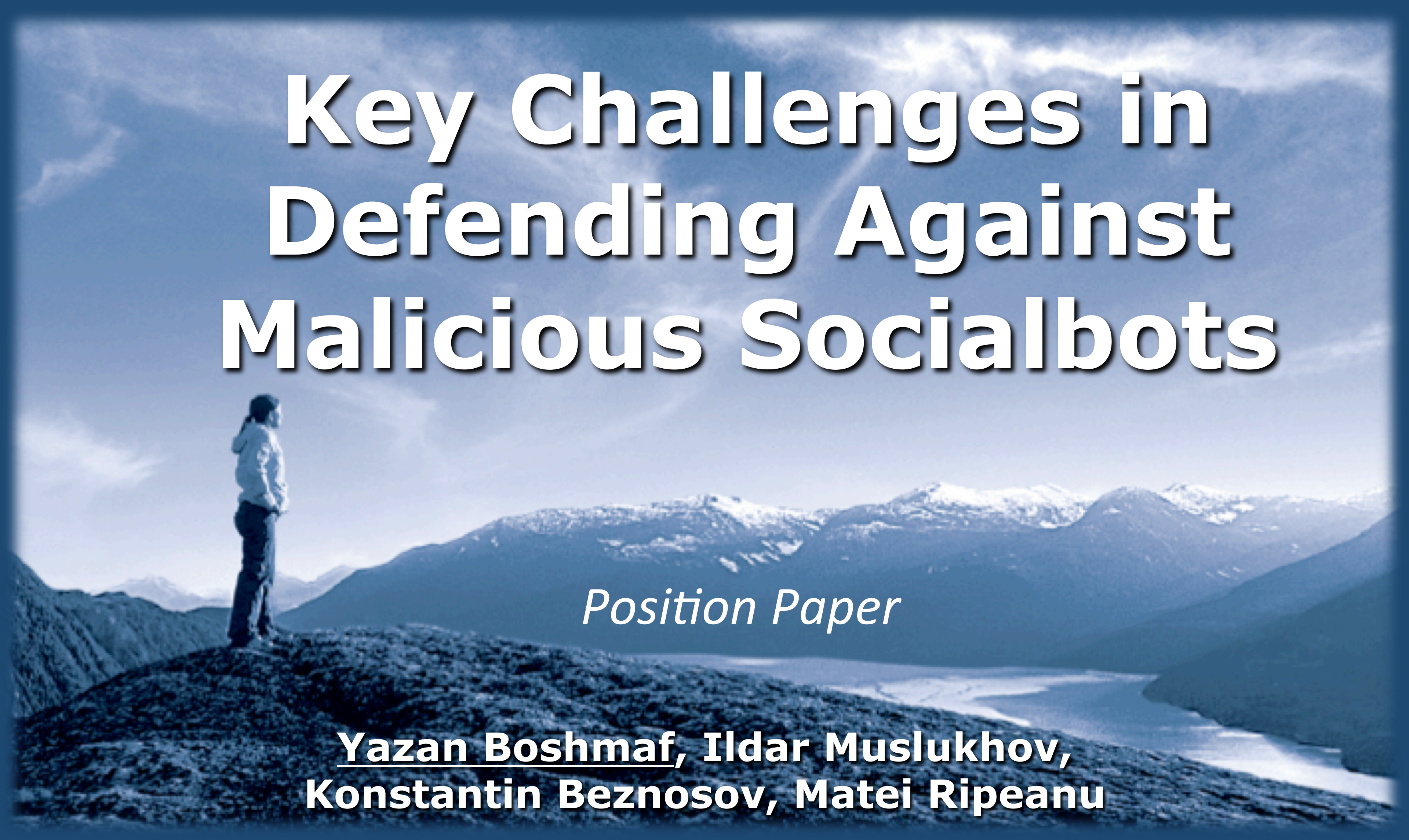


Key Challenges in Defending Against Malicious Socialbots

Position Paper

Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

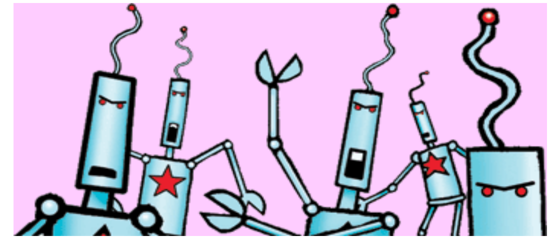
Laboratory for Education and Research in Secure Systems Engineering (LERSSE)

Networked Systems Laboratory (NetSysLab)

Department of Electrical & Computer Engineering

Outline

Problem Motivation



Socialbots

OSN Security

Challenges

Problem Motivation

Reaching Out to Millions

Obama Raised Half a Billion Online in 2008

(Source: Jose Vargas, Voices on The Washington Post, November, 2008)

Mobilizing the Masses

The Arab Spring, January 2011 - Now

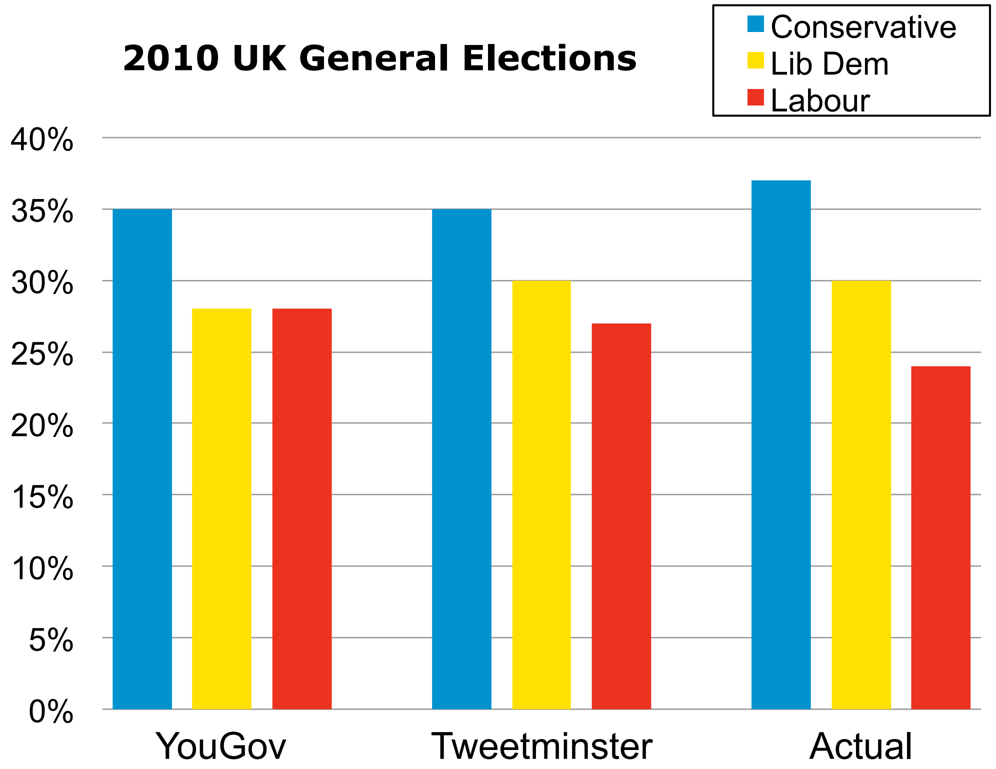
Photo credit: Peter Macdiarmid, Getty Images

Photo credit: Steve Crisp, Reuters

Salem et al. Civil movements: The impact of Facebook and Twitter. The Arab Social Media Report, 2011

Predicting the Future: Elections

Twitter elections predictions (*Tweetminster*) outperform market research (*YouGov*)

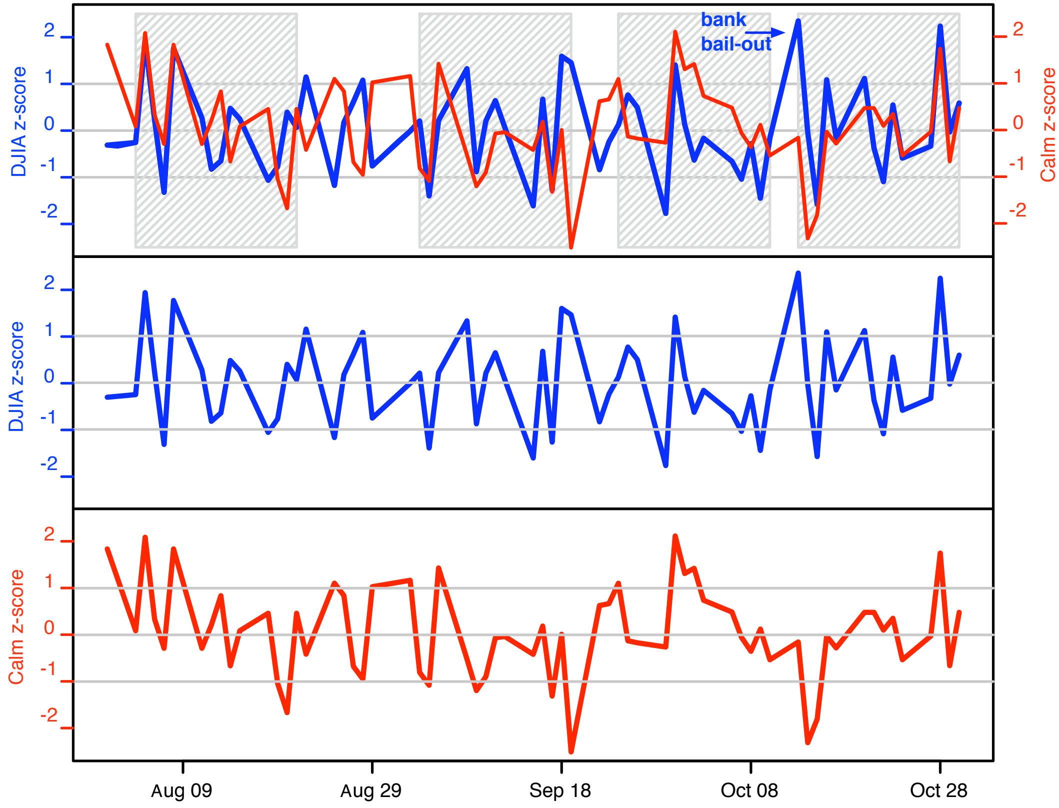


(Source: Jemima Koss, The Guardian, May 2010)

