Talkback: Reclaiming the Blogosphere

Elie Bursztein, Baptiste Gourdin, John Mitchell
Stanford University & LSV-ENS Cachan
What is a blog?

- A Blog ("Web log") is a site, usually maintained by an individual with
  - Regular entries
  - Commentary
  - LinkBack
- Entries displayed in reverse-chronological order.

http://elie.im/blog
Key Statistics

- 184 Millions blogs
- 73% of users read blogs
- 50% post comments
Anatomy of a blog post

1. Title
   - New MailChimp Logo By Jon Hicks

2. Permalink

3. Body / Content
   - This post has absolutely nothing to do with email marketing. But if you're interested in graphic design and branding, you might enjoy.
   - I've been wanting to redesign the MailChimp first designed in 2001. I kinda hacked the logo together really fast in Fireworks (which is just not meant for high-res print). I think it went something like this. Mark, my co-founder, said: "Yo Ben, MailChimp's logo now. Um, I think it could be a logo." My 10th amp. Here's the sketch.

4. Publish Date
   - September 11, 2008 at 4:49 am

5. Category
   - MailChimp News

6. Summary / Excerpt
   - The story behind MailChimp's new branding, including sketches from Jon Hicks

7. Author
   - Ben
Why blogs are special?
Why blogs are special?
What is a TrackBack?
1. "Wow! Jimmy Lightning has written the best post ever! It's so funny! And it's true! That's why it's so good. I need to tell the world!"
2. "Check it out world! I've written all about Jimmy Lightning's post on my weblog. My weblog's called 'The Unbloggable Blogness of Blogging'. It's a good name huh? Wow, I sure hope Jimmy sees what I said about him..."
3. "Hey! I wonder what happens when I click on that Trackback link at the bottom of Jimmy's post?"

"Far out! In that funny pop-up is a link back to my site! Too cool for school!"
Why the LinkBack problem is different?
Why the LinkBack problem is different?

- A single spam can reach thousand of users
Why the LinkBack problem is different?

- A single spam can reach thousand of users
- LinkBack notification are automated
30 million LinkBack spam by day
Spam Campaign example

Trackback Spams

Number of Spams

0 25000 50000 75000 100000

Spam Campaign example
Dec 20, 2006

The Day The Trackbacks Died

You might read a post on this blog and decide I feel this way. And, while you’re at it, feel free to public dialog is why I believe so strongly in comment.

But sometimes a mere comment isn't enough. I write an entire post on your blog explaining, in person, that I, the target of your vitriol, have a little too intimate. Or, you could leave a comment.
The end of all hope?
Have Trackbacks Become Too Spammy To Be Worthwhile?

You may have also discovered a surge in trackback spam recently as autoblogging software is being used by more and more spammers to reach out and cull RSS feeds. This phenomenon has led to many disabling trackbacks, or raising the “blacklist” level so high that you might never see some trackbacks again. Or, as some newer remotely-hosted commenting technologies like IntenseDebate and Disqus show, they simply do not show trackbacks because of the spam problem.
Adversary Model

- Resourceful
- Efficient
- Knowledgable
- Adaptive
Threat

- Blog spoofing
- Cried Wolf attack
- Linkback tampering and replay
- Spam in breath or in deapth
## Current Linkback specifications

<table>
<thead>
<tr>
<th></th>
<th>RefBack</th>
<th>PingBack</th>
<th>TrackBack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Mechanism</td>
<td>Visit from the sender site</td>
<td>Code executed at posting time</td>
<td>Code executed at posting time</td>
</tr>
<tr>
<td>Notification medium</td>
<td>HTTP referer</td>
<td>XML-RPC call</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Information sent</td>
<td>none</td>
<td>- $S$ post URL</td>
<td>- $S$ post URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- $R$ post URL</td>
<td>- $S$ site name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- $S$ post title</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- $S$ post excerpt</td>
</tr>
<tr>
<td>Auto-discovery mechanism</td>
<td>none</td>
<td>LINK Tag</td>
<td>Specially formatted info in the body</td>
</tr>
</tbody>
</table>

As shown in the table above, TalkBack is the only LinkBack mechanism that provides authenticity and ensures sender and receiver contacts. It also has been designed to be robust and lightweight, making it easy to implement. This is why we chose it over other mechanisms.
Threats are not addressed by current Linkback specifications
Introducing Talkback!
Use a light-weight PKI to fight Spam
Table 1: Linkback mechanisms comparison

<table>
<thead>
<tr>
<th>Trigger Mechanism</th>
<th>RefBack</th>
<th>PingBack</th>
<th>TrackBack</th>
<th>TalkBack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification medium</td>
<td>HTTP referer</td>
<td>XML-RPC call</td>
<td>HTTP POST</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Information sent</td>
<td>none</td>
<td>- S post URL</td>
<td>- S post URL</td>
<td>- S post URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- R post URL</td>
<td>- S site name</td>
<td>- S site name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- S post title</td>
<td>- S post title</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- S post excerpt</td>
<td>- S post excerpt</td>
</tr>
<tr>
<td>Auto-discovery</td>
<td>none</td>
<td>LINK Tag</td>
<td>Specially formatted information in the body</td>
<td>LINK Tag</td>
</tr>
<tr>
<td>mechanism</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S Authenticity</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>R Authenticity</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Integrity</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
</tbody>
</table>
Talkback Overview

