RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

Evaluating Attack Amplification in Online Social Networks

Blase E. Ur and Vinod Ganapathy

blaseur@rci.rutgers.edu , vinodg@cs.rutgers.edu

Rutgers University

Online Social Networks

- facebook
  - 200 million monthly unique visitors
  - Founded in 2004
- myspace.com
  - 126 million monthly unique visitors
  - Founded in 2003
- flickr™
  - 64 million monthly unique visitors
  - Founded in 2004

Hubs Exists in Social Networks

- Hubs- very popular users
  - Large number of friends
  - Large number of page views
- Average MySpace user has 200 friends
- MySpace Hubs include celebrities, musicians
  - Rihanna: 1,600,000 friends, 85,000,000 views
  - Tila Tequila: 3,700,000 friends, 184,000,000 views

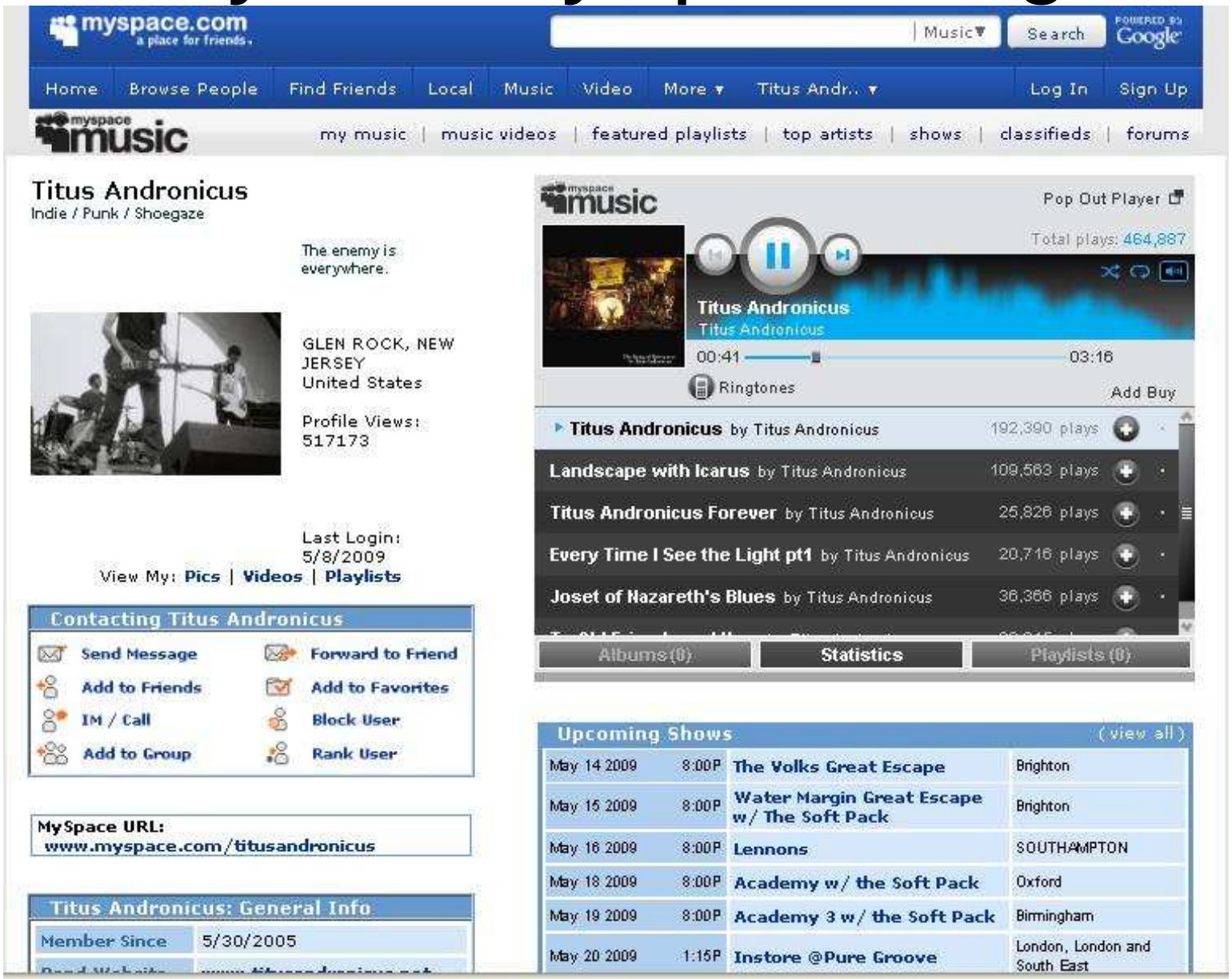
Hubs Enable Attack Amplification

- Attack Amplification: increasing the effects of an attack by coercing a large number of Web users to unwittingly join in
- Hubs are treated the same as ordinary users
- By posting on hubs' pages, ordinary users can amplify attacks
- This threat should be stopped by Social Networks

Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

Anatomy of a MySpace Page



Comments Allow HTML

HTML

Outline

- Motivation
- Background on Social Networks
- Attack Description
  - Denial of Service
  - Botnet Command & Control
- Evaluation
- Remediation

