ISC 2008
INFORMATION SECURITY CONFERENCE

Antisocial Networks

Turning a Social Network into a Botnet

E. Athanasopoulos (FORTH/Greece), A. Makridakis (FORTH/Greece), S. Antonatos (FORTH/Greece), D. Antoniades (FORTH/Greece), S. I‖‖oannidis (‖FORTH/Greece), K. G. Anagnostakis (I2R/Singapore), E. P. Markatos (FORTH/Greece)

So, this paper is about

Social Networks

…Or…

Antisocial Networks

Social Networks

- A new Web platform
  - MySpace, Facebook, LinkedIn, Orkut
- Built over human habits and interests
  - Groups, fun clubs, games, etc.
- Significant‼ ‼ market penetration
  - Major attractor of ad campaigns

Amazingly popular!

By Numbers

- Millions of active users
- Millions of photos
- Millions of interest groups
- Thousands of different applications
- Thousands of Games

MySpace

- More than 110 million monthly active users
- 1 in 4 Americans is on MySpace
- As common to have MySpace as it is to own a dog (UK)
- 300,000 new users per day

(source: myspace.com)

Facebook

- More than 100 million active users
- 4th most-trafficked Web site in the world
- No. 1 photo sharing application
- More than 24 million photos uploaded per day

(source:‼ facebook.com)

In Other Words

A distributed platform
of **millions** of
active Web browsers

Research Question

Can we use this platform for **antisocial activities**, i.e. launching a Distributed Denial of Service attack?

Antisocial is not only DDoS!

- Unsolicited Web requests that can brake a Web site's statistics
  - Nobody wants auto generated requests by scripts
- Port Scanning
  - Use Web 2.0 technologies for port scanning
- Malware propagation
- XSS Attacks

Antisocial in our context

Any malicious activity,
which may be launched using a
Web browser

RoadMap

- FaceBot Architecture
- Experimental Evaluation
- Attack Firepower
- Countermeasures
- Conclusions

RoadMap

- **FaceBot Architecture**
- Experimental Evaluation
- Attack Firepower
- Countermeasures
- Conclusions

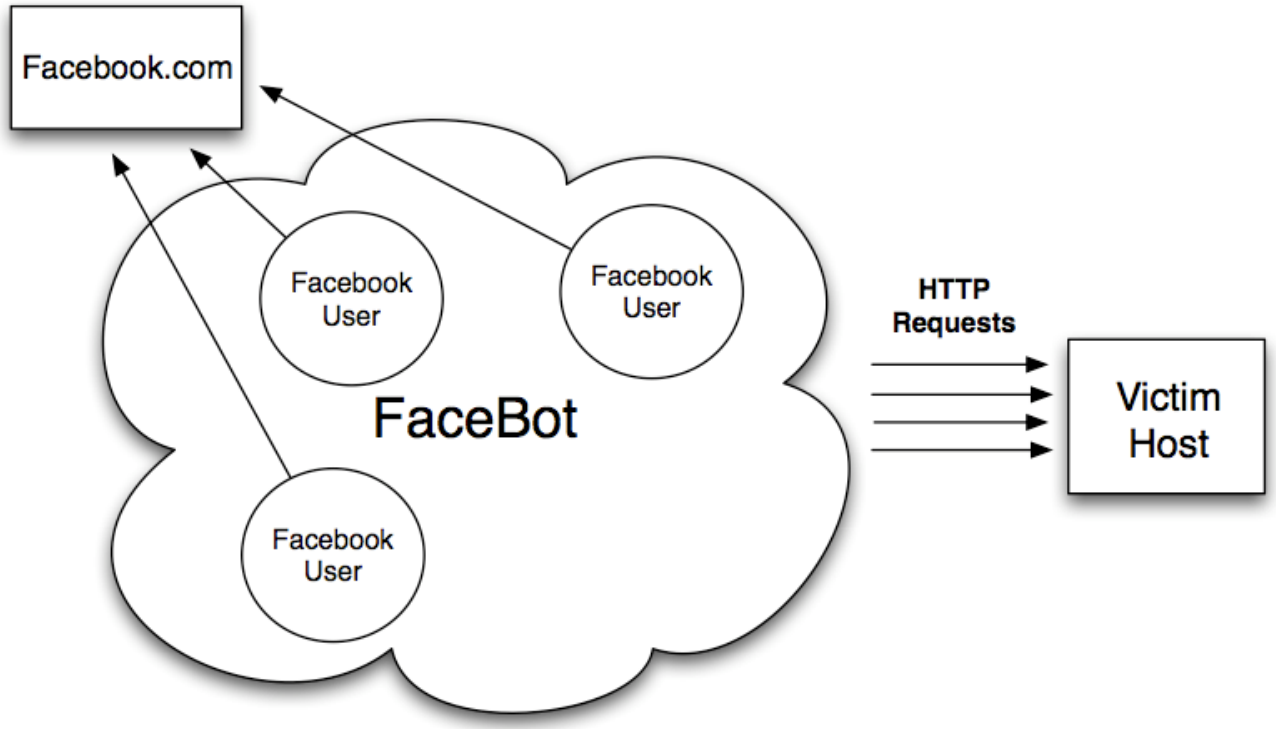
What is a FaceBot?

