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

<table>
<thead>
<tr>
<th>CAPTAIN POLAROID and the Betamax Conspiracy</th>
<th>May 9 2009 6:28 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="CAPTAIN POLAROID and the Betamax Conspiracy" /></td>
<td>Say I was gonna come see you in Birmingham UK but I’m already going to gig that day! Typical! Please come back again...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry Open mic New Broadcasts live on 90.3FM!!</th>
<th>May 8 2009 9:48 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Industry Open mic" /></td>
<td>Hi, we would like to invite to our Open Mic Radio Showcase this Tuesday! And every Tuesday! The last show was the launch and was huge!!! Our open mic was broadcasted on 90.3FM!!! And will be airing now every week! Performers can listen to their performance the very next day on 90.3FM with Friends and Family! This is major exposure! 700,000+ listeners! This Tuesday @ The Karma Lounge First Ave Between 3rd and 4th Street Manhattan NY Artist sign up 6:30PM Show starts 9:30PM Admission only $10 Hope you can make it!</td>
</tr>
</tbody>
</table>

HTML
Outline

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

Hub

Jon

Dec 5  11:47 AM

Awesome Music
DoS Attack

Hub’s Page

Internet Users
DoS Attack

Victim Web Server

Hub’s Page

Internet Users
DoS Attack

Victim Web Server

Can be launched by an arbitrary Web user

Hub’s Page

Internet Users
Botnet C&C Channel

Hub’s Page
Botnet C&C Channel

Internet Users

Hub’s Page

myspace.com
Botnet C&C Channel

Uninfected Users

Hub’s Page

Botnet Members
Outline

• Motivation
• Background on Social Networks
• Attack Description
• Evaluation
• Remediation
Methodology

- 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

1. How many internet users join the attack?
DoS Research Questions

2. How do hubs differ in popularity?
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

1. How many internet users see each post?
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
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