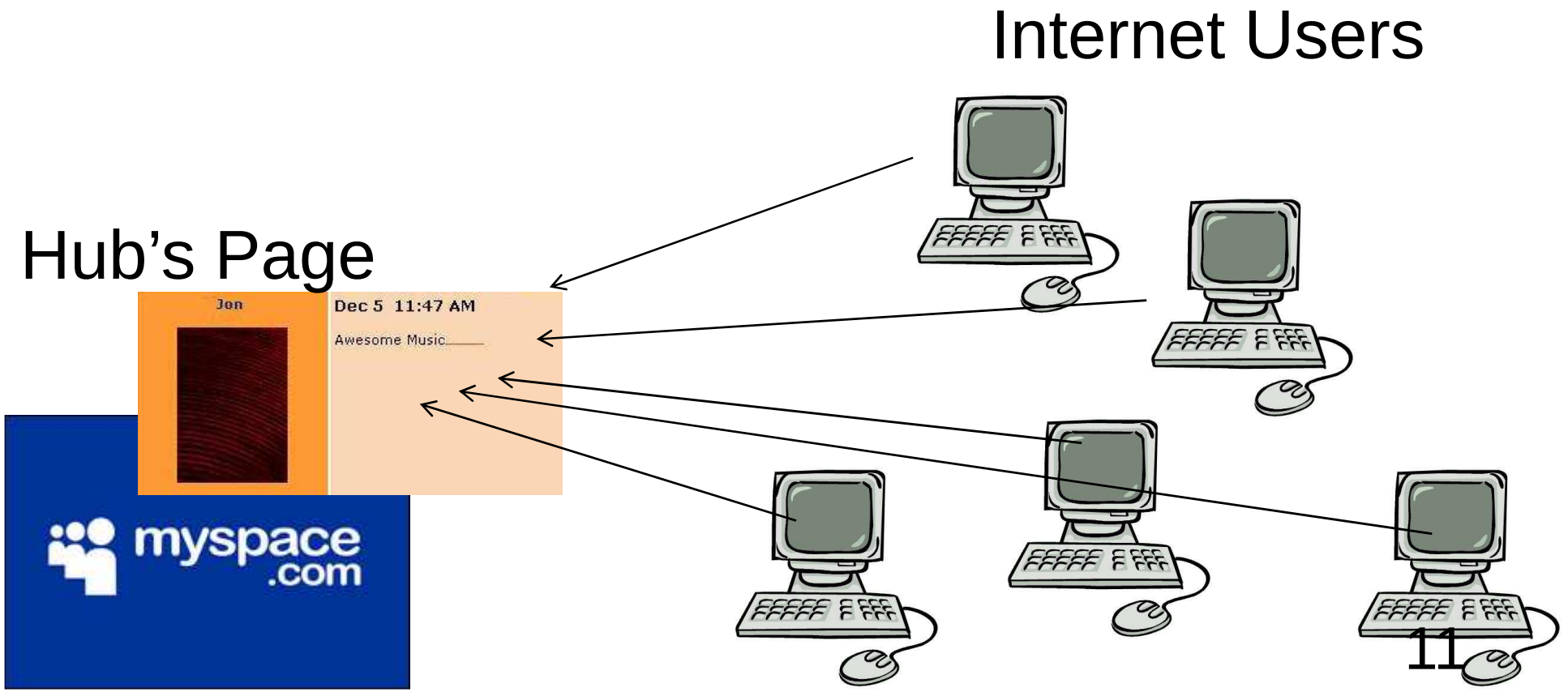
DoS Attack

Hub's Page

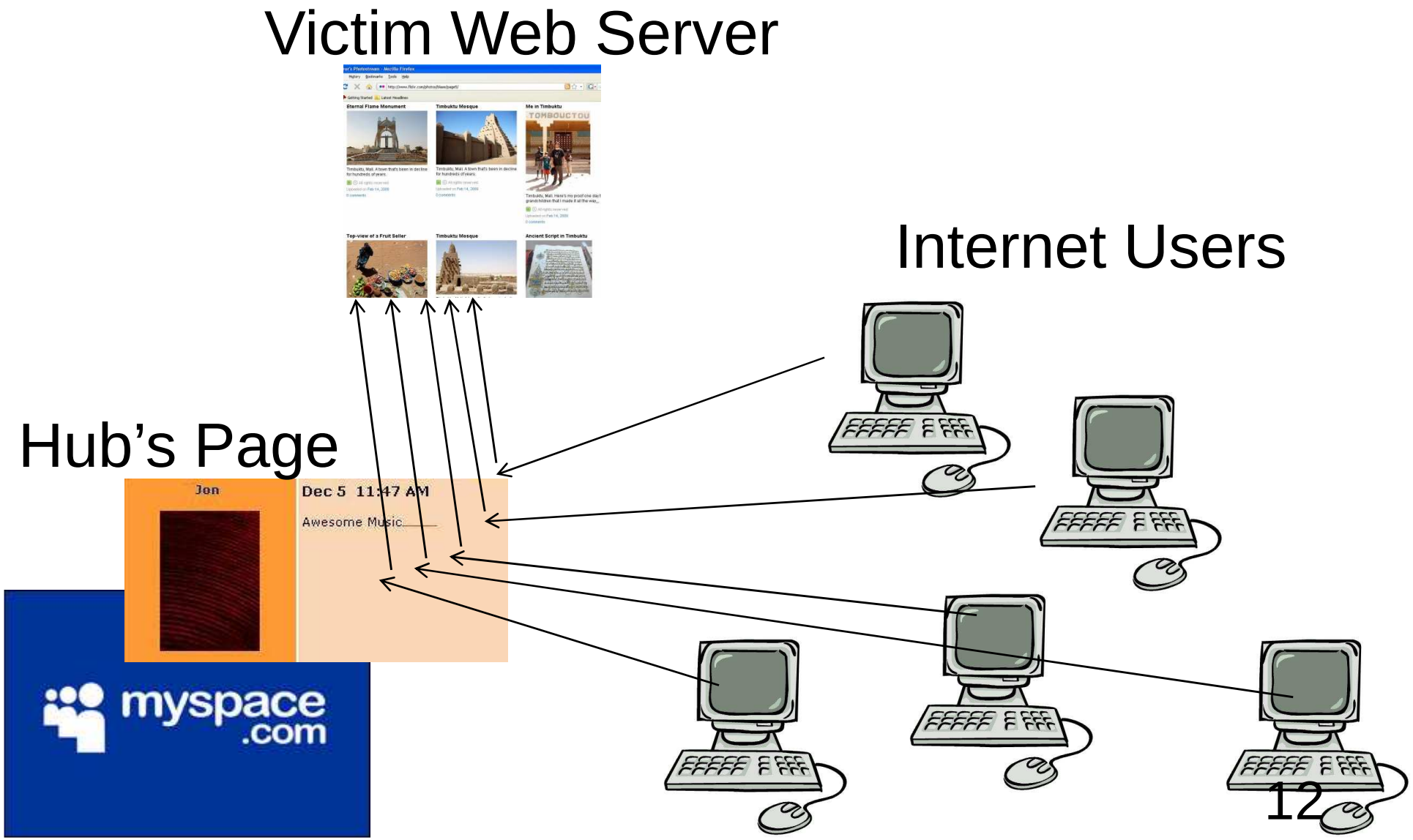
DoS Attack

Hub

DoS Attack

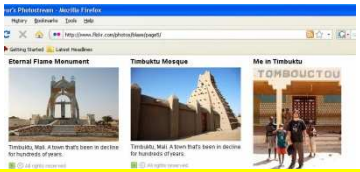

Internet Users
Hub's Page
Jon
Dec 5 11:47 AM
Awesome Music
myspace
.com

DoS Attack


Victim Web Server
Internet Users
Hub's Page
Jon
Dec 5 11:47 AM
Awesome Music
myspace
.com