A Facebook application, which, secretly (i.e. the user does not notice), requests resources from a **victim** host.

Recipe

- Find an idea for a Facebook application
  - It doesn't need to be something unique, for example: "What is your name in Hebrew?", "How much do you love insects?"
- Implement the application
  - Needs basic knowledge of PHP, HTML
- Insert some hidden frames in your code
  - `<iframe name="1" src=http://victim/image1.jpg/>`
- Publish your application in a Facebook hosting provider
  - Joyent Free Accelerator
- Announce your application to your friends

Result


Facebook.com
Facebook User
Facebook User
Facebook User
FaceBot
HTTP Requests
Victim Host

RoadMap

- FaceBot Architecture
- **Experimental Evaluation**
- Attack Firepower
- Countermeasures
- Conclusions

Setup

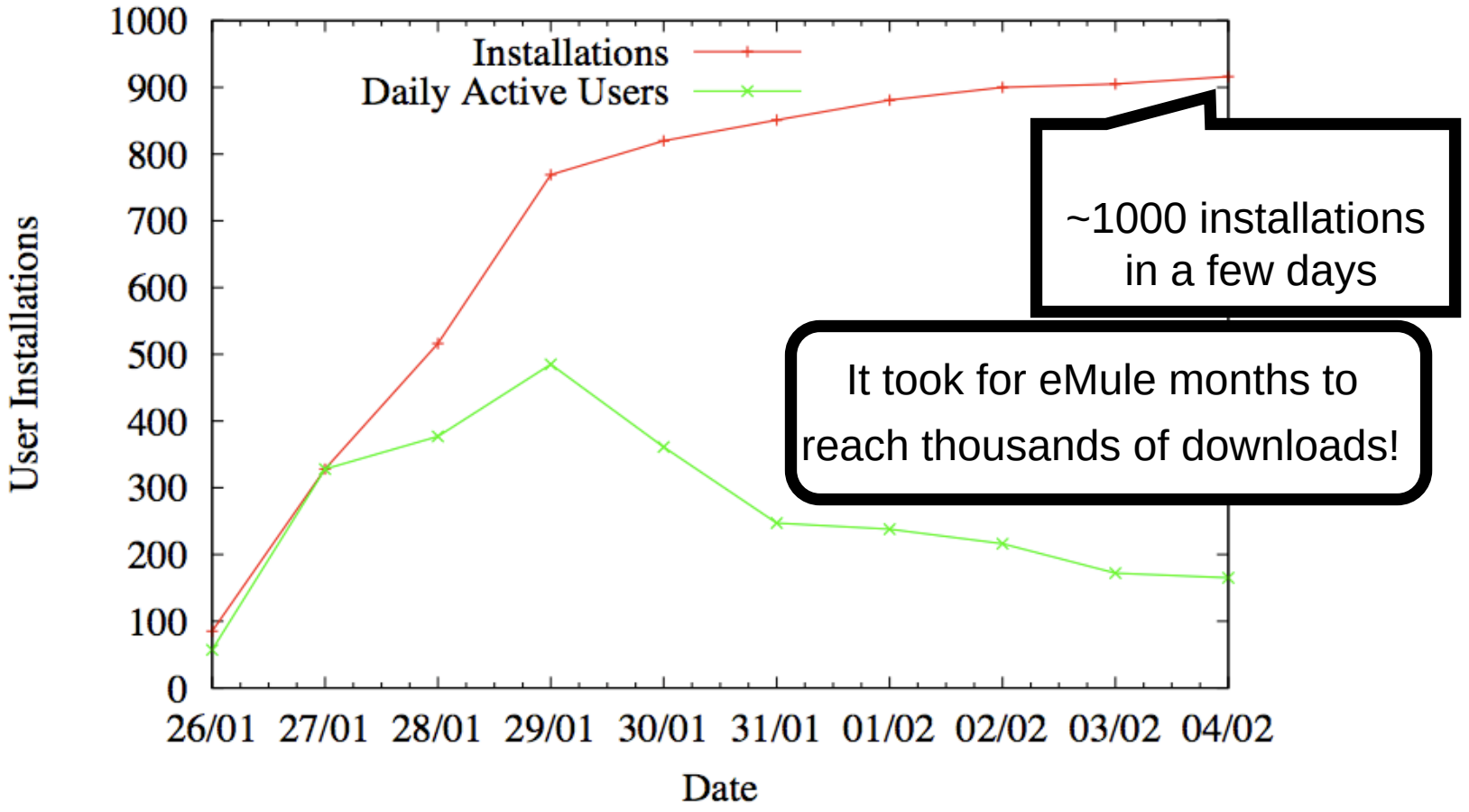
- We created an application, namely “Photo of the Day”
- Each time a user was visiting the application a photo was displayed
- In addition, without the user knowing, requests of 600 Kbytes were sent to one of our Web servers
- We announced our application to Facebook

Least Effort

- Most of the Facebook applications require the user to invite friends in order to install them
  - “I am application Foo. If you want to install me you must tell about me to 20 of your friends”.
- We did not implement this feature to our application
- We announced our application only to our colleagues and friends

Experimental Results

Popularity



~1000 installations in a few days

It took for eMule months to reach thousands of downloads!