Predicting the Future: Markets

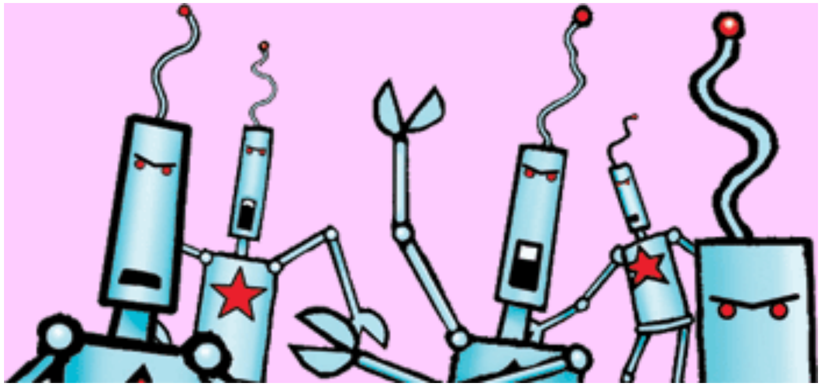
Twitter mood (*Calm*) predicts Dow Jones Industrial Average (*DJIA*)

Day-to-day Overlap



Calm lagged by 3 days

Bollen et al. Twitter mood predicts the stock market. J. Comp. Sc. March, 2011.



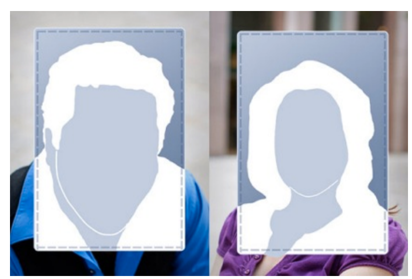
Socialbots

Bots and Socialbots

Computer program used to perform highly repetitive operations (AI?)

Automation software
(to pass off as human)

+

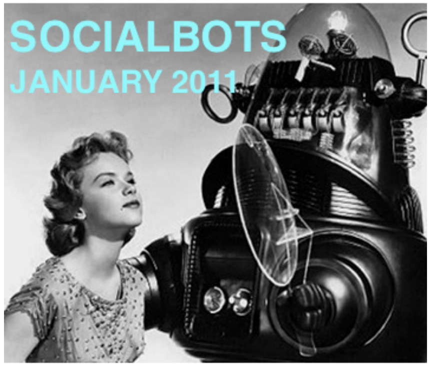


Social media account

Socialbot

Rise of the Socialbots

Zack Coburn and Greg Marra, Olin College, 2010



The Web Ecology Project (Social Engineering), 2011

ACM Interactions Magazine Cover Story, April 2012

Misusing Socialbots on a Large Scale?

An automated social engineering tool for:

Infiltration

Misinformation

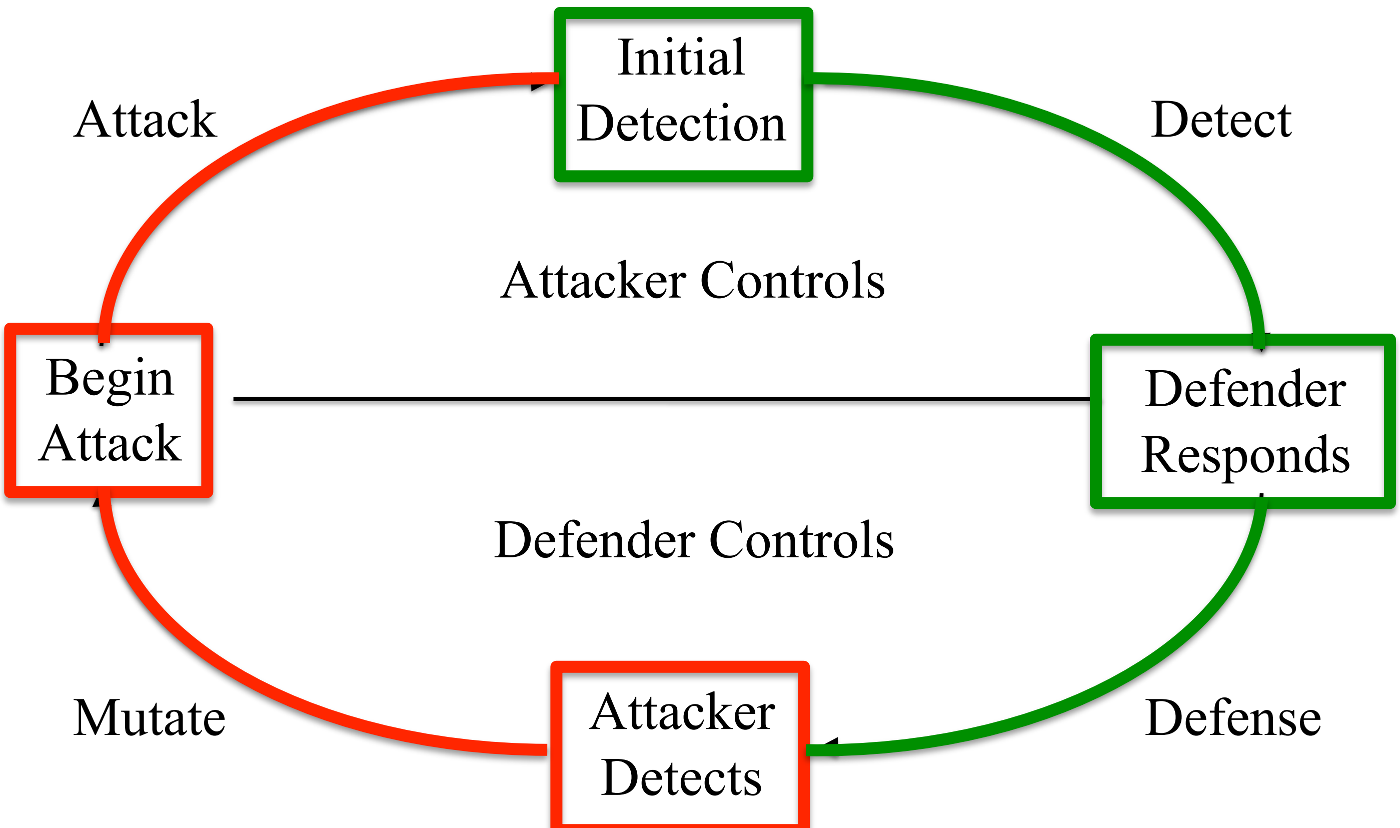
Data collection

Boshmaf et al. The Socialbot Network: When Bots Socialize for Fame and Money. ACSAC'11

OSN Security

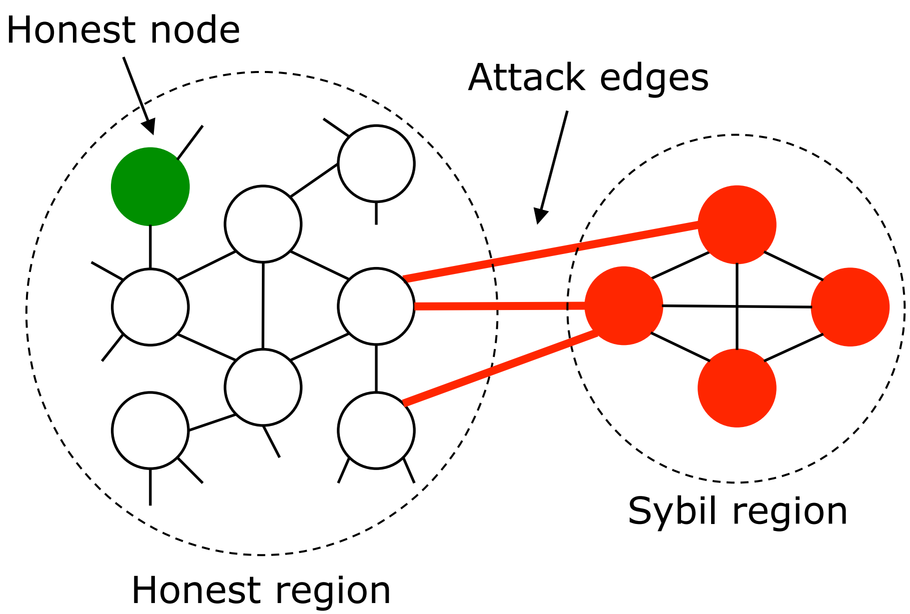
Tolerate Socialbots

Adversarial Machine Learning

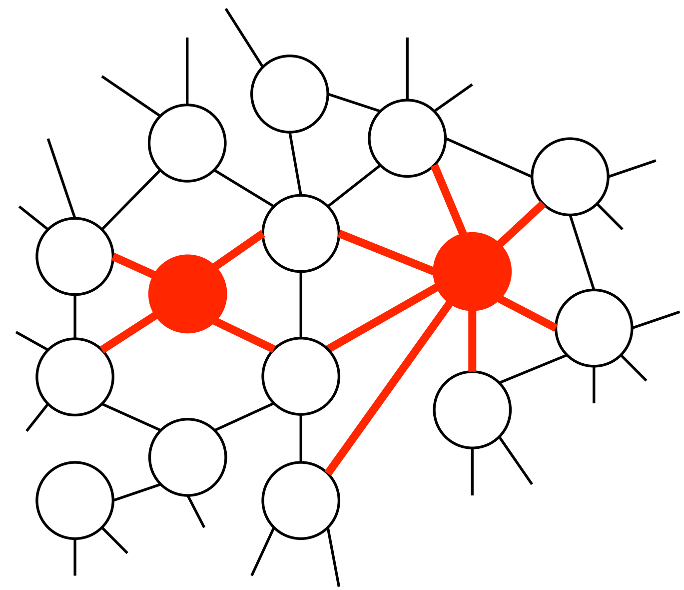


Stein et al., The Facebook Immune System, EuroSys – SNS, 2011

Graph-theoretic Defense Techniques



Sybil detection via social networks[1]