DoS Attack

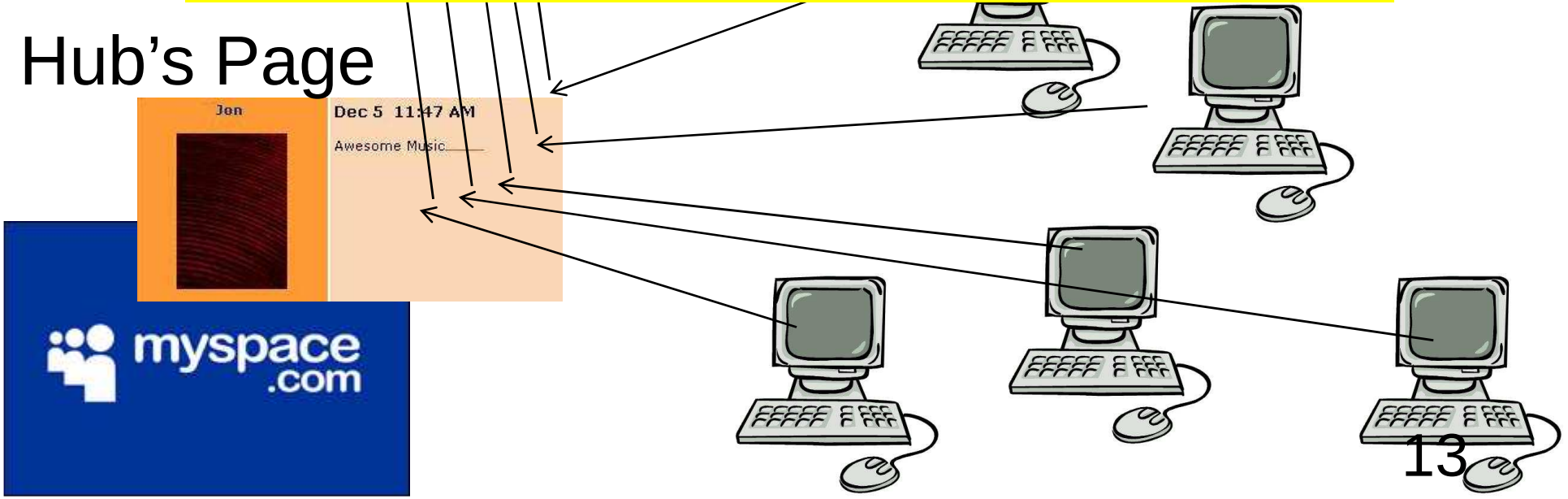
Victim Web Server



Can be launched
by an arbitrary Web user

s

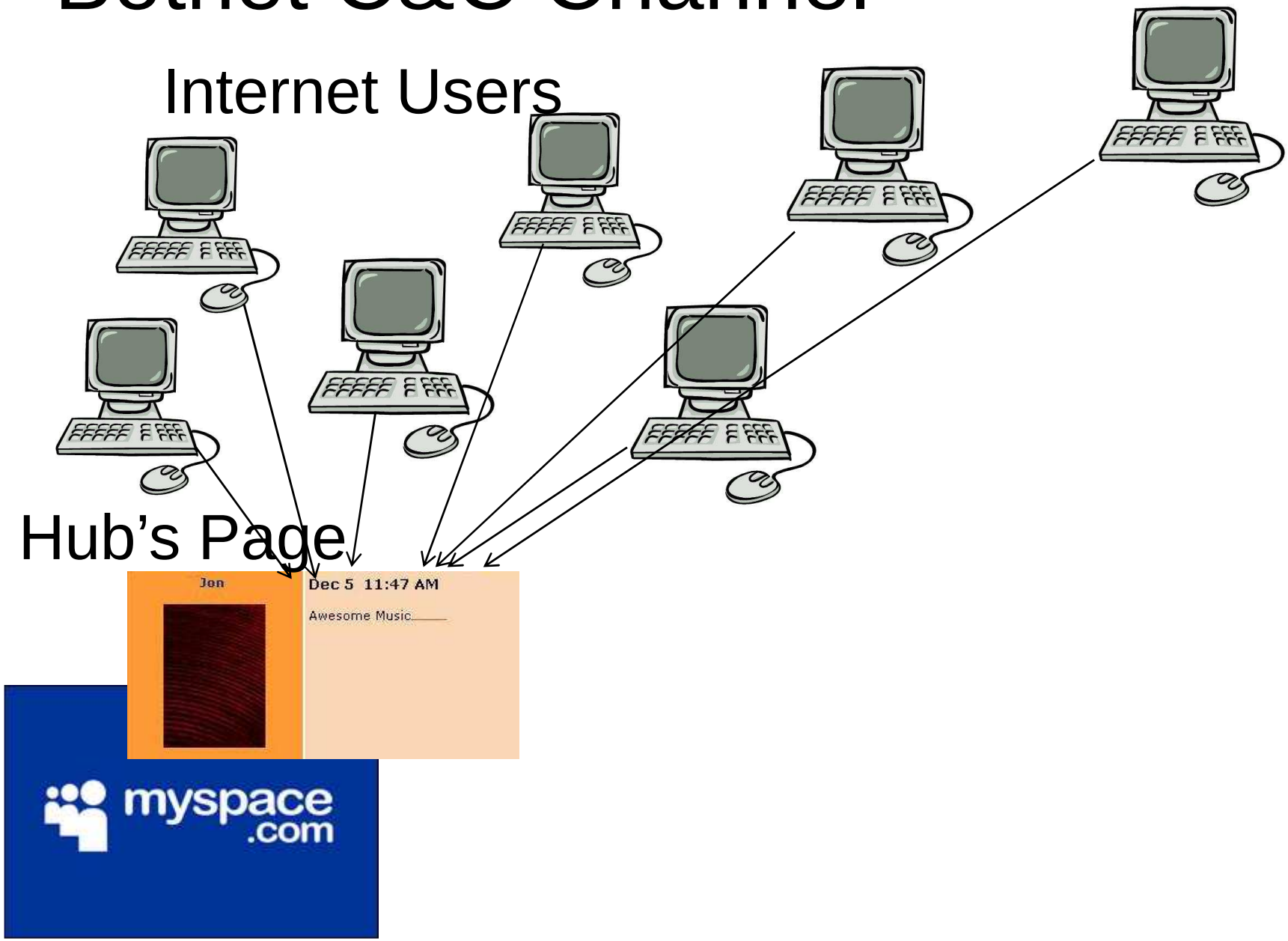
Hub's Page



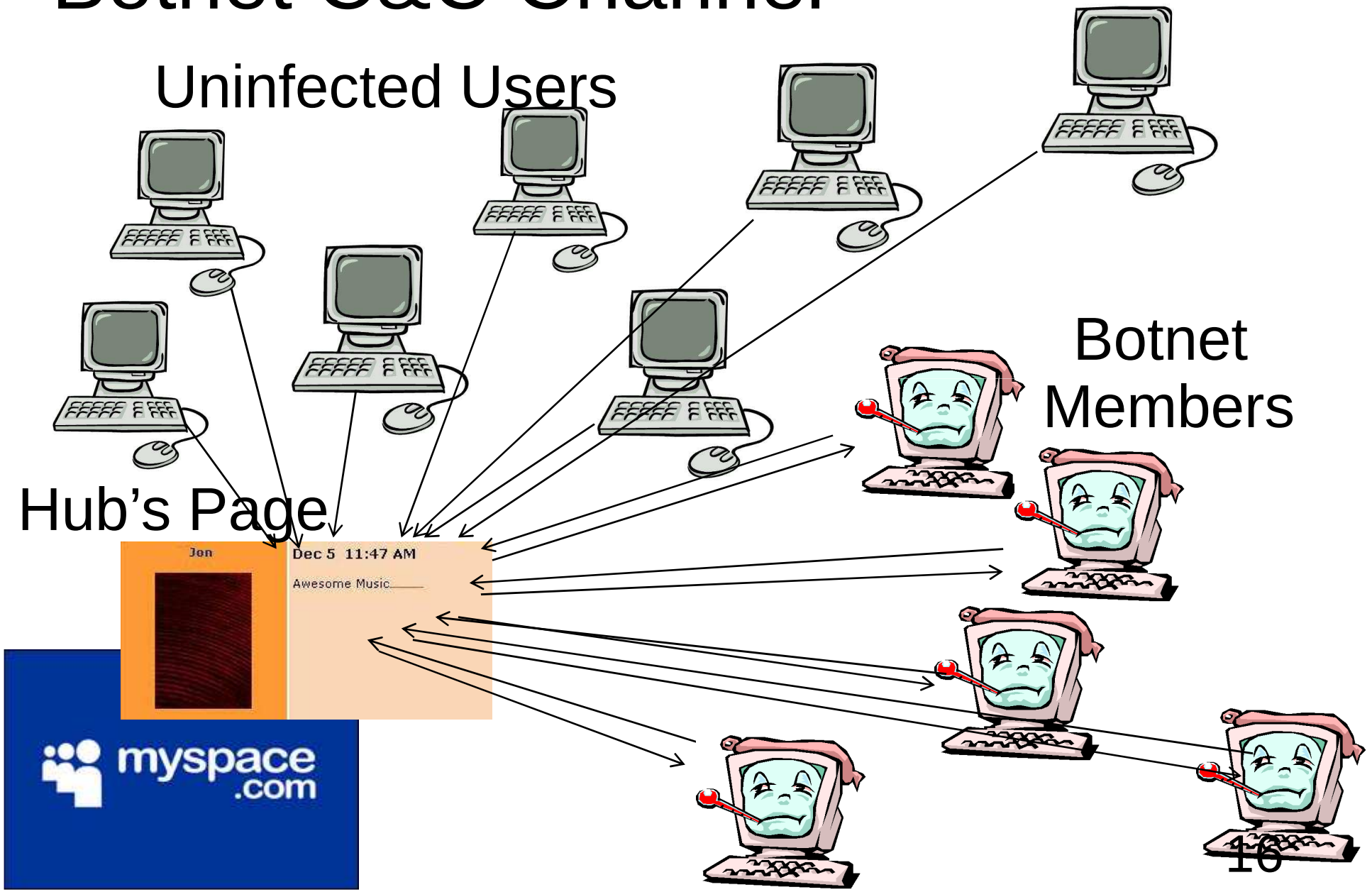
Botnet C&C Channel

Hub’s Page

Botnet C&C Channel



Botnet C&C Channel

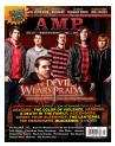


Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