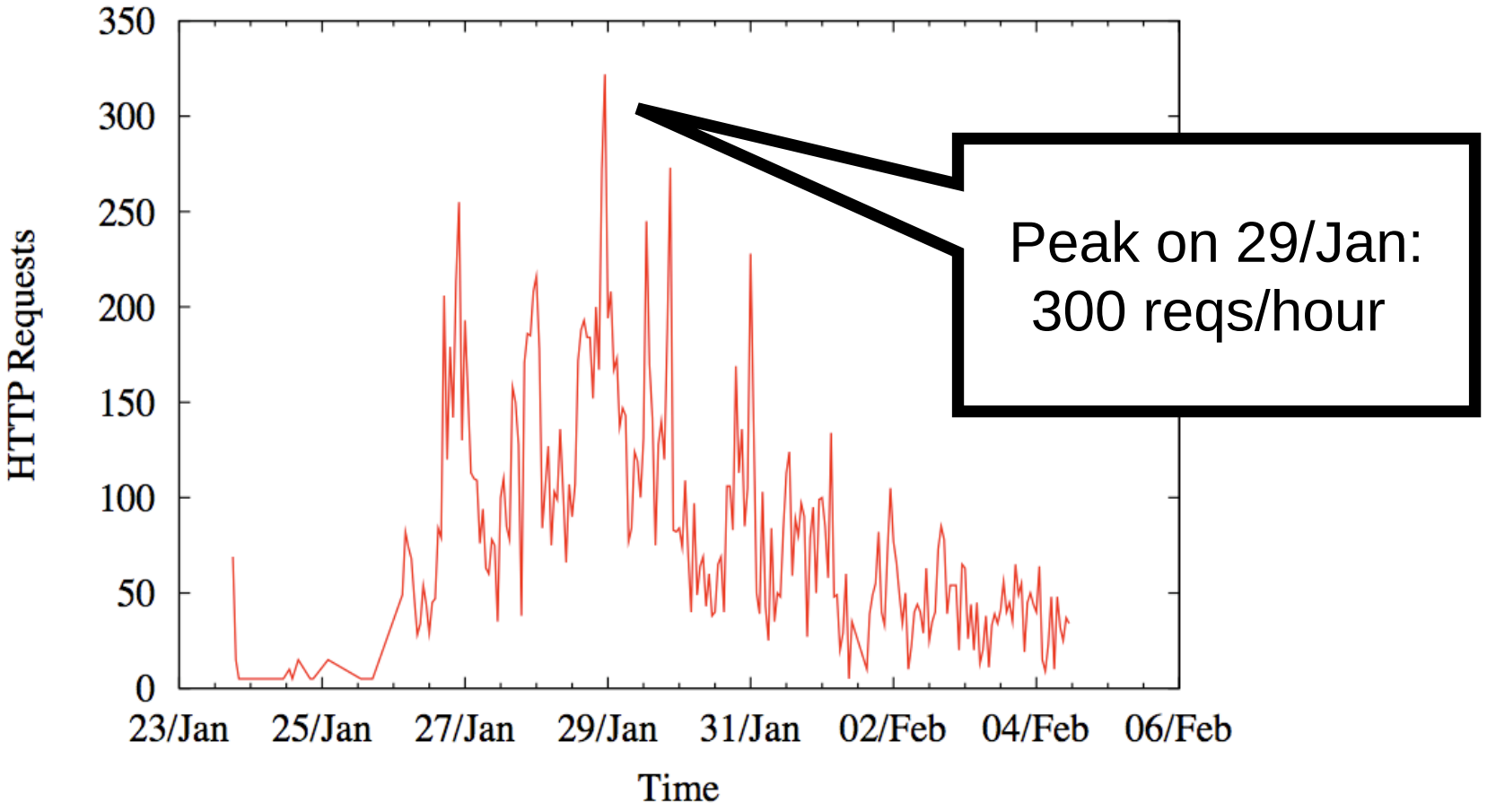
Popularity

Facebook applications are spreading