With adversary running large-scale infiltration[2]

[1] Haifeng Yu. Sybil Defenses via Social Networks: A Tutorial and Survey. ACM SIGACT News'11
[2] Boshmaf et al. The Socialbot Network: When Bots Socialize for Fame and Money. ACSAC'11

Prevent Socialbots

Observation: It's all about automation

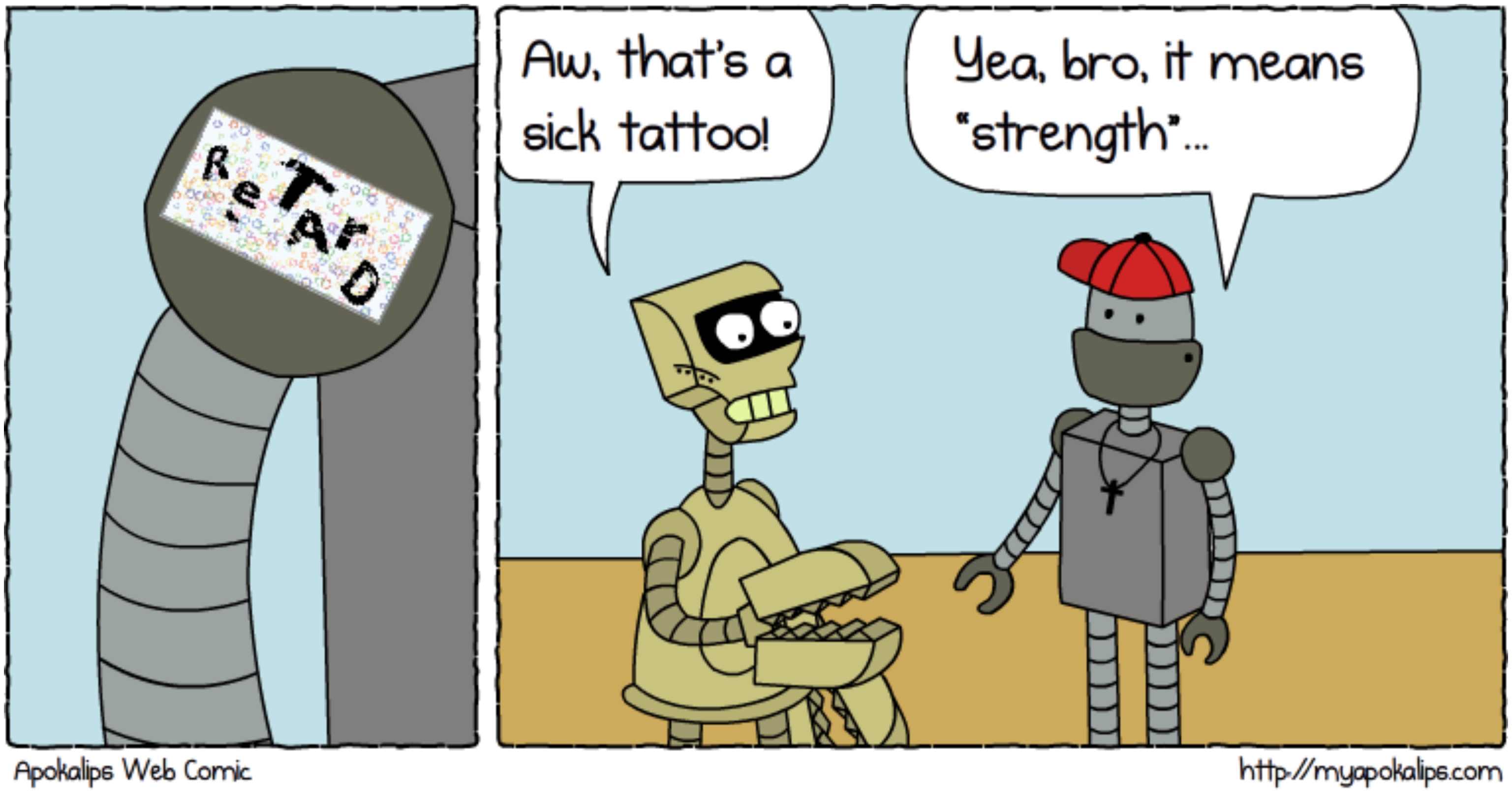
Prevent it and the socialbot threat will go away (almost surely)

Not an easy job!

Challenges

Solve at least one

OSN Vulnerabilities: Ineffective CAPTCHAs

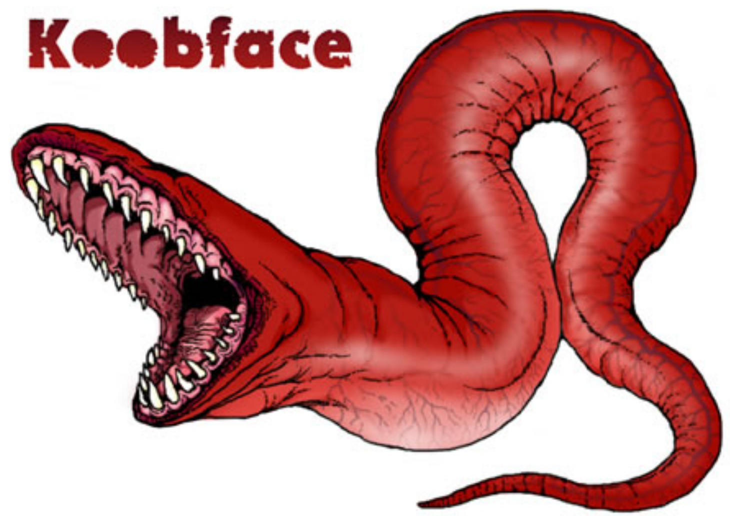


OSN Vulnerabilities: Ineffective CAPTCHAs

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

CAPTCHA-solving businesses



Koobface Botnet

Motoyama et al. Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context. Usenix Security, 2010
Baltazar et al. The Real Face of Koobface: The Largest Web2.0 Botnet Explained. Trend Micro Threat Research, 2009

UBC

OSN Vulnerabilities: Ineffective CAPTCHAs

CAPTCHA-solving businesses

Koobface Botnet

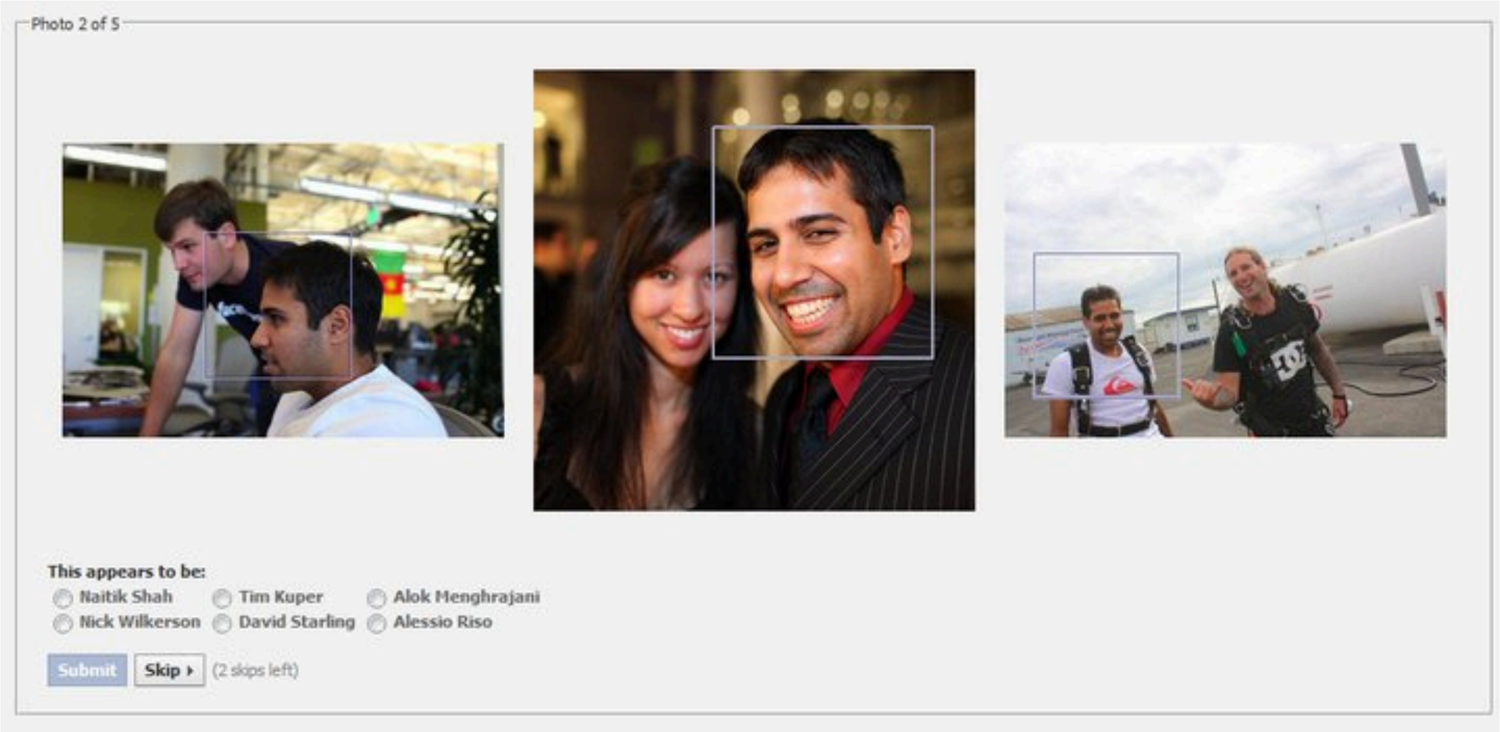
Motoyama et al. Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context. Usenix Security, 2010
Baltazar et al. The Real Face of Koobface: The Largest Web2.0 Botnet Explained. Trend Micro Threat Research, 2009

Challenge #1

Design a reverse Turing test that is *usable* and *effective* even against "illegitimate" human solvers

How about Social Authentication?