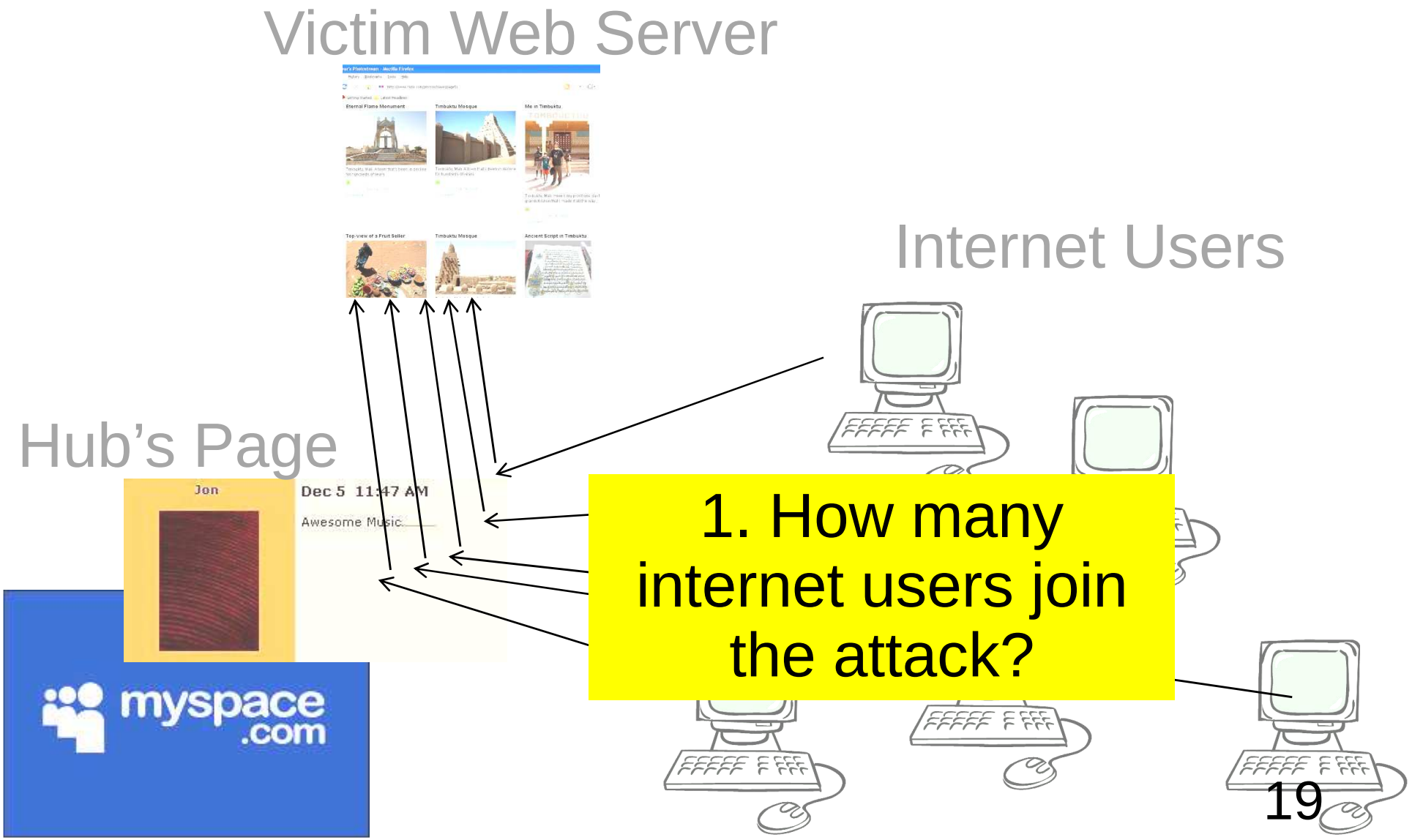
Methodology

Today's Top Artists

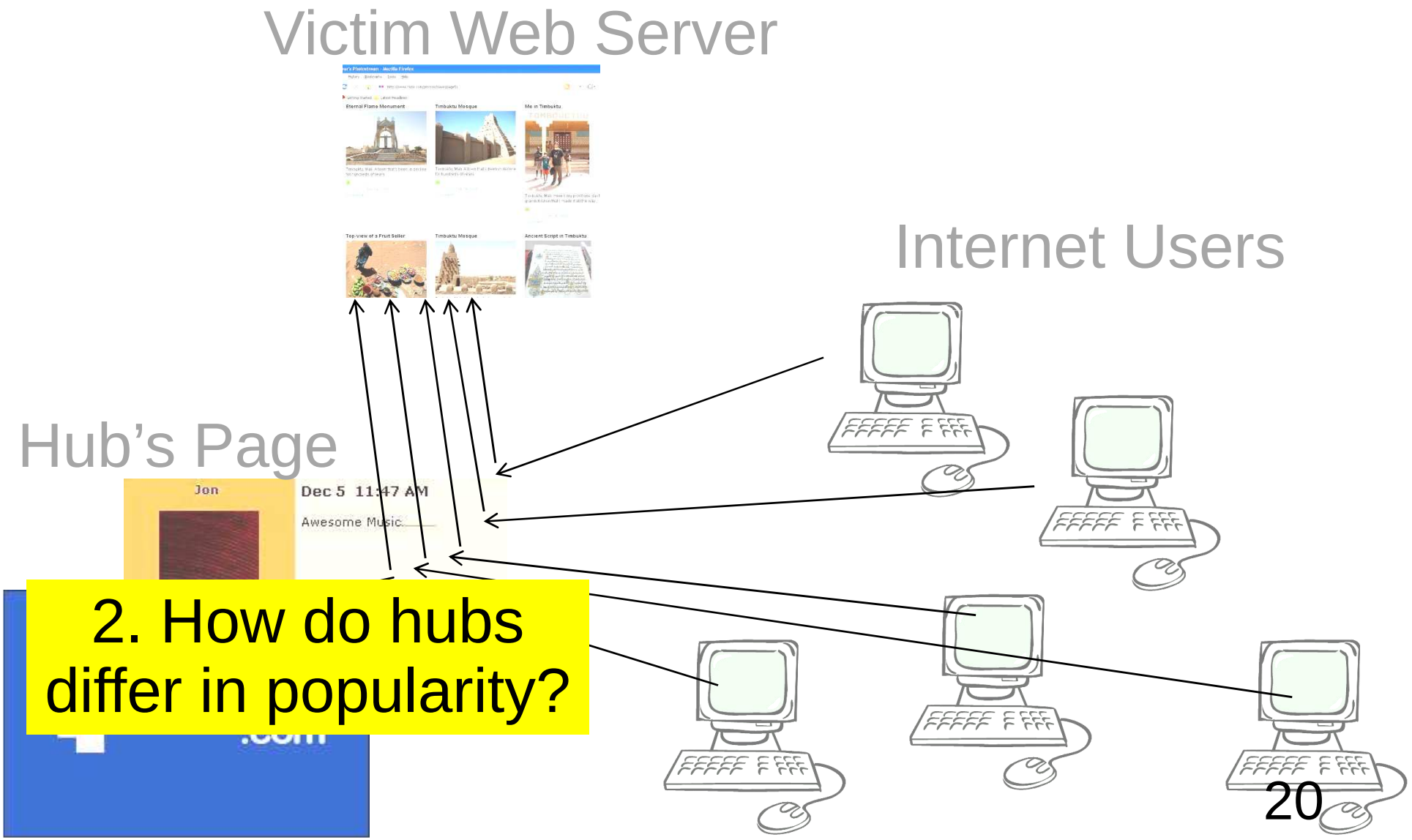
	Unsigned	Indie	Major
1	 **Never Shout Never (anotha n...** Joplin Lounge	 **3OH!3 (is on the 2009 AP TOUR)** BOULDER, Colorado Rock / Electronica / Thrash	 **Beyonce** NEW YORK, New York R&B / Hip Hop / Pop
2	 **Arcangel**	 **paramore** Franklin, Tennessee Alternative / Pop / Regional Mexican	 **Taylor Swift** Nashville, Tennessee Country / Acoustic / Folk
3	 **Pitbull** MIAMI, Florida Hip Hop	 **The Devil Wears Prada (NEW ...** Dayton, Ohio Hardcore / Metal / Christian	 **Akon** Atlanta, Georgia Hip Hop / R&B / Pop

- Post comments on MySpace hubs' profiles
- Comments hotlink images from own server
- 1,073 out of 3,000 permitted HTML
- 942 out of 1,073 accepted friend request