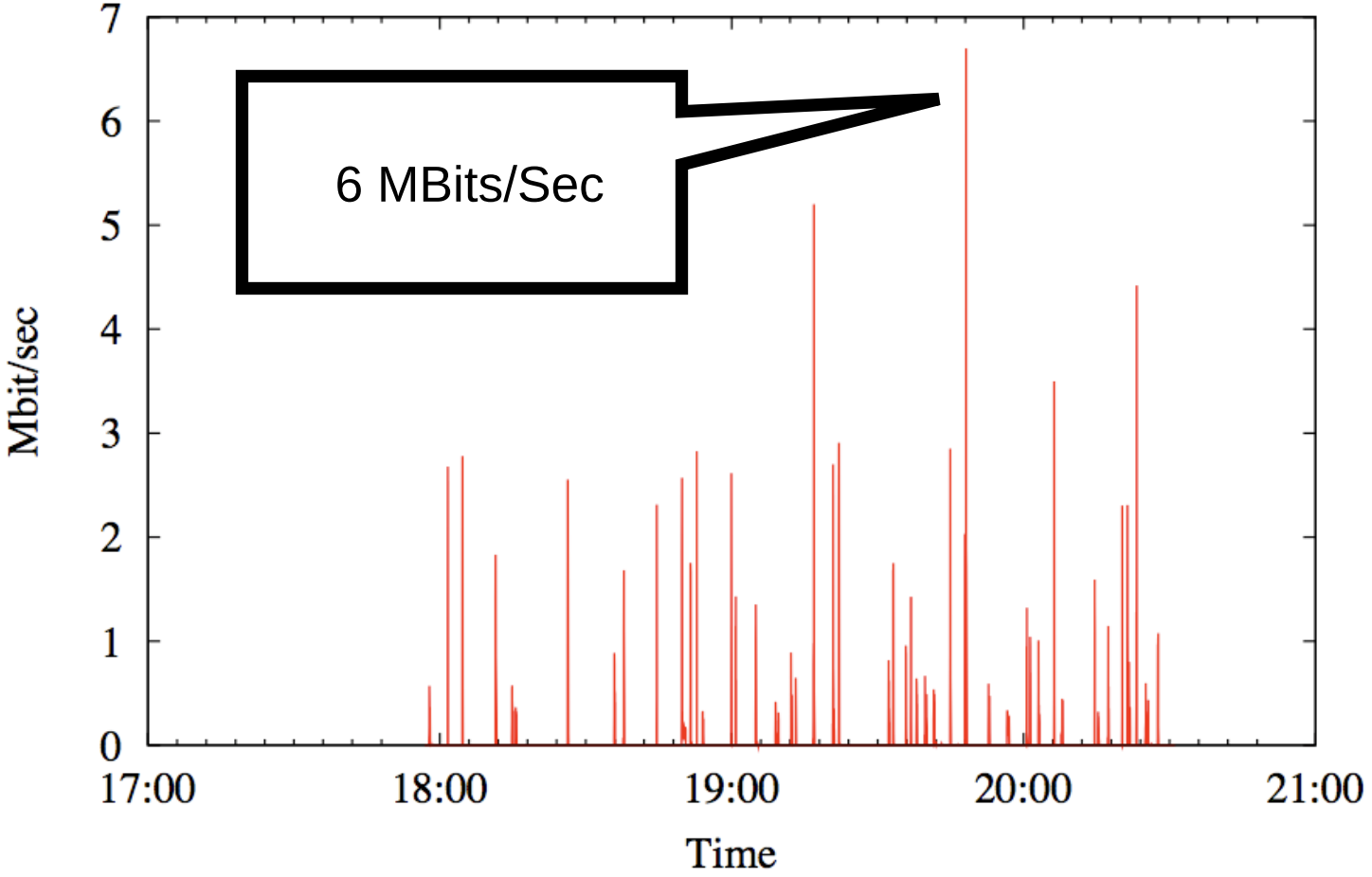
faster

than ordinary software

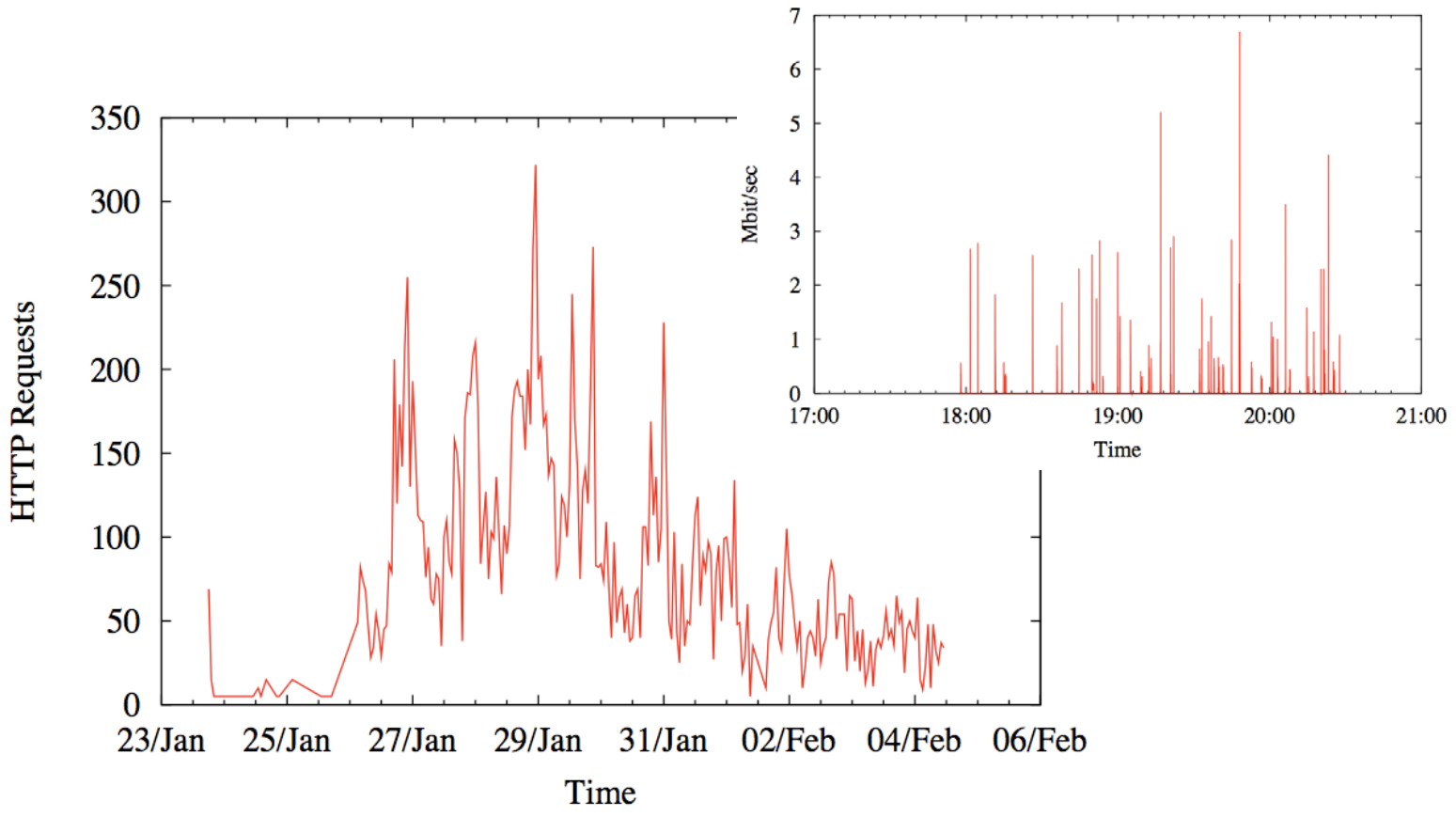