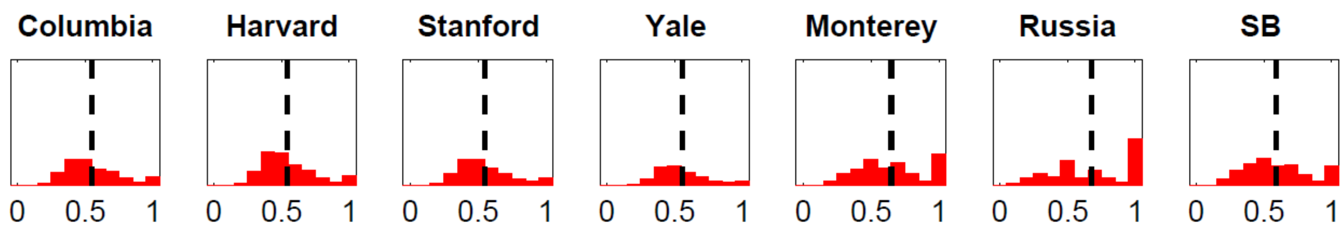
Use "personal" social knowledge to challenge users



Kim et al. Social authentication: Harder than it looks. FC'12

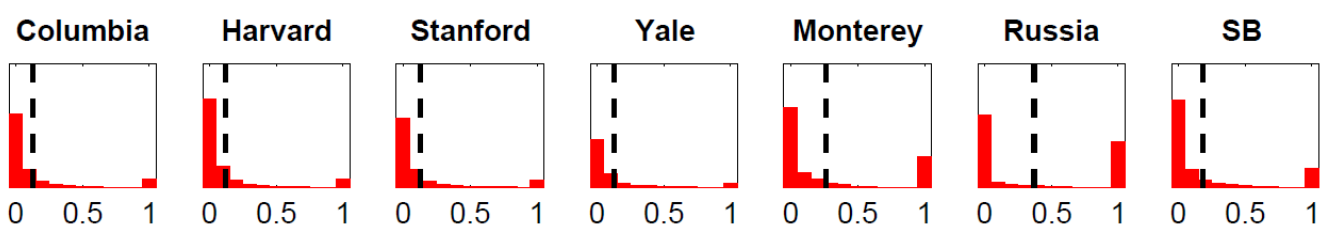
Histogram of Attack Advantage

When the number of challenge images is 1,



many people are vulnerable to impersonation.

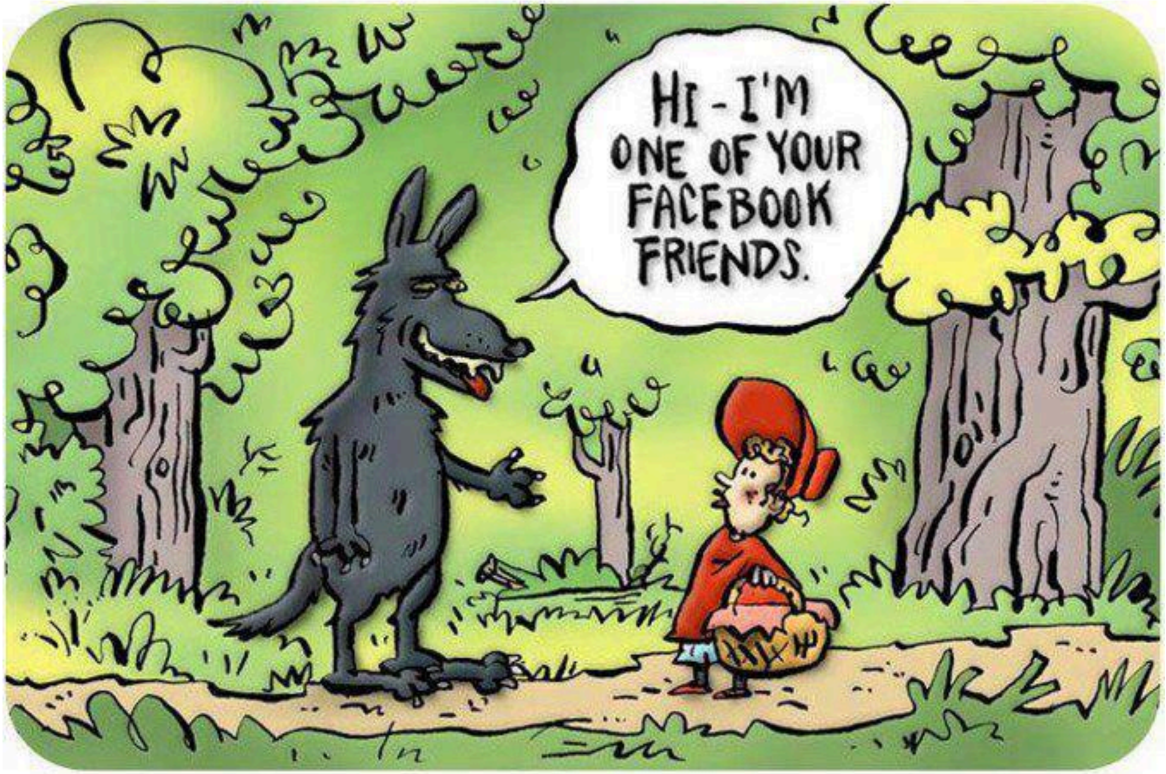
Even for 5 challenge images,



some people can be impersonated with probability 100%.

Kim et al. Social authentication: Harder than it looks. FC'12

OSN Vulnerabilities: Fake (Sybil) User Accounts and Profiles



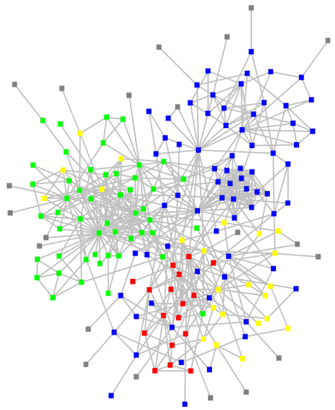
Challenge #2

Guarantee an anonymous, yet credible, online-offline identity binding in online and open-access systems

How can we deal with Sybils?

