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 it.
   - I've been wanting to redesign the MailChimp logo since I first designed it 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. My co-founder, Mark, said: "Yo Ben, MailChimp's logo guy. I think it could use a logo." My 19-year itch for a new logo was thus also cured.
4. Publish Date
   - Published on: September 11, 2008 at 4:49 am
   - Last edited by Ben on September 11, 2008 at 4:49 am
   - Draft saved at 10:01:29 pm.
   - Word count: 1492
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?

User

Elie Bursztein, Baptiste Gourdin, John Mitchell

TalkBack: reclaiming the blogosphere from spammer

http://ly.tl/p20
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..."
"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!"

Trackback: "Jimmy Lightning is swell"

"Best Post Ever"

"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!"

1. "Jimmy Lightning is swell"
   
   "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..."

2. Little Timmy said to me...
   
   "What's Trackback, Daddy?"

   "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!"

3. Trackback: "Jimmy Lightning is swell"
   
   "Best Post Ever"

   "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!"
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
Trackback Spams

Number of Spams

Mar 1, 2007
Mar 14, 2007
Mar 27, 2007
Apr 9, 2007
Apr 22, 2007
May 5, 2007
May 18, 2007
May 31, 2007
Jun 13, 2007
Jun 26, 2007
Jul 9, 2007
Jul 22, 2007
Jul 26, 2007
Aug 4, 2007
Aug 17, 2007
Aug 30, 2007
Sep 12, 2007
Sep 25, 2007
Oct 8, 2007
Oct 21, 2007
Nov 3, 2007
Nov 16, 2007
Nov 29, 2007
Dec 12, 2007
Dec 25, 2007
Jan 7, 2008
Feb 2, 2008
Feb 15, 2008
Feb 28, 2008
Mar 12, 2008
Mar 25, 2008
Apr 7, 2008
Apr 20, 2008
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 you know that I, the target of your vitriol, have a little too intimate. Or, you could leave a comm...
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 Intense Debate and Disqus show, they simply do not show trackbacks because of the spam problem.
Adversary Model

- Resourceful
- Efficient
- Knowledgable
- Adaptive
• 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 information in the body</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Threats are not addressed by current Linkback specifications.
Introducing Talkback!
Use a **light-weight PKI** to fight **Spam**
In the TalkBack protocol there are at least three or four steps used to send a Linkback. These steps are depicted in Figure 1: TalkBack protocol overview.

Here is what happens during these steps:

1. **Auto-discovery**
   - S Authority requests a seed from the authority.
   - This information is fetched in a visit from the sender site.

2. **Authority posting**
   - S authority posts a link to the blog.

3. **Receiver authority**
   - A receiver authority contacts the receiver to fetch and validate the sender's public key.
   - This is done by contacting the receiver authority with the notification URL and public key fetched at step 1.

4. **Receiver**
   - A receiver sends the secure LinkBack to the sender at posting time.

Table 1: Linkback mechanisms comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>RefBack</th>
<th>PingBack</th>
<th>TrackBack</th>
<th>TalkBack</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>
<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>
<td>HTTP POST</td>
</tr>
<tr>
<td>Information sent</td>
<td>none</td>
<td>- S post URL, - R post URL</td>
<td>- S post URL, - S site name, - S post title, - S post excerpt</td>
<td>- S post URL, - S site name, - S post title, - 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
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.
• Open-source library
• Wordpress plugin
• Authority: https://talkback.stanford.edu
Elie Bursztein, 242 Million TrackBack Validator. which is more than enough even for very high traffic the latest version equipped with our plugini As in an hour basis, because blogs notification is spread relatively our central authority this problem does not exist. only the attack with amplificationv the attacker spoofs a simple HTTP network load because each receiver will look at the sender's contains the URL of the receiver. This approach increases the 10. ADDITIONAL RELEVANT WORK

It is unlikely that a single blog will receive more than a million talkbacks a day. A blog is able to process more than a million talkbacks a second on a nighz Intel quad core. As visible in figure 3: Number of Talkback by second. To process per second. To make sure that the bottleneck was on the authorityg we generated ahead of time many TalkBacks the number of senders increases the number of TalkBacks the authorityi The senders are not actual blogs but custom and used several senderskmachines to send them at once to the authority g we generated ahead of time millions TalkBacks the receiving blog is able to process Talkback notifications. To the previous test, senders are custom scripts that send millions of TalkBacks the receiving blog Wordpress. The WordPress TrackBack Validah Vector Machines cSVMd to classify blog spami In a blog can be used as a blocking defensei Similarly, Spamg examines ways that the language appearing in the blogosphere than by email. In previous work on linkback defense study. There are a number of studiesg including experiences in generated by Storm spami Former spammers relate their infiltrating the Storm botnetg while note that ideas spread more quickly in a small number of IPsg it is not a sustainable solution because currently work as the spammers today seem to use only a IP Blacklisting.

Small specificationdi is no way to prevent spoofing under the current TrackBack specification based on TrackBack is bound to fail because there the blog URL for every postsi Therefore any longhterm clash between the previous test, senders are custom scripts that send millions TalkBacks the receiving blog Wordpress. The WordPress TrackBack Validah Vector Machines cSVMd to classify blog spami In a blog can be used as a blocking defensei Similarly, Spamg examines ways that the language appearing in the blogosphere than by email. In previous work on linkback defense study. There are a number of studiesg including experiences in generated by Storm spami Former spammers relate their infiltrating the Storm botnetg while note that ideas spread more quickly in a small number of IPsg it is not a sustainable solution because currently work as the spammers today seem to use only a IP Blacklisting.

Using a reputation system alone for Community filtering. Reputation system. It is possible to combine TalkBack Community filtering. It is unlikely that a single blog will receive more than a million talkbacks a day. It is likely that a single blog will receive a million talkbacks a day. Talkback notifications as fast as possible. We also used a the previous test, senders are custom scripts that send millions TalkBacks the receiving blog Wordpress. The WordPress TrackBack Validah Vector Machines cSVMd to classify blog spami In a blog can be used as a blocking defensei Similarly, Spamg examines ways that the language appearing in the blogosphere than by email. In previous work on linkback defense study. There are a number of studiesg including experiences in generated by Storm spami Former spammers relate their infiltrating the Storm botnetg while note that ideas spread more quickly in a small number of IPsg it is not a sustainable solution because currently work as the spammers today seem to use only a IP Blacklisting.

Figure 3: Number of Talkbacks processed by second

Figure 4: Number of Talkbacks processed by second
Blog benchmark (Wordpress 3.1)

Number of Talkbacks processed by second

Number of Talkbacks by seconds

Number of senders

Blog benchmark (Wordpress 3.1)

Figure 3: Number of Talkbacks processed by second

Figure 4: Number of Talkbacks processed by second

TrackBack: reclaiming the blogosphere from spammers

Elie Bursztein, Baptiste Gourdin, John Mitchell

http://ly.tl/p20
Thank you!
Talkback
http://ly.tl/talkback

Follow-us on Twitter
@elie, @baptiste