Requests/Hour



29th/Jan Exported Traffic



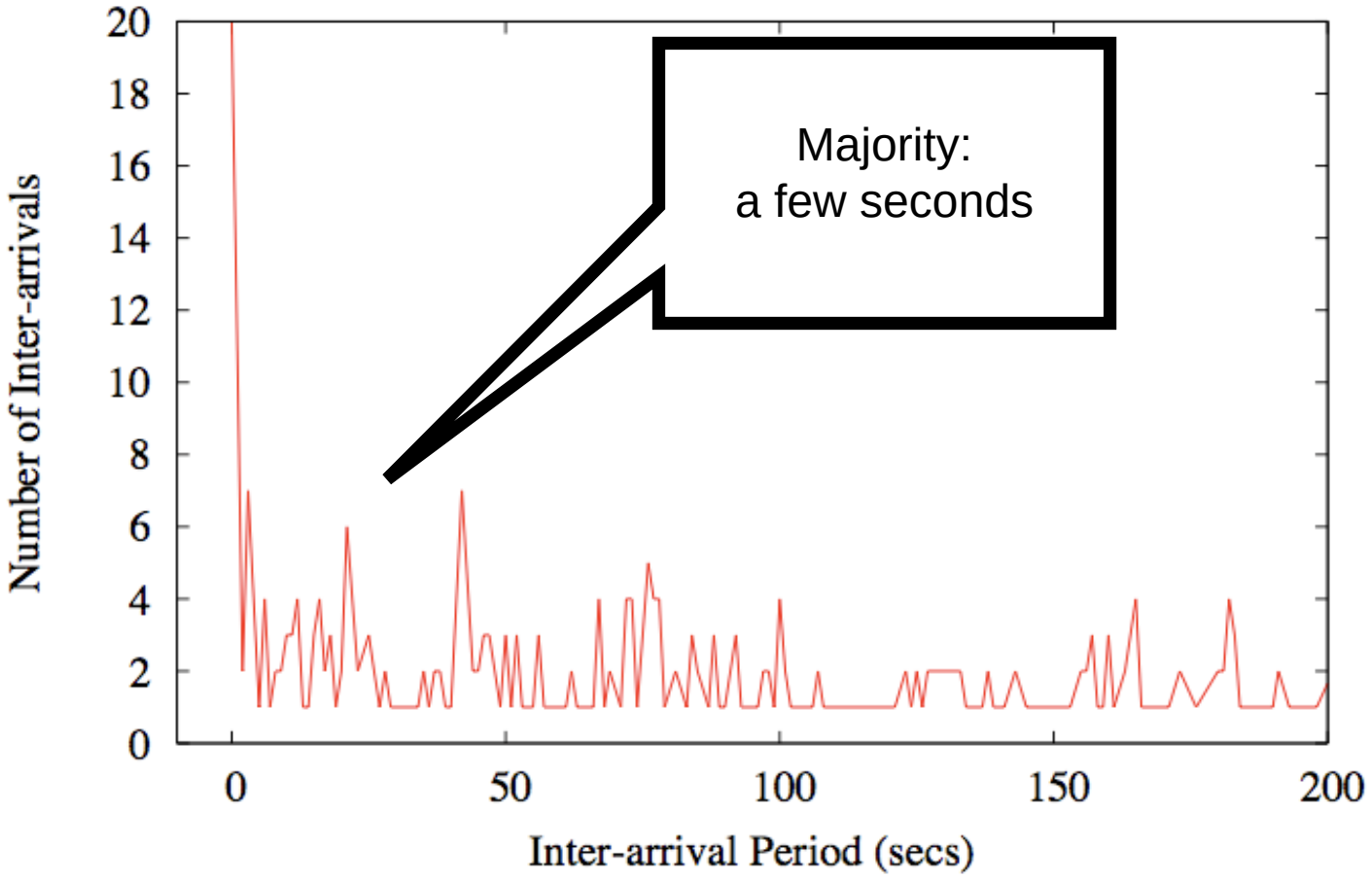