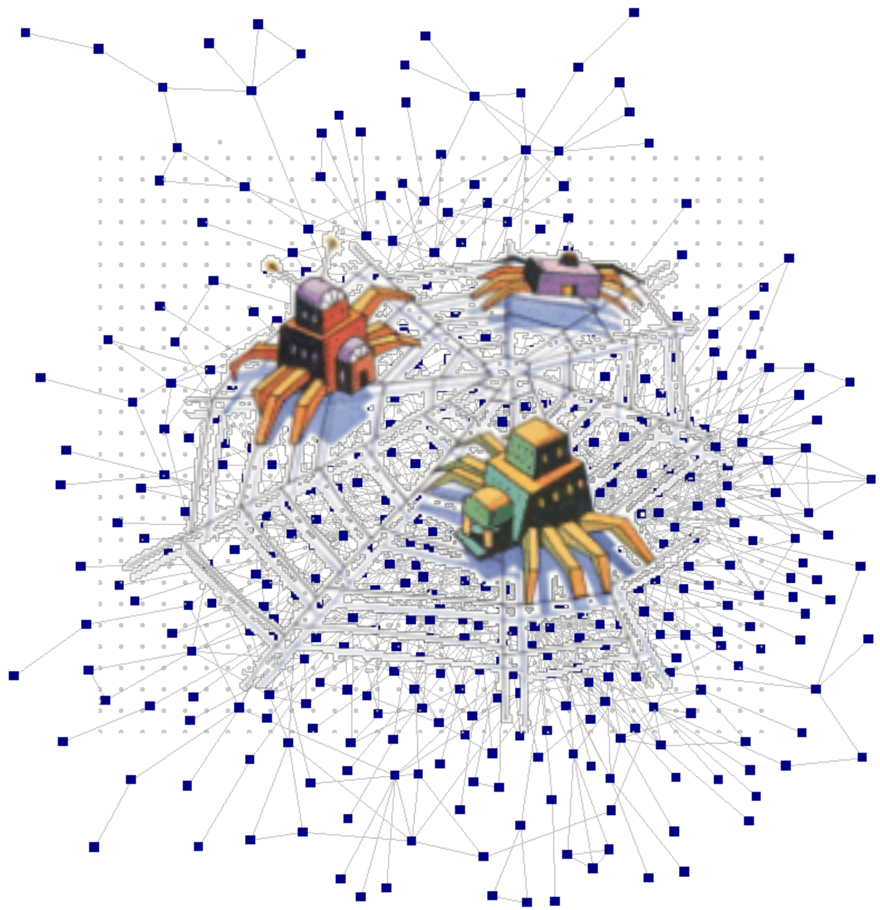
Centralized trusted authority

Tie identities to resources



Use external information

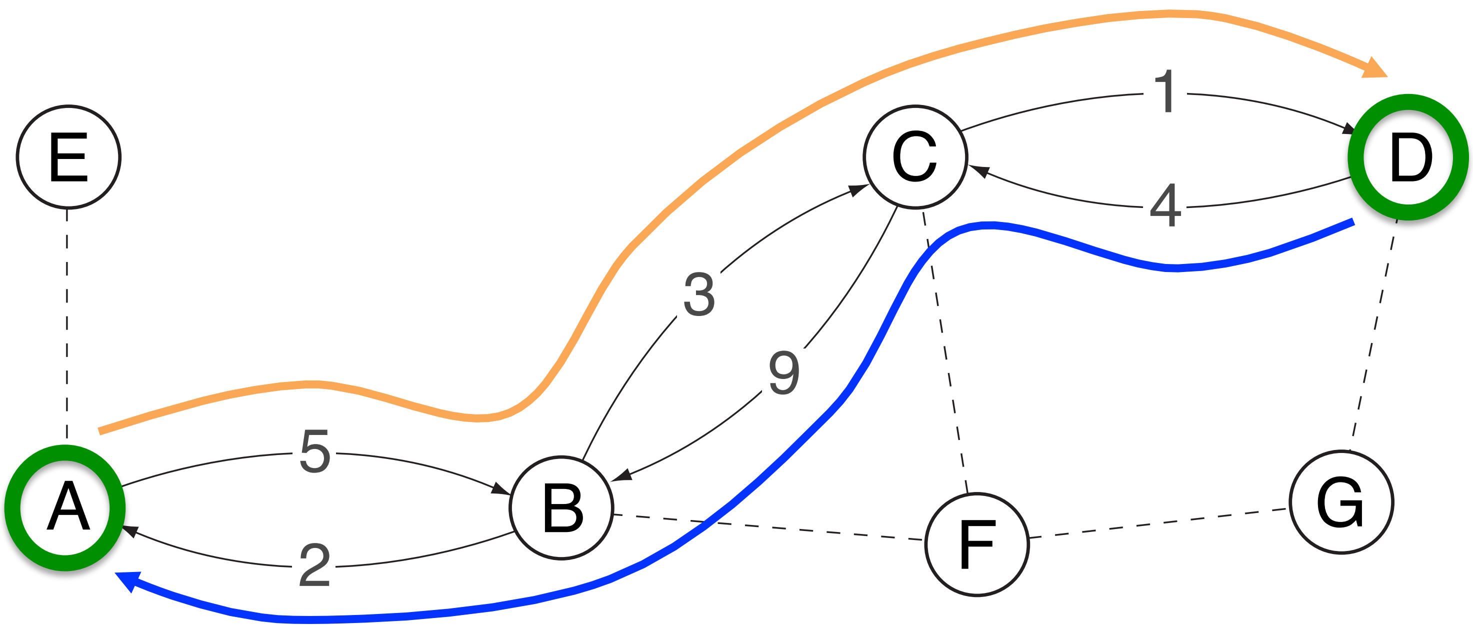
OSN Vulnerabilities: Large-Scale Network Crawls



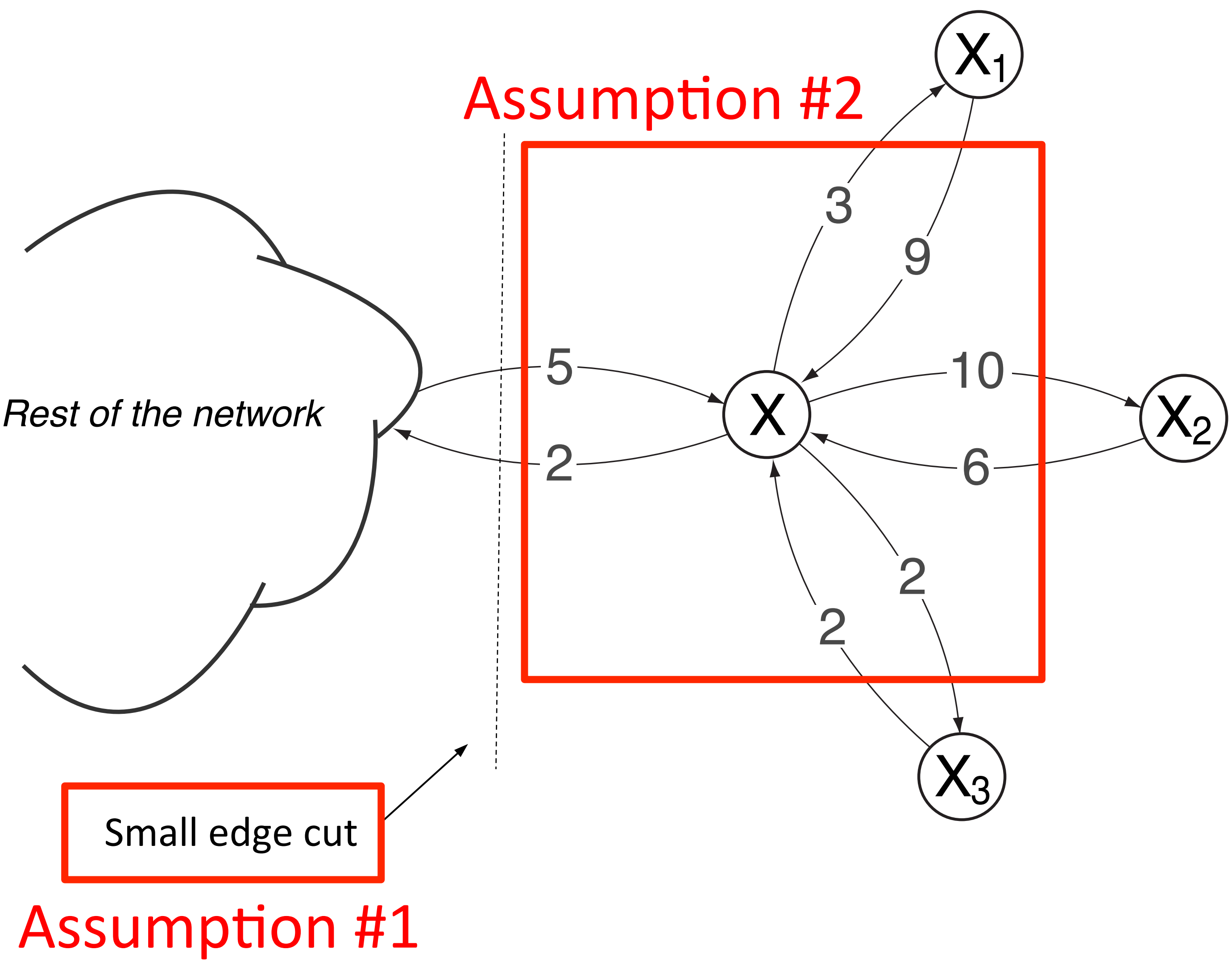
Challenge #3

Effectively limit large-scale Sybil crawls of OSNs without restricting users' social experience.

How about using a credit network?

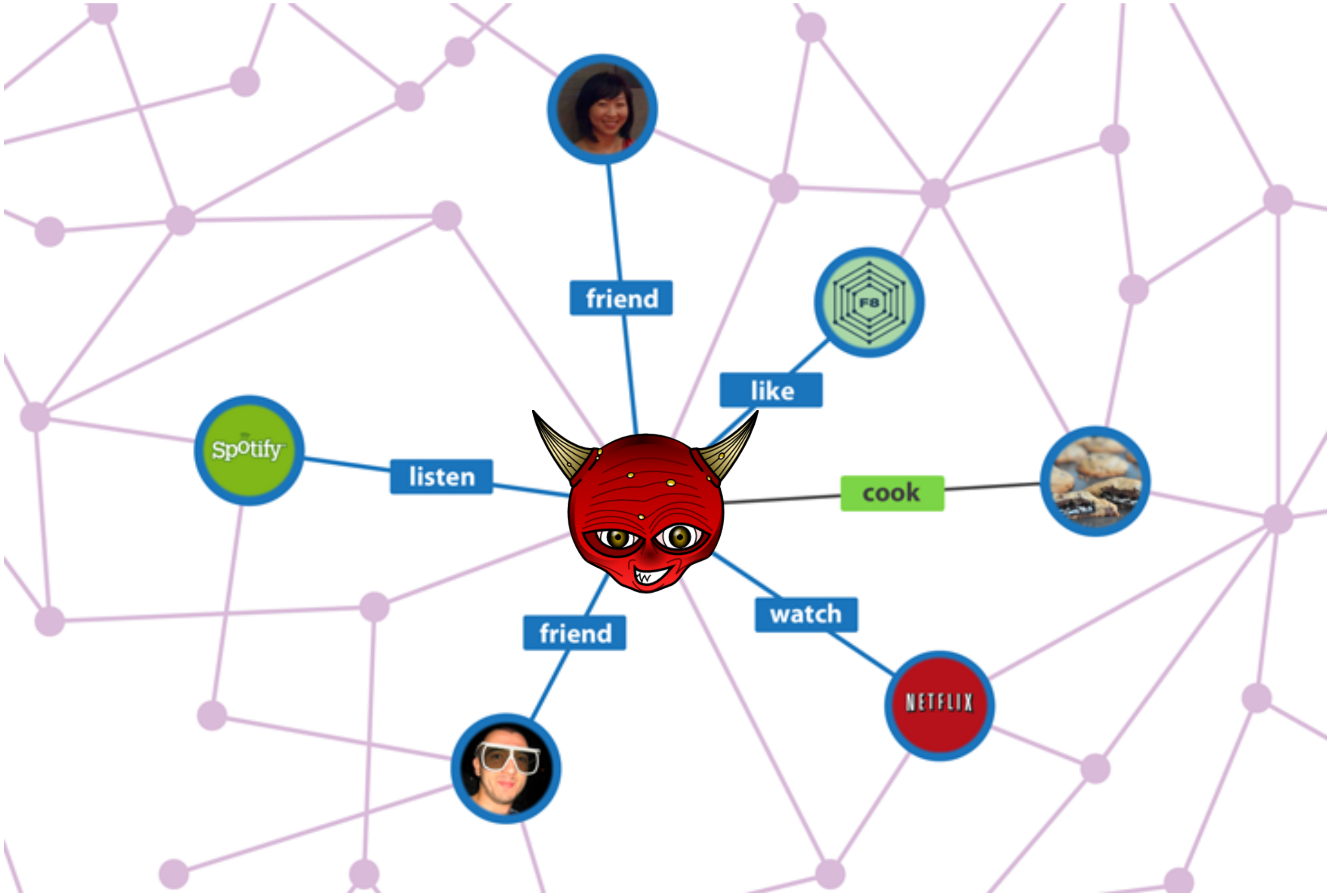


Viswanath et al. Exploring the design space of social network-based Sybil defenses. COMSNETS'12



