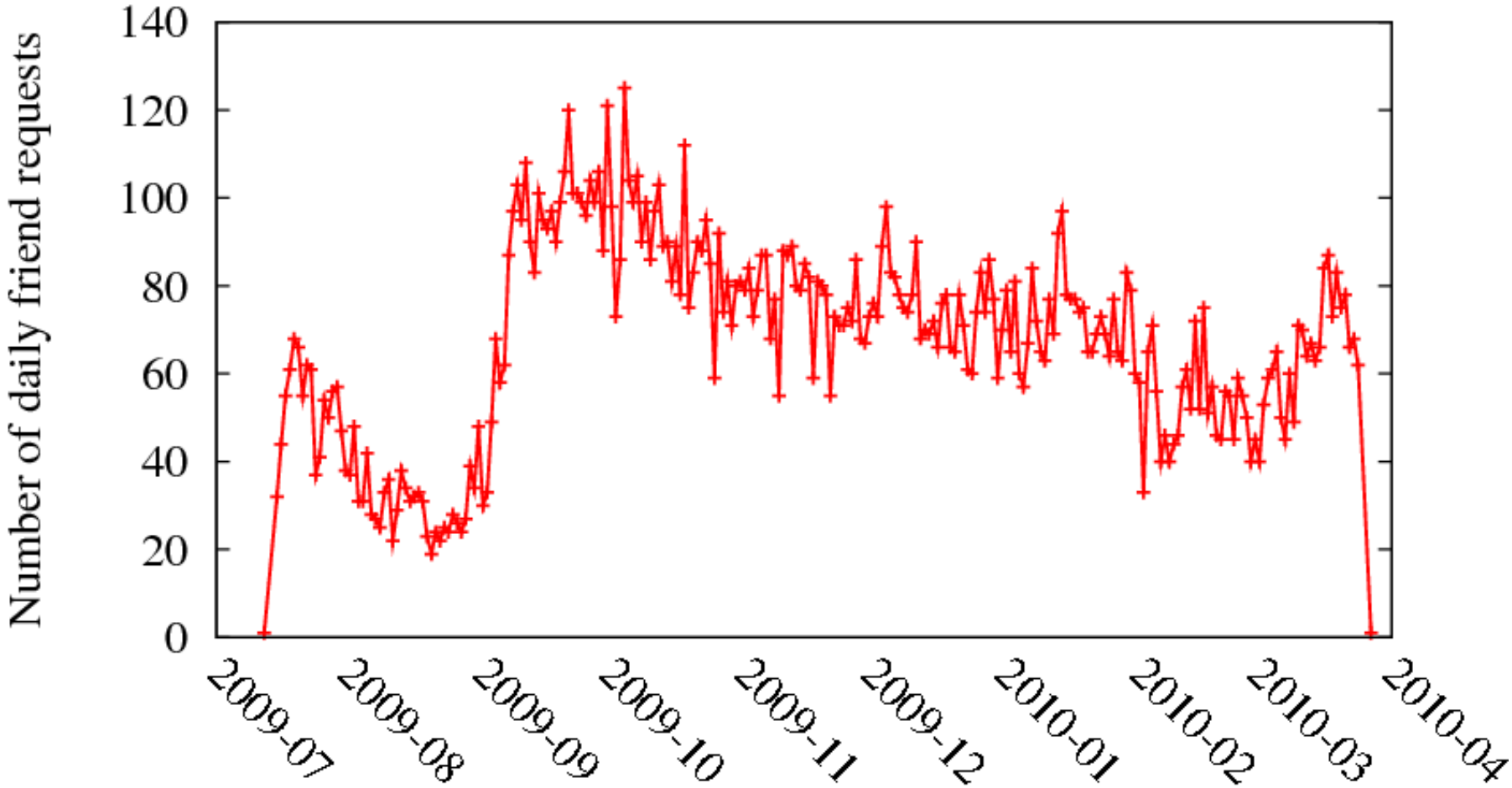
- Previous study (Balduzzi05) demonstrated using email addresses to find profiles:
  - Spammer email list from dropzone on compromised machine
  - Over 1.2 million user profiles found

Social Network	# of Targets	Example RSE Attack
Badoo	-	Demographic-Based
Facebook	250,000	Recommendation-Based
Friendster	42,000	Visitor Tracking-Based

Table 2: Number of users targeted on different social networks.

Recommendation Based RSE – Facebook Initial Experiment Results

- Account used (in Balduzzi05) received a large number of



What Do We Learn?

- Profile effectiveness
  - Attractive female profiles are highly successful
    - The urban legend is true!
  - Can be tuned to demographics of target victim(s)

- Pretexting – critical for RSE attacks
  - Excuse needed to “break the ice”
  - Recommendation system provides strongest pretexting
  - Dating site (Badoo) provides pretext based on close location

Countermeasures to RSE

- Perform recommendations based on very strong links
  - Ensure at least a few friends in common (or within n-degrees of separation)
- Adapt behavioral 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