Burst Fashion



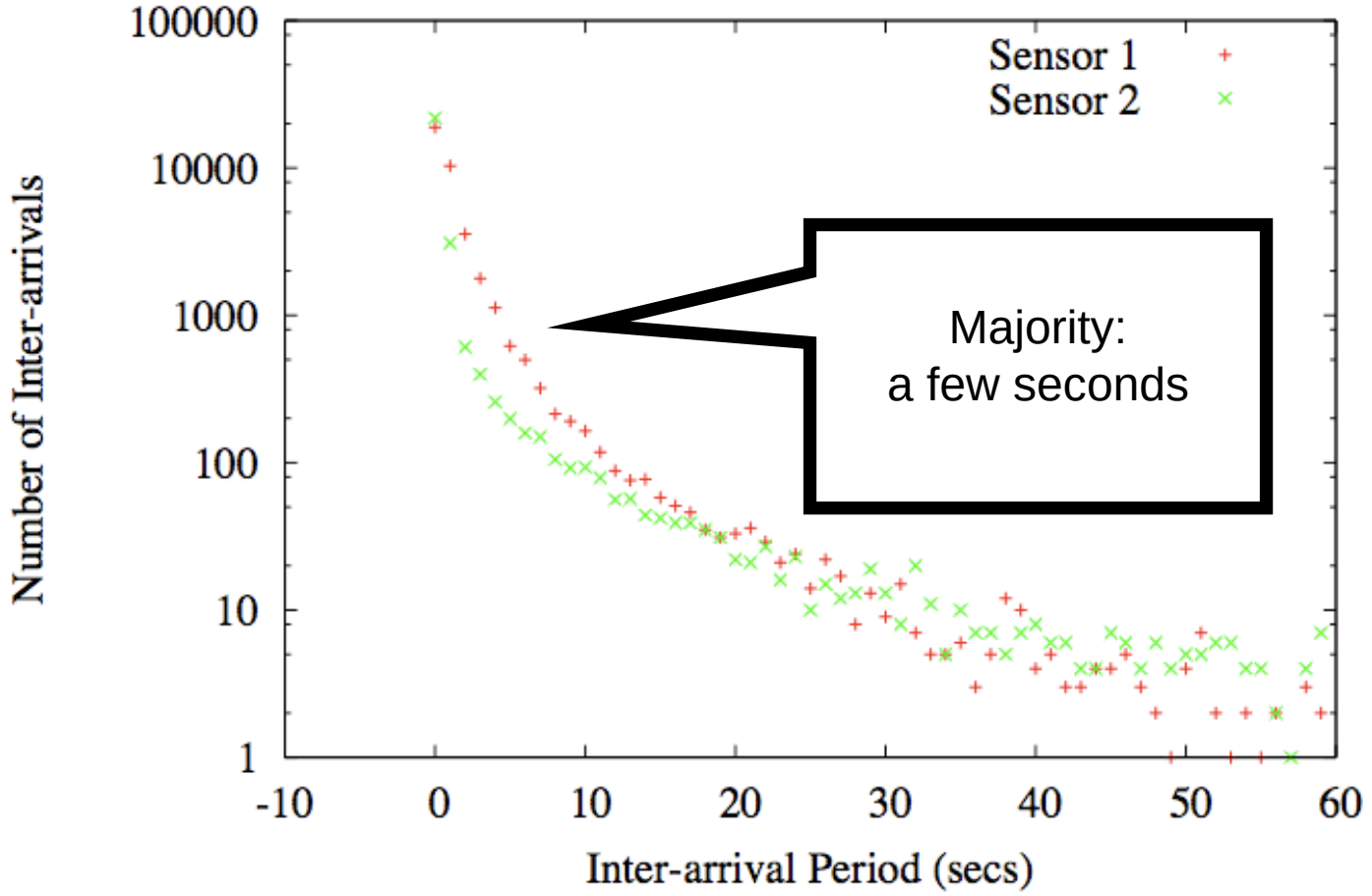
Social == Bursty?