Viswanath et al. Exploring the design space of social network-based Sybil defenses. COMSNETS'12

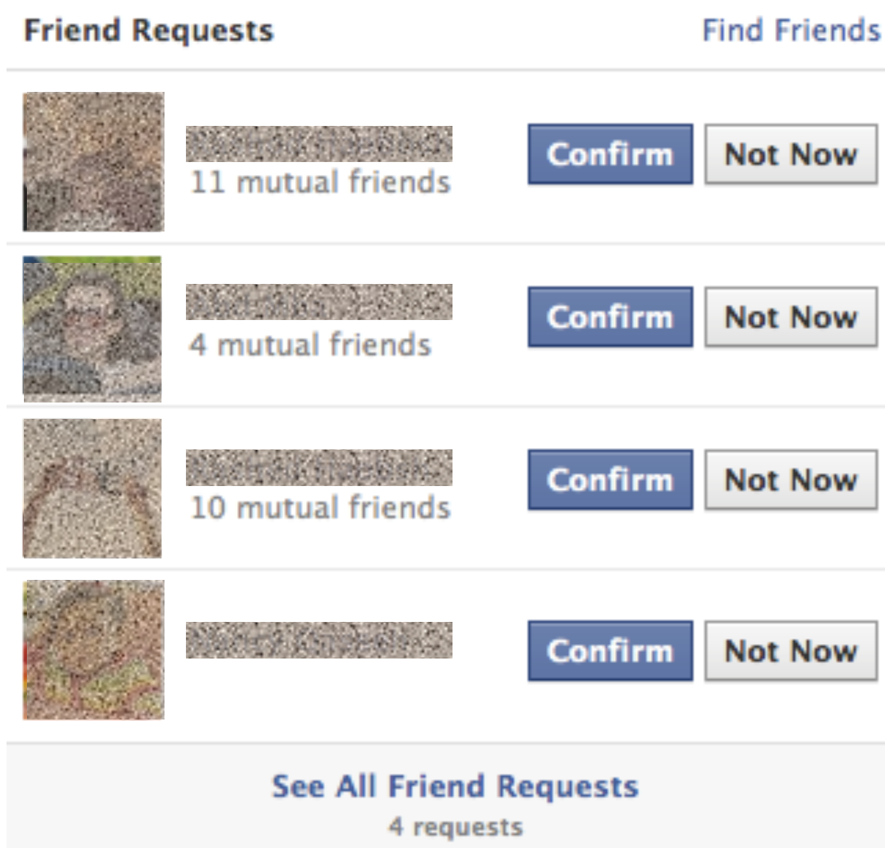
OSN Vulnerabilities: Exploitable Platforms and APIs



#4

Detect abusive and automated usage of OSN platforms and their social APIs across the Internet

OSN Vulnerabilities: Poorly Designed Privacy/Security Controls



Challenge #5

Develop usable OSN security and privacy controls that help users make more informed decisions


Risk Communication
Risk Management
Risk Analysis
Public

Take-home message(s)

- Large-scale infiltration is feasible
  - has serious privacy and security implications

- Socialbots make it difficult for OSN security defenses and their users to detect their true nature
  - defending against such bots raises a set of unique challenges

- Effective, socio-technical defenses less vulnerable to *both* human and technical exploits are needed

Key Challenges in Defending Against Malicious Socialbots

Yazan Boshmaf

Ildar Muslukhov

Konstantin Beznosov

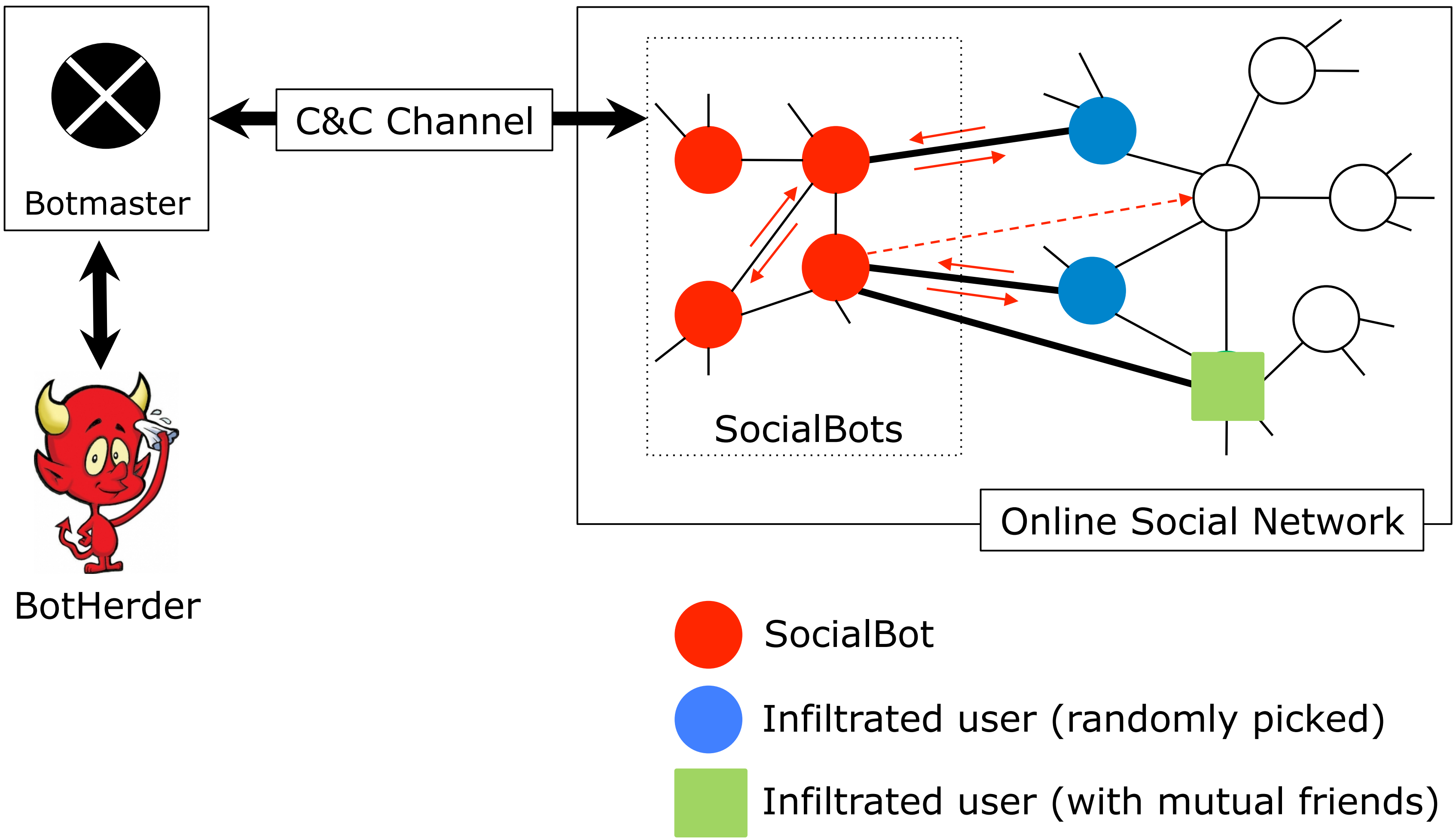
Matei Ripeanu

Funded by:

NSERC CRSNG

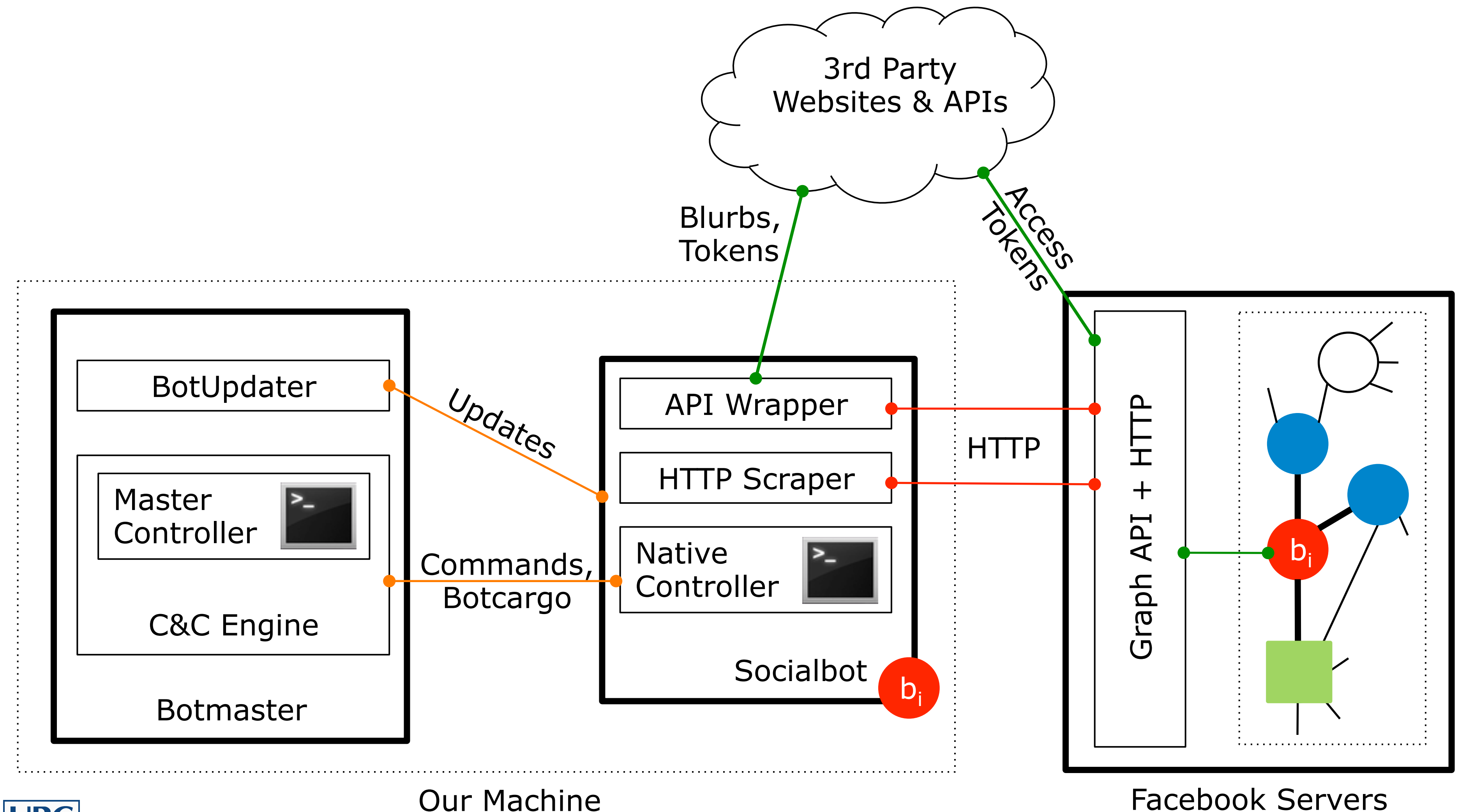
Backup

Socialbot Network: Concept



Boshmaf et al. The Socialbot Network: When Bots Socialize for Fame and Money. ACSAC'11

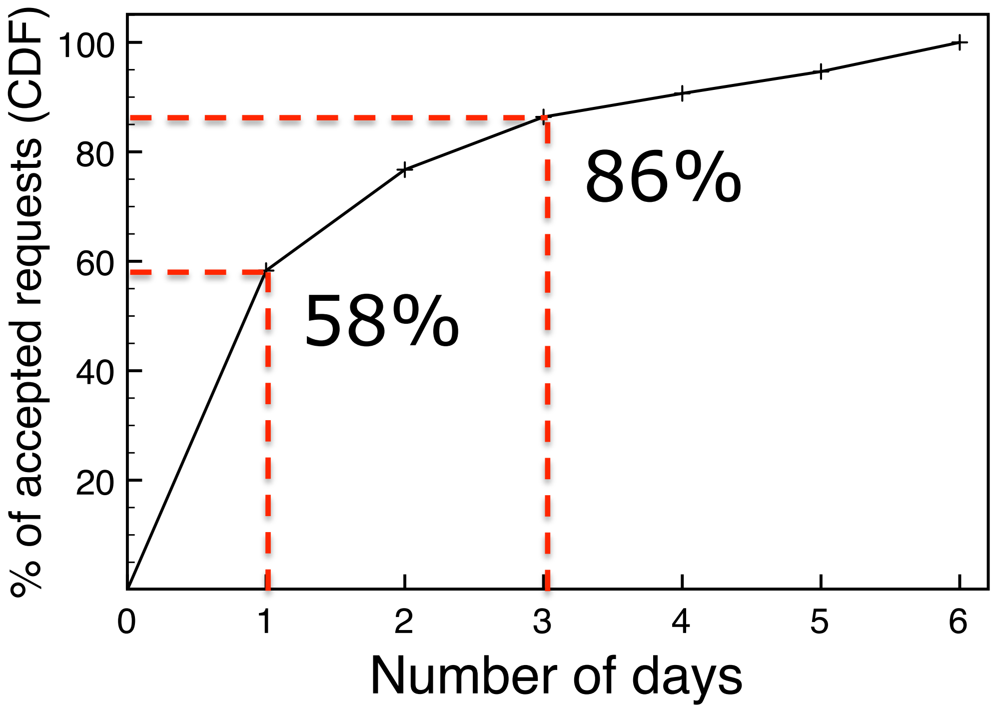
Prototype Architecture



Methodology

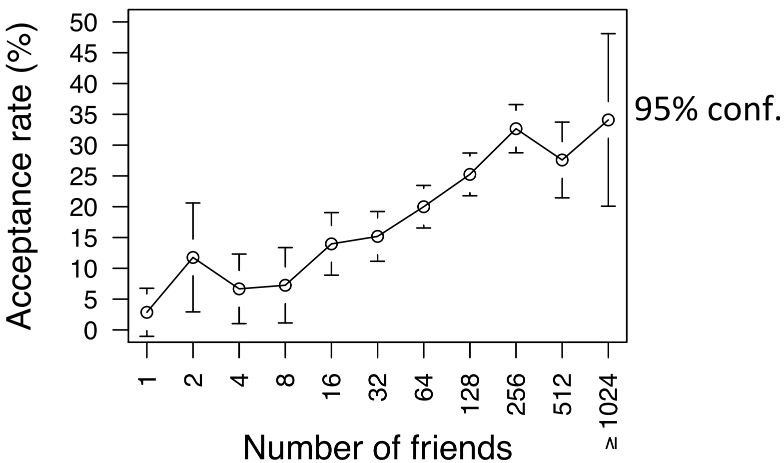
- Prototype on Facebook
- 102 Socialbots, single Botmaster
- Operated for 8 weeks (Spring 2011)
- Single machine
  - Different IPs
  - HTTP proxy emulating different browsers and OSs
- Approved by UBC ethics board

Most Users Decide Within Three Days

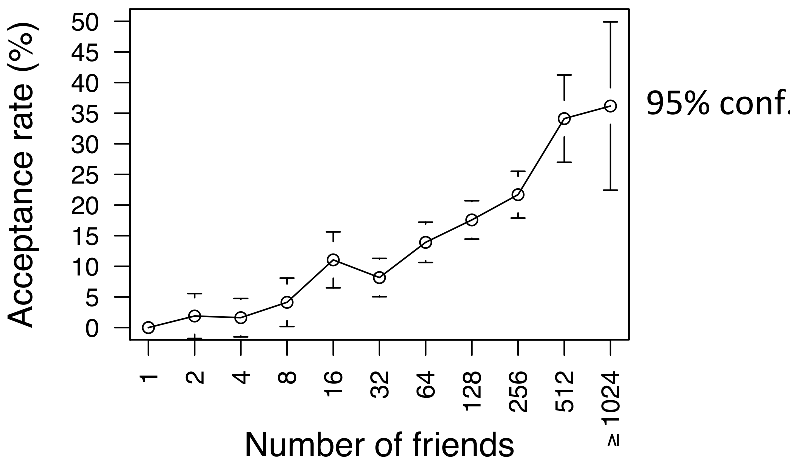


Too Many Friends: Too Many Bots?