DoS Research Questions

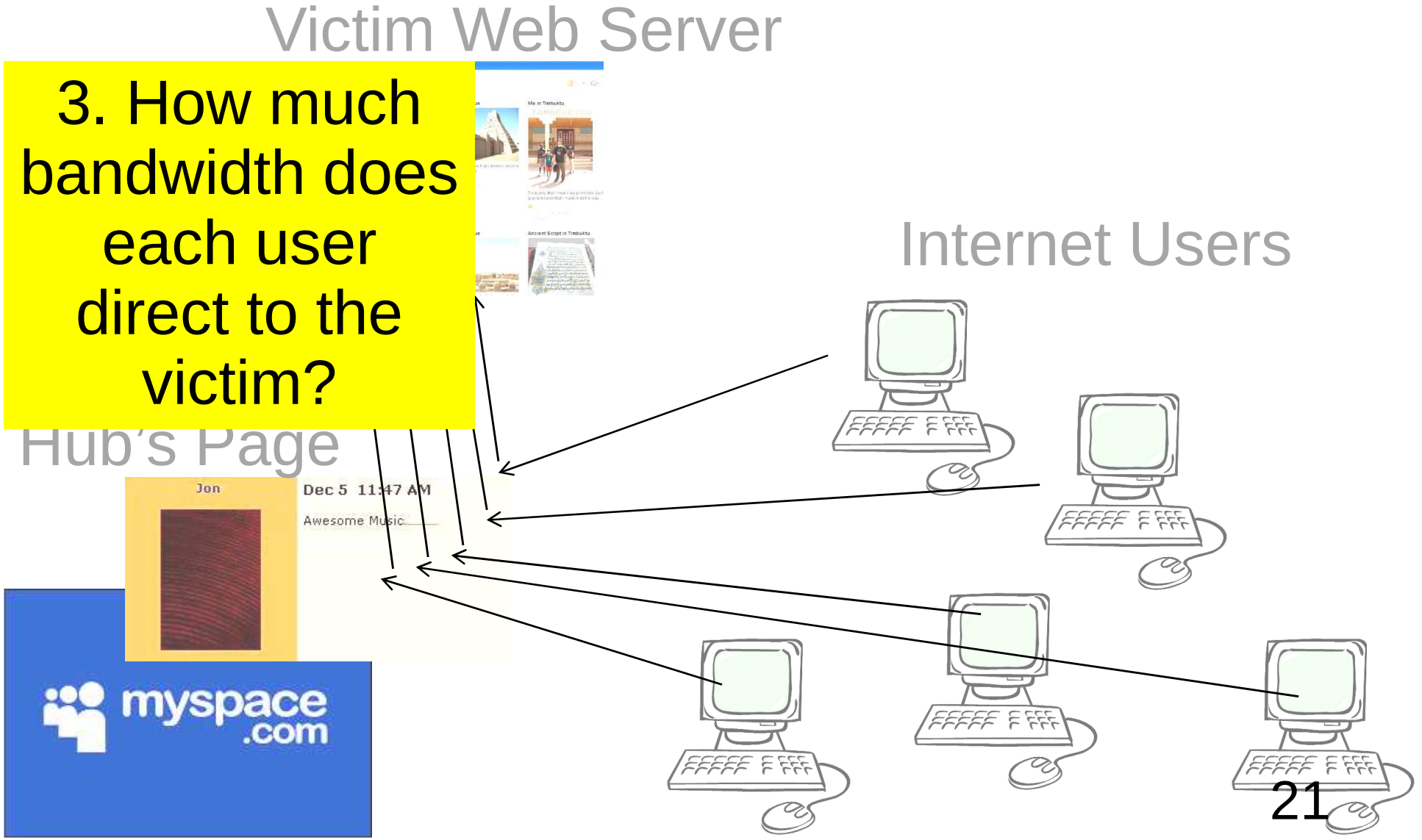


DoS Research Questions



DoS Research Questions

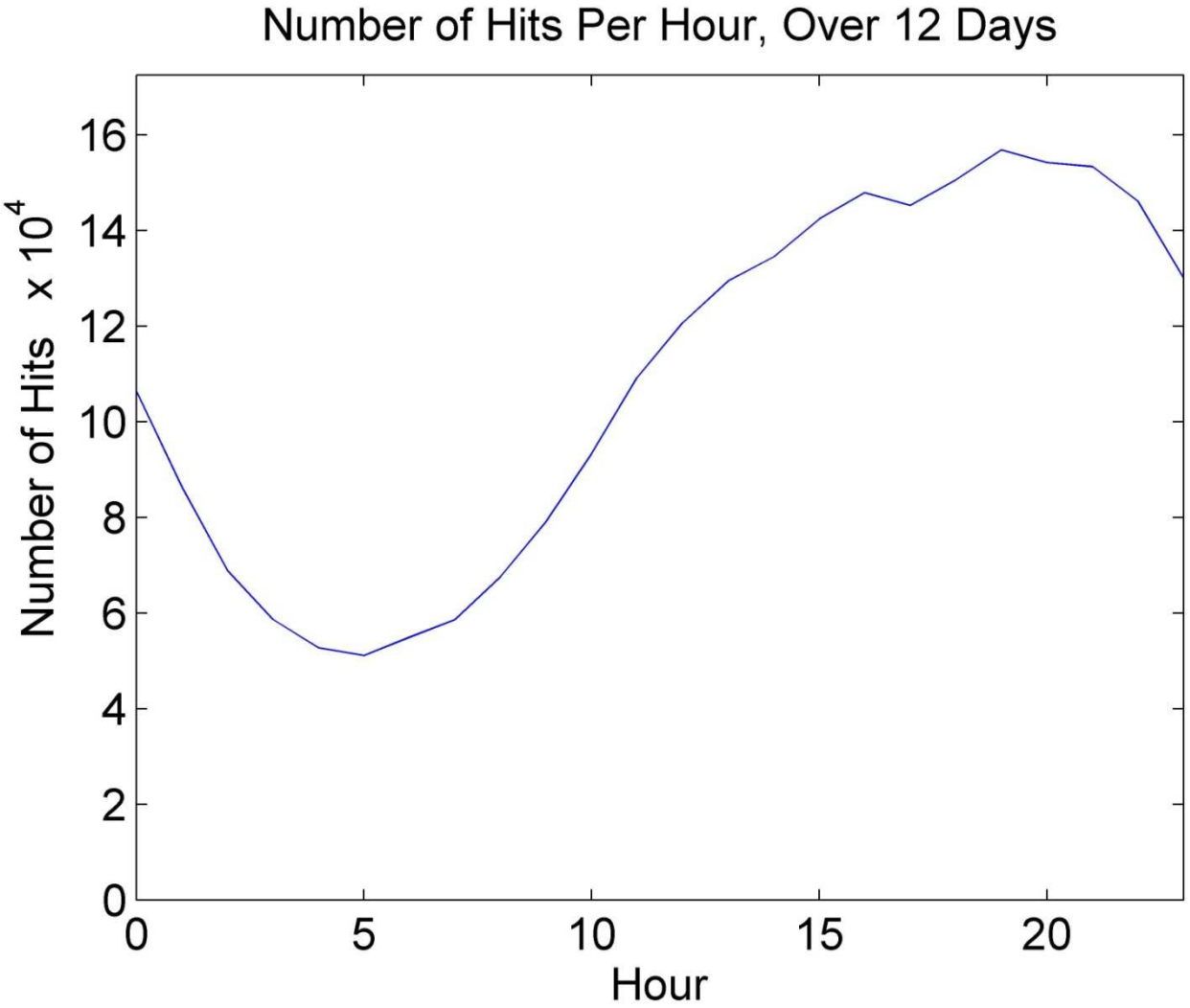
3. How much bandwidth does each user direct to the victim?



DoS- How Many Users

- Goal: How many users will take part?
- Method: Hotlink 1 pixel image, 12 days
- 719 different profiles
- 2,598,692 total hits
- 1,828,589 unique IP addresses

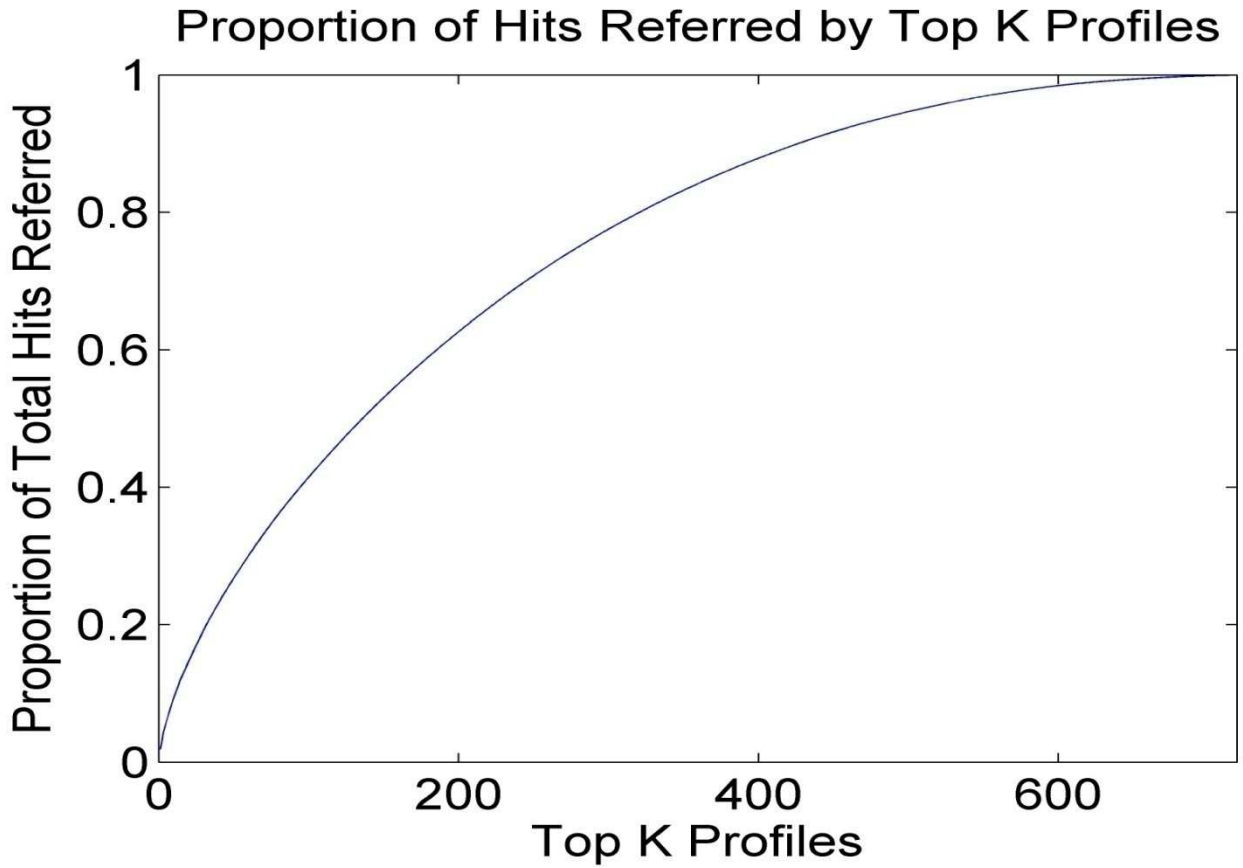
DoS- Diurnal Patterns



- A very large number of users participate

DoS- Hub Popularity

- Goal: How do hubs differ in popularity?