- Web logs from victim
  - User inter-arrivals. How frequently users are visiting the application?
- Traces from two Sensors (Europe, Asia)
  - User inter-arrivals. How frequently users are visiting Facebook.com
  - How long do they stay in Facebook?

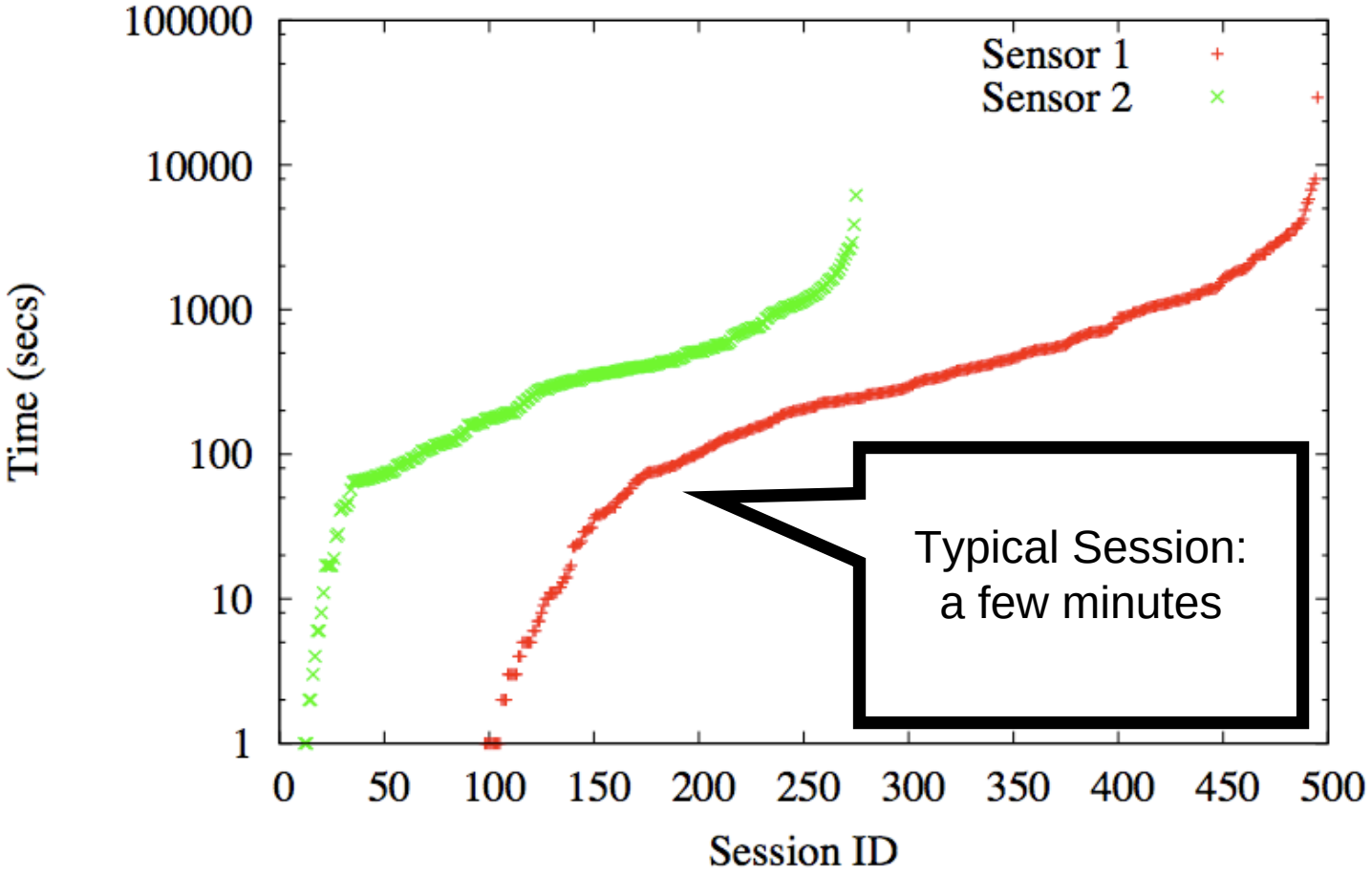
User Inter-arrivals 29th/Jan



User Inter-arrivals



Session Times



Bursty == Social

- Most users are visiting the social network:
  - Every few seconds
  - For a few minutes
- Facebot leaves in the social network:
  - Inherits the same behaviour
- Facebot exports traffic in a bursty fashion

Geographical Distribution

RoadMap

- FaceB⁉ot Architecture
- Experimental Evaluation
- **Attack Firepower**
- Countermeasures
- Conclusions

How far can we go?