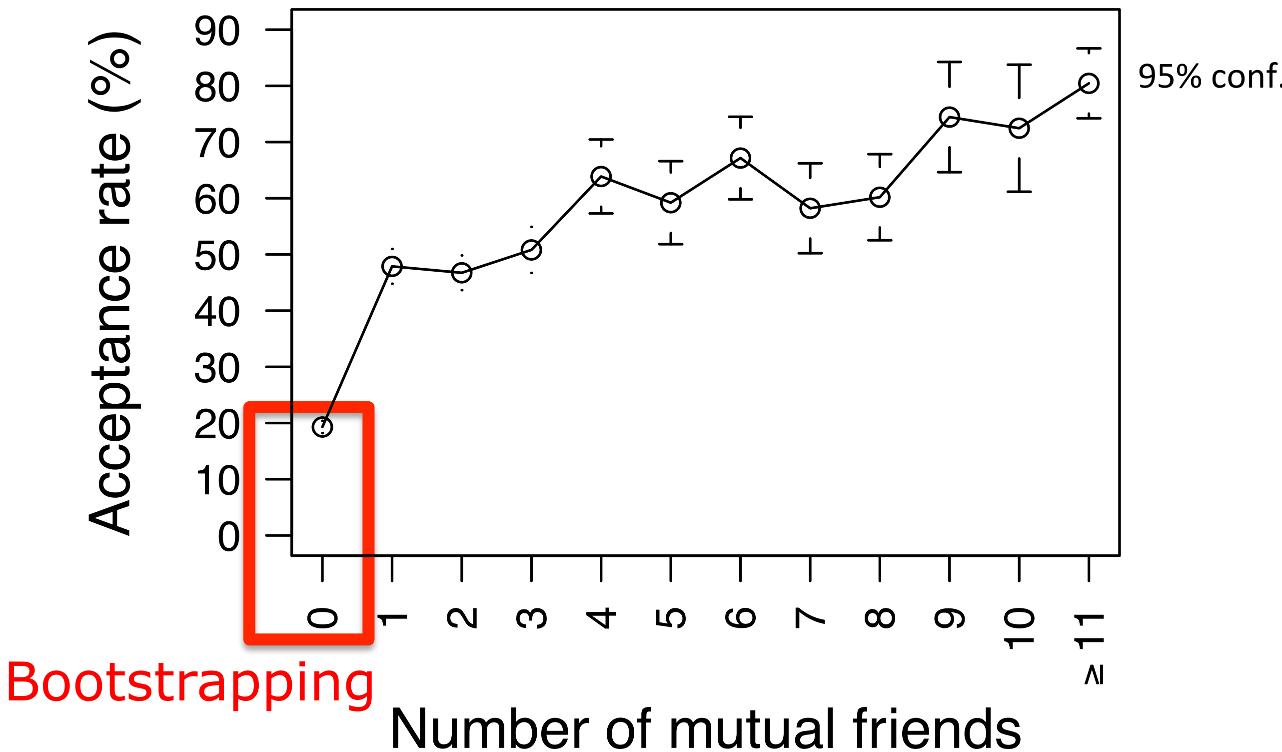
f-socialbots



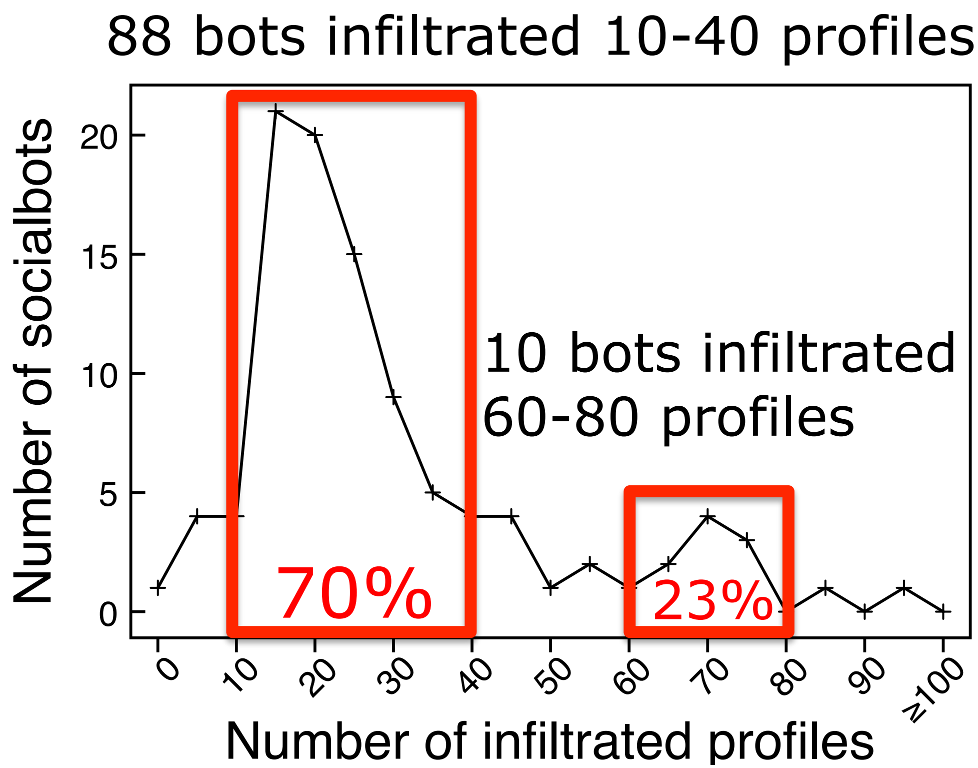
m-socialbots



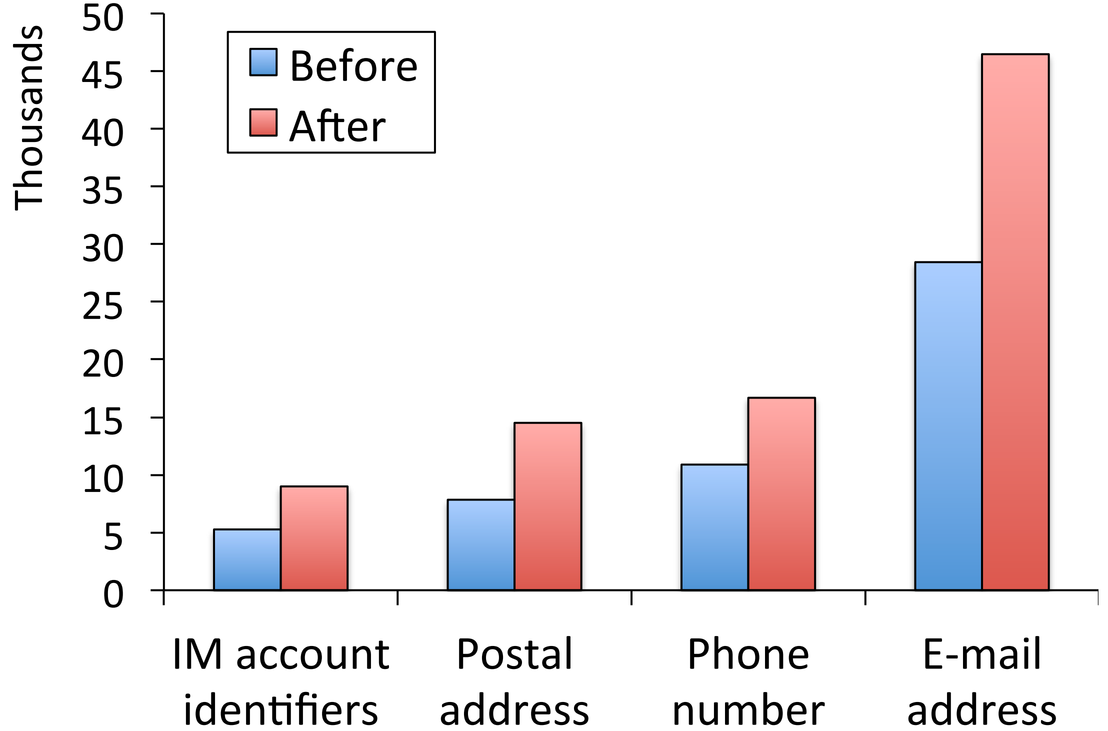
Mutual Friends Matter



Successful Infiltration is Team Work



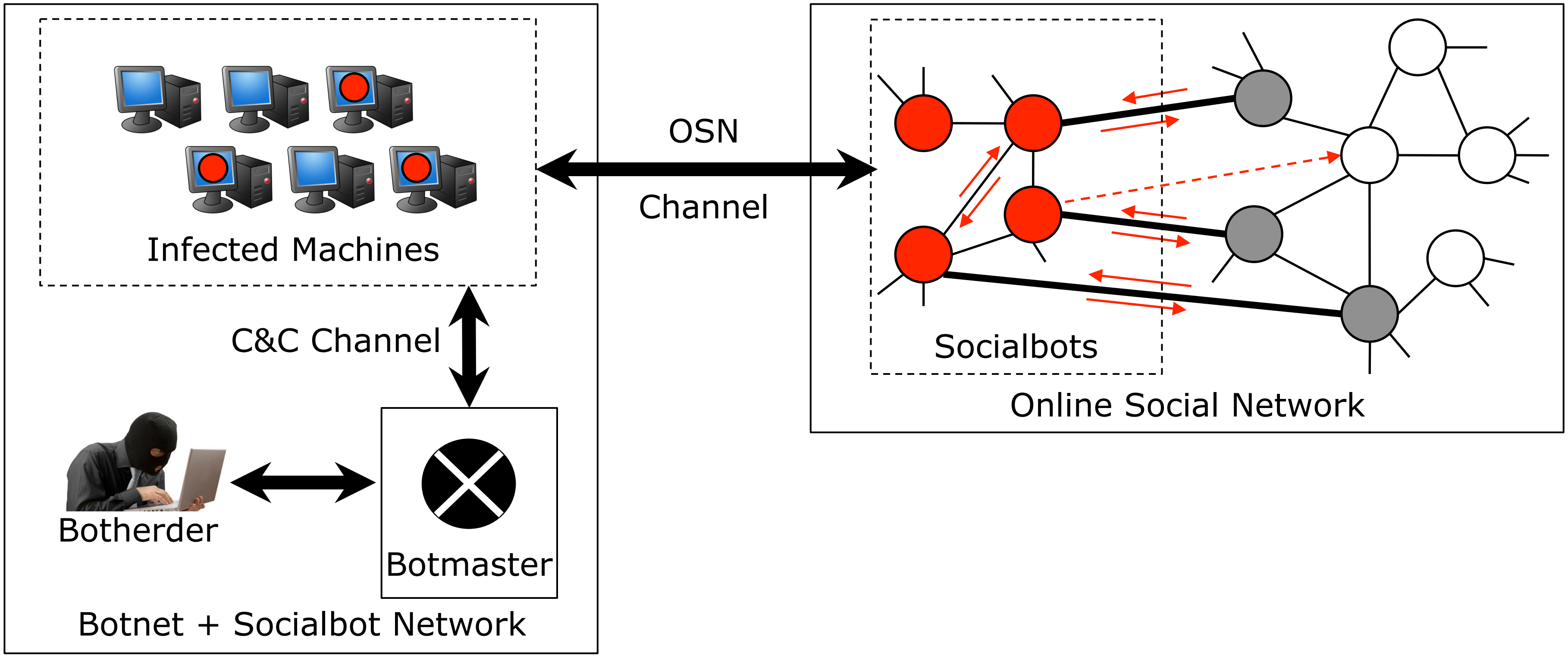
Private Data Exposed



Socialbots: **102**, their friends: **3,055**, their friends' friends: **1,085,785**

Birth dates: 48,810 before ➔ 580,649 after (11.9x more)

Web-based Botnet Integration



Advice: OSNs and Security Research