1. Seed request
2. Auto-Discovery
3. TalkBack posting
4. TalkBack reporting
5. Receiver validation
Talkback Security Equation
Limited number of blogs
Talkback Security Equation

Limited number of blogs

+ Limited number of LinkBack by blog
Talkback Security Equation

Limited number of blogs

+ Limited number of LinkBack by blog

= Spam under-control
Making blog registration costly

- Captcha
- Email verification
- Domain verification
LinkBack benefits

• Blog
  • Authenticity
  • Whitelisting / blacklisting
• Linkback
  • Integrity
  • Non-repudiable
• Confidentiality (optional)
Reducing authority power

- Can’t forge LinkBack: authorities have only blog public keys
- Respect privacy: authorities don’t see LinkBack content in secure mode
- No single point of failure/control: protocol allows blog to choose the authority of their choice.
Implementation

- Open-source library
- Wordpress plugin
- Authority: https://talkback.stanford.edu
Elie Bursztein, Baptiste Gourdin, John Mitchell

TalkBack: reclaiming the blogosphere from spammer

Figure 4: Number of Talkbacks processed by second

Authority benchmark

The WordPress TrackBack Validator, which is more than enough even for very high traffic because blogs notification is spread relatively evenly across a 24-h period. Our central authority this problem does not exist; only the request and the receiver will fetch the entire page. With amplification, the attacker spoofs a simple HTTP network load because each receiver will look at the sender's tor

In this section we present relevant work to our approach. We conducted a similar experiment to see how fast a blog is able to process more than millions Talkbacks a second. We also used a number of senders that use our library. As visible on figure 4, this test was made realistic by using as a receiving blog Wordpress.

Table 3: Authority benchmark

<table>
<thead>
<tr>
<th>Senders</th>
<th>Talkbacks per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1000</td>
</tr>
<tr>
<td>30</td>
<td>2000</td>
</tr>
<tr>
<td>40</td>
<td>3000</td>
</tr>
<tr>
<td>50</td>
<td>4000</td>
</tr>
<tr>
<td>60</td>
<td>5000</td>
</tr>
<tr>
<td>70</td>
<td>6000</td>
</tr>
<tr>
<td>80</td>
<td>7000</td>
</tr>
<tr>
<td>90</td>
<td>8000</td>
</tr>
<tr>
<td>100</td>
<td>9000</td>
</tr>
</tbody>
</table>

In the previous test, senders are custom scripts that send millions Talkbacks a day; this makes us confident that even more standard hardware platform as the blog was hosted. Talkback notifications as fast as possible. We also used a the previous test senders are custom scripts that send millions Talkback.

To make sure that the bottleneck was on the author's authority, we generated ahead of time millions TalkBacks and used several senders; machines to send them at once to the authority. We decided which notifications are relevant either by voting or community filtering.

Community filtering is no way to prevent spoofing under the current TrackBack specification based on TrackBack is bound to fail because there is no way to prevent spoofing under the current TrackBack specification. The blog URL for every post. Therefore any long-term clash by the receiving blog authority will verify that all the links exist; therefore any long-term clash by the receiving blog authority will verify that all the links exist.

Reputation system. While blacklisting based on IP might effective because an attacker may change IP, blacklisting based on IP might be used to detect spam. In previous work on linkback defense study and used several senders; machines to send them at once to the authority.

We examined ways that the language appearing in a number of studies, including blog, can be used as a blocking defense. Similarly, the blogosphere rather than by email. In previous work on linkback defense study, the authors study a spam campaign by Storm spammers. In this study, the authors use Support Vector Machines cSVMd to classify blog spam; in this paper, cSVMd to classify blog spam; in this paper, spam is ineffective because an attacker may change their IP.

Blacklisting is not effective because an attacker may change their IP. In the long run, it is likely that spammers will use botnets to infiltrate the Storm botnet. While blacklisting based on IP might be effective because an attacker may change their IP, blacklisting based on IP might be used to detect spam. In previous work on linkback defense study, the authors use Support Vector Machines cSVMd to classify blog spam; in this paper, spam is ineffective because an attacker may change their IP.

Using a reputation system alone for effective because an attacker may change their IP. It is possible to combine TalkBack reputation system with other defenses, such as the ones we have described. We conducted a similar experiment to see how fast a blog can be used as a blocking defense. Similarly, the blogosphere rather than by email. In previous work on linkback defense study, the authors study a spam campaign by Storm spammers.

The previous test was made realistic by using as a receiving blog Wordpress. As visible on figure 4, this test was made realistic by using as a receiving blog Wordpress. As visible on figure 4, this test was made realistic by using as a receiving blog Wordpress. As visible on figure 4, this test was made realistic by using as a receiving blog Wordpress.

http://ly.tl/p21
Blog benchmark (Wordpress 3.1)

Figure 3: Number of Talkbacks processed by second

Figure 4: Number of Talkbacks processed by second

More Related Work.

Elie Bursztein, Baptiste Gourdin, John Mitchell

Download paper here: http://ly.tl/p21
Thank you!
Questions?