Definitions

- α_{out} : outgoing traffic of a Facebot
- $u(t)$: active users distribution
- u_r : user inter-arrival
- F_T : firepower at time T

Firepower

Active Users

App Fan Out

$$F_T = a_{out} \frac{\int_0^P u(t)dt}{< u_r >}$$

User inter-arrivals

An Example

- Consider an application installed by 1000 users
- From 1000 users, 100 were active in a period of 10 seconds
- Users have inter-arrival time of 2 secs
- I.e. user rate is 50 users/sec
- Assume α_{out} = 10 Kbit/sec

$F_{(10)}$ = 0.5 Mbit/sec

Popular Applications

Application	Installations	Daily Active Users
FunWall	23,797,800	2,379,780
Top Friends	24,955,200	2,245,970
Super Wall	23,274,800	1,861,980
Movies	15,934,700	1,274,780
Bumper Sticker	7,989,700	1,118,560

(adonomics.com)

The Facebot

- Consider an application with 2 millions of daily active users
- Assume uniform distribution and inter-arrival time
  - 23 users/sec are using the application
- Assume α_{out} = 1 Mbit/sec
  - Equal to a file request for an image of 125 KBytes

The Facebot

The victim Web server will have
to cope with exported traffic of
23 Mbit/sec

The victim Web server will have
to serve in one day nearly
248 Gbytes

RoadMap

- FaceBot Architecture
- Experimental Evaluation
- Attack Firepower
- **Countermeasures**
- Conclusions

Filtering a FaceBot

- Use IDS/FireWalls to filter out Web requests that have Facebook.com as a referrer
  - However you can hide the referrer field (details in the paper)

Preventing a FaceBot

- Hacks
  - Prevent the usage of `fb:iframe` tags
  - Provide constraint environment (limited Web interaction, limited JavaScript) for Facebook applications

Trade Off: The more secure the less usable

- Invest more peopleware for application auditing

RoadMap

- FaceBot Architecture
- Experimental Evaluation
- Attack Firepower
- Countermeasures
- **Conclusions**

Conclusions

- We developed a PoC FaceBot
  - A Facebook application that performs requests to a victim Web server
- Social networks are ideal for a FaceBot
  - Applications gain popularity fast
  - Users visit social networks in a bursty fashion
  - Social networks have a huge (millions) user base
- A popular application can be misused
  - Mbits/sec
  - GigaBytes of daily unwanted traffic

Road to Publicity

- **30/Aug**
  - Article in NewScientist
- **4/Sept**
  - Request for an interview in Technology Review (MIT)
- **5/Sept**
  - Contact from IDG News, UK (ComputerWorld, PC World, etc)
  - ZDNet is publishing a related article
  - We are in Wired
  - We are becoming Slashdotted
- **6/Sept - Now**
  - We are practically everywhere…

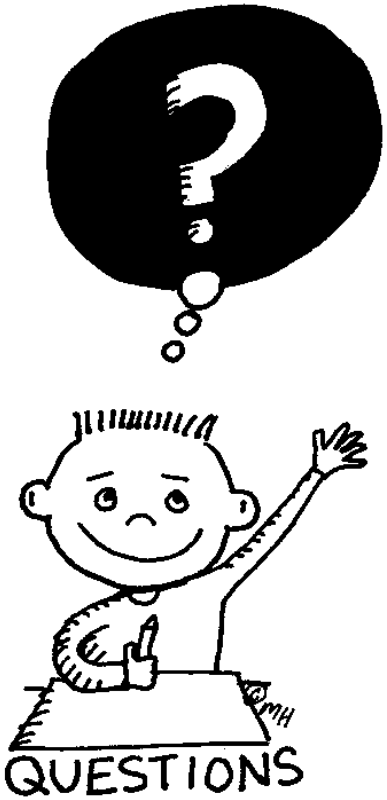
ISC 2008
INFORMATION SECURITY CONFERENCE

Using Media as a Title Generator

- NewScientist
  - Facebook application turns users into attackers
- ZDNet
  - DDoS + Web 2.0 == Buckets o' traffic
- Yahoo News
  - Facebook botnet risk revealed
- Slashdot
  - Researchers Build Malicious Facebook App
- Wired
  - Researchers Use Facebook App to Create Zombie Army

RIP Photo of the Day

多謝



Backup

How Hard is Getting 2M Users?

- Create plenty of less popular ones
  - 100 apps of 1,000 users is 100,000 user base
- Compromise an already popular one
  - Hard to do, but maybe easier than compromising a popular Web site
- Social Phishing
  - Create a fake application that resembles one popular one

ISC 2008
INFORMATION SECURITY CONFERENCE

Is the App Host also Attacked?

- There a plenty of optimized solutions for hosting a Facebook application
  - Joyent Facebook Accelerator
- Provide your own hosting
  - One request to your application is translated to multiple requests towards the victim
  - Add a JavaScript loop to create infinite requests towards the victim

It's not only about DDoS!

- Unsolicited Web requests brake statistics
  - Nobody wants auto generated requests by scripts
- Port Scanning
  - Use Web 2.0 technologies for port scanning
- Malware propagation, XSS Attacks
  - Users trust applications, because they trust the social network
  - They are more likely to get convinced for doing something