- 1% of the hubs provide 10% of the traffic

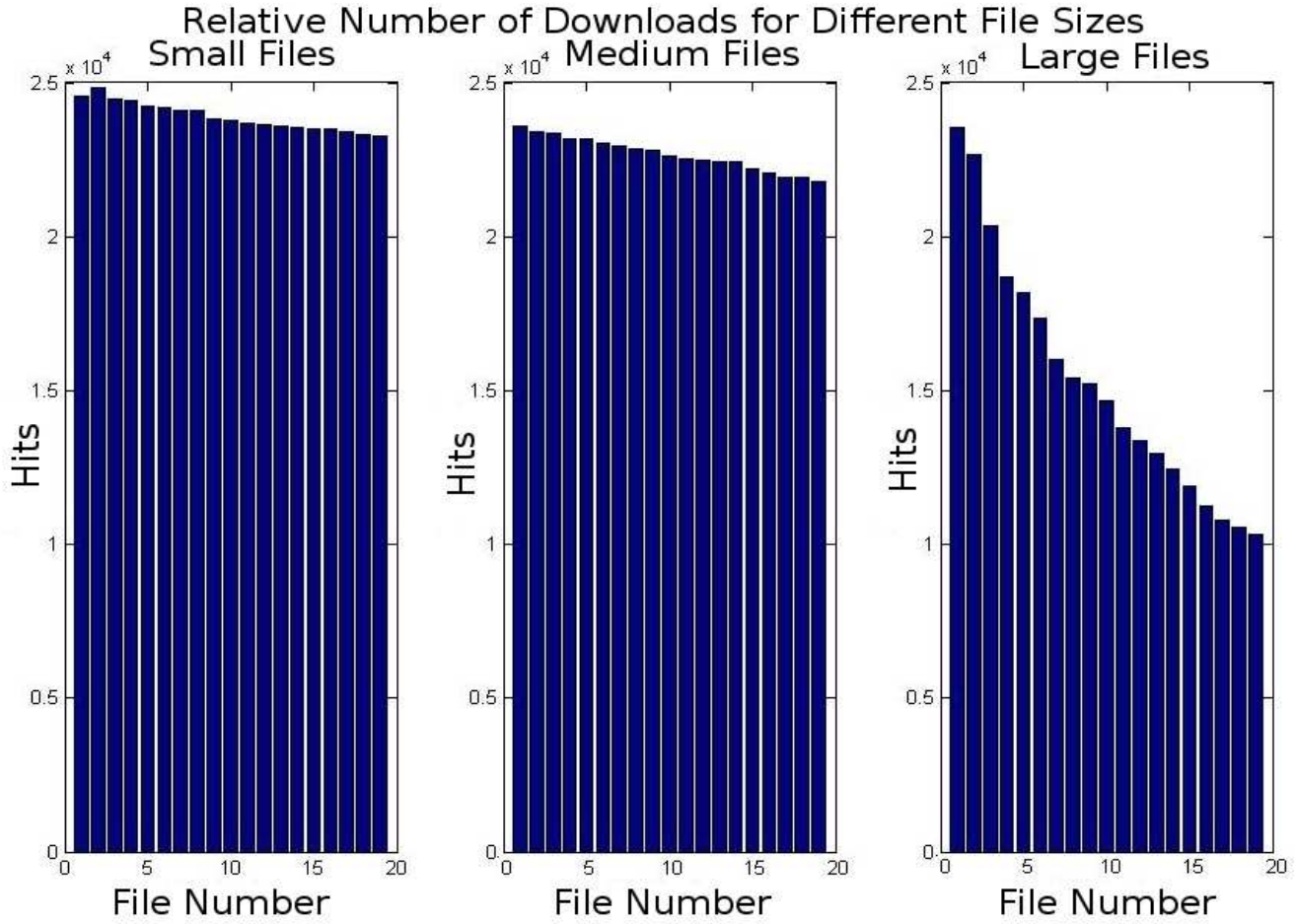
DoS- Total Bandwidth

- Goal: Are users leaving pages and reducing the bandwidth directed to a victim server?

- Total size of all files in comment: 42 MB

- Method: Hotlink 19 small (20 kb),
  19 medium (80 kb), 19 large (2 MB) images

DoS- Total Bandwidth



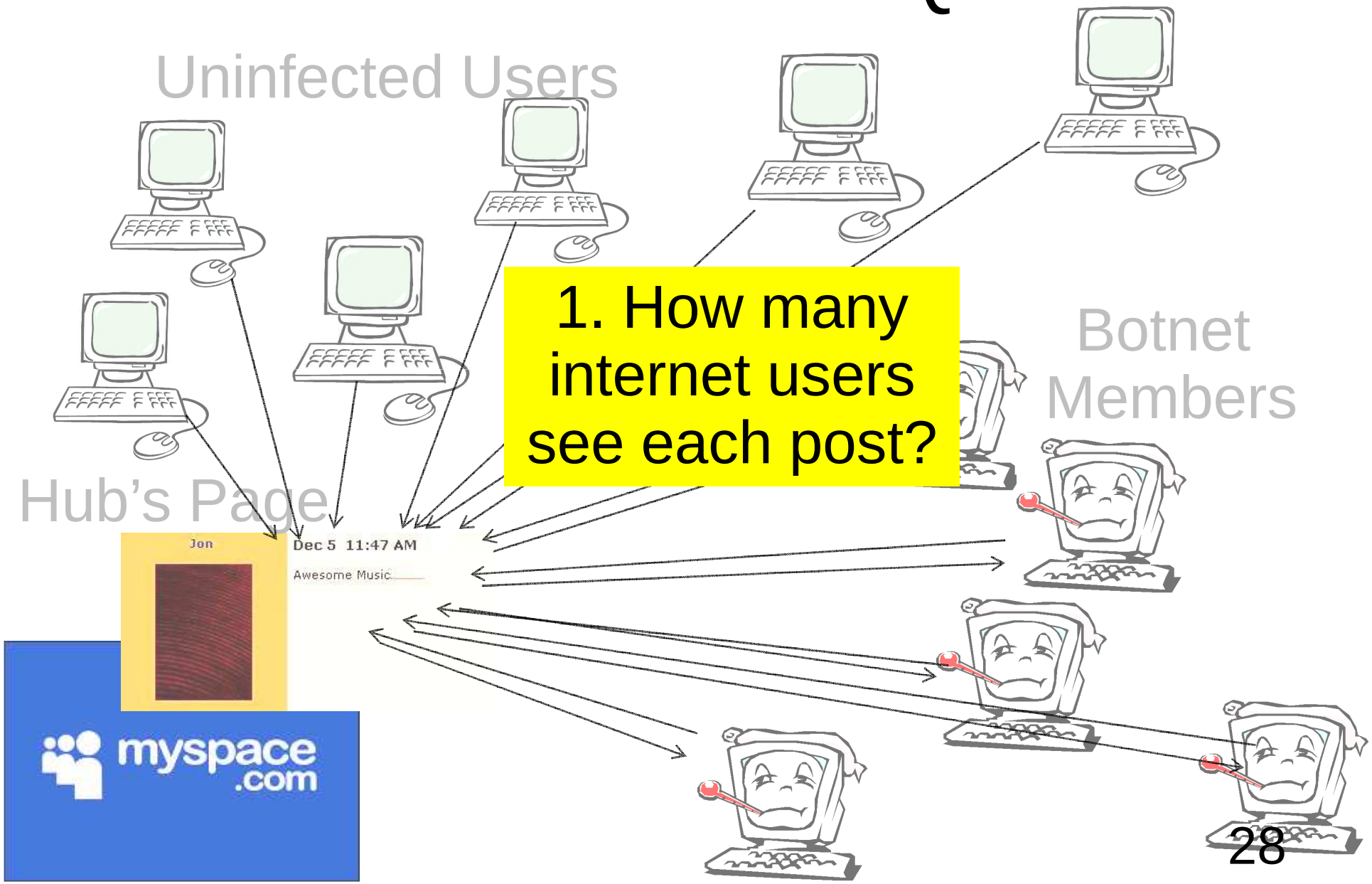
- Users are leaving pages before they load
  - 60% of theoretical efficiency (42 MB)

DoS- Total Estimate

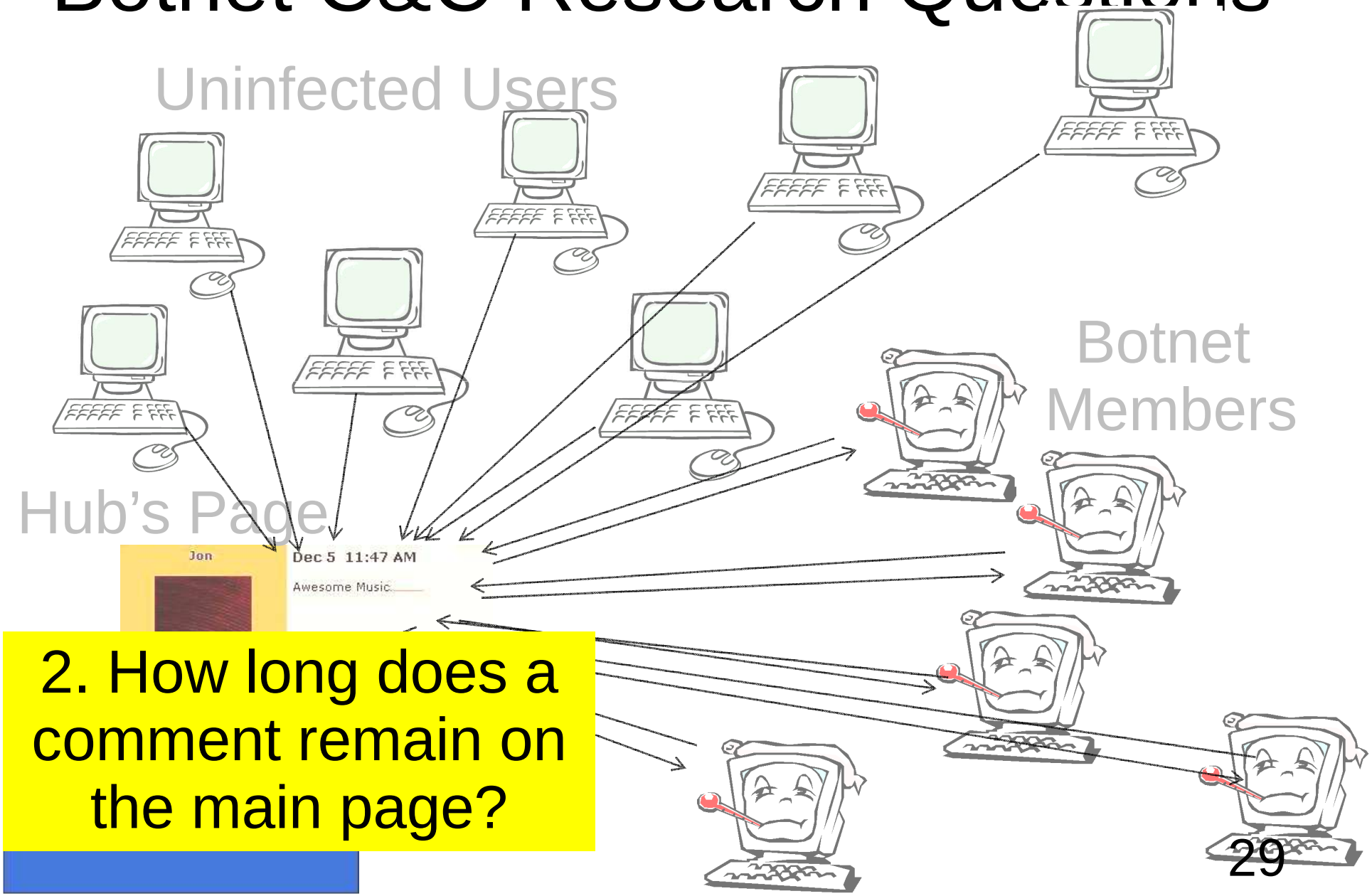
- Hotlink 42 MB on 719 profiles
- 65 Terabytes total (12 days)
- 525 Gigabytes directed toward victim server in the peak hour

- Attackers Can Concentrate on Top 10 Hubs
- Hotlink 42 MB on top 10 profiles
- 6.5 Terabytes total (12 days)
- 52.5 Gigabytes directed toward victim server in the peak hour

Botnet C&C Research Questions



Botnet C&C Research Questions



2. How long does a comment remain on the main page?

C&C- Lifetime of a Comment

- Goal: How long does a comment stay on a page? (Avoid reposting)
- Method: Measure when traffic drops below 10% of maximum from each profile
- Median Lifetime of a comment: 137 hours (5.5 days)
- 10 posts can reach 180,000 unique IP addresses over a few days

Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

Technique 1- Restrict Hubs

- By default, disallow HTML/media in posts on popular pages
- Why not restrict all HTML use?
  - Freedom / Customization
  - It’s in use and popular
- At what threshold of friends / page views does a user become a hub?

Technique 2- Focused Monitoring

- Amplification attacks require hubs
- Monitor hubs only for suspicious posts

Technique 3- Friend Hierarchy

- Only allow friends of a certain relationship (other musicians) or particular social circle to post

- Friend Lists don’t suffice
  - Huge time investment, few obvious rewards
  - Requires an automated solution

Technique 4- Reputation System

- Only allow posts from users whose previous comments have met some criteria
- Require greater time investment from attacker
- What metrics?
- Can be gamed!

Take-Away Points

•Hubs allow ***arbitrary*** adversaries to ***amplify*** bandwidth-based attacks and the distribution of content

- Just 10 posts by arbitrary user:
  - Reach 180,000 unique IP addresses
  - Can direct 50+ GB of traffic toward a victim server in an hour
- Remediation is necessary at social network
  - Without losing “openness” of network

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

Thank You!

Evaluating Attack Amplification in Online Social Networks

Blase E. Ur and Vinod Ganapathy

blaseur@rci.rutgers.edu , vinodg@cs.rutgers.edu

Rutgers University