Great Circle

Firewalls Mailing List

The *Firewalls* mailing list is for discussions of Internet firewall security systems and related issues. Relevant topics include the design, construction, operation, maintenance, and philosophy of Internet firewall security systems.

The *Firewalls* mailing list was created by Great Circle Associates in September 1992, and was hosted here until April 1998, when it was moved to a new home at GNAC. In June 2002, the list was moved again, to its current home at the Internet Software Consortium.

This web site provides access to the archives of the Firewalls mailing list from the period when it was hosted by Great Circle Associates, from the list's creation in September 1992 until it moved to GNAC in April 1998. For archives after April 1998, see the current Firewalls mailing list web page hosted by the Internet Software Consortium.

Next Generation Firewall
Get Advanced Network Protection Across Your Enterprise w/ McAfee.

Subscription Information

To subscribe to or unsubscribe from the Firewalls mailing list, see the current Firewalls mailing list web page hosted by the Internet Software Consortium.

Archives

All messages sent to the list while it was hosted by Great Circle Associates (from the list's creation in September 1992 until it moved to GNAC in April 1998) are publicly available in a web-based archive, as well as searchable via Google and other search engines.

Messages sent to the list after it moved to GNAC in April 1998 (and, eventually, further moved to ISC) are available via the current Firewalls mailing list web page hosted by the Internet Software Consortium.

We strongly believe that searchable archives of past messages are one of the most important features of Internet mailing lists such as this one, and that it's critical that those archives be complete and accurate representations of the discussions on the list. Therefore, as a general rule we will not honor requests to edit the archives to remove or modify particular postings. So, subscribers were advised to be thoughtful before posting; as they were going to have to live with whatever they said being in the archives forever, searchable by employers, family members, etc.

The email address that messages were posted from will likely be harvested from the archives by spammers. We have carefully considered this problem, and concluded that there really isn't any way we can prevent that while still maintaining useful and searchable archives. Subscribers were advised to take whatever steps they felt were appropriate to protect themselves, such as using a strong spam-

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

For Further Information

Brent Chapman
Great Circle Associates, Inc.
brent@greatcircle.com

Great Circle Associates, Inc.

2608 Buena Vista Ave.
Alameda, CA 94501 USA

Please report problems to Webmaster@GreatCircle.COM
Copyright © 2015 Great Circle Associates, Inc.

WWW: www.greatcircle.com
Email: info@greatcircle.com
USA Toll Free: 877 GRT CRCL
(877 478 2725)
International: +1 415 861 3588
Fax: +1 415 552 2982

Google [ ] Google Search

○ Search Internet ● Search www.greatcircle.com

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Great Circle

Firewalls
(June 1995)

Indexed By Date: [Previous] [Next] Indexed By Thread: [Previous] [Next]

IT Perimeter Security S/W

Manage security device & firewall logs with Firewall Analyzer.Try now

Subject: **Re: Java and HotJava security issues (fwd)**
From: Brian Rogers <brogers @ integctr . com>
Organization: The Integrity Center (214)484-8140 (800)456-1811
Date: Thu, 8 Jun 1995 17:10:58 -0500 (CDT)
To: Ken Hardy <ken @ bridge . com>
Cc: firewalls @ greatcircle . com, Frank Westervelt <fwesterv @ hub . eng . wayne . edu>
In-reply-to: <Pine . SUN . 3 . 90 . 950607215427 . 14125A-100000 @ ernie>

On Wed, 7 Jun 1995, Ken Hardy wrote:

> Brian Rogers <brogers @
> integctr .
> com> postulates:
>
> >HotJava and other Java browsers could use a system/global config and a
> >user config. The sys admin would set up the global config as securely as
> >is appropriate. The browser could also be written so that the sys admin
>
> What about all those programmers, &c., who are root for their own
> workstation? What about all those Linux & FreeBSD &c. boxes with no
> central administration? What about Windoze in all its guises?

Browsing the WWW from root is a bad idea. Doing anything from root that does not require root access is generally considered a bad habit to get into, because a typo can be more costly.

Independent Linux and BSD systems can be dangerous on your network, but that's a political problem. If the users want their own workstations, they should know that it could threaten the safety of the network. They should also know what the **** they're doing if they're running their own workstation; otherwise, they don't deserve one.

Windows NT and Windows 95 are multi-user operating systems; therefore, they have both global and user configs. Windows 3.1 systems have no user config, just a global. Overridability options can still be used in Windows 3.1.

Also, in a network I would not rely just upon the configuration of the browser, especially if there are Windows 3.1, Linux, BSD, or other user-administered systems on the network. On a network, users should go through a firewall proxy to access the internet. The firewall gives the network administrator an opportunity to centrally screen Java code (see below).

>
> I postulate:

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

> trivial. But I, too, suspect that there will be a lot of really cool
> and/or useful "applets" out there, and significant user pressure would
> build against blanket blocking. That'll lead to end-runs around the
> firewall, as has been oft discussed here.

You could block URL's, but the http proxy could also scan for Java code. Java code could be removed, or a heuristic scan could be applied to the Java code that would check for things like editing of .rhosts, piping /etc/passwd into /bin/mail, or whatever. This may be too complex for a simple (and therefore secure) firewall.

Another option would be to scan for Java code and block all Java by default. When users clamor for a Java applet, the administrator could inspect the applet for safety. The administrator could use some sort of heuristic scanner. He could also simply decompile and read the code. Once the administrator is certain the code poses no threat, he could add the code's URL and checksum to a database of applets that are not filtered. If the applet changes, then the checksum verification would fail and the admin would have to re-verify the applet. Unfortunately, an annoyance would develop if an applet were being continuously revised and debugged "in public."

Some companies already forbid use of outside software not approved by MIS. Java, unfortunately, almost redefines "outside software."

I don't think the problem is insoluble. I just think that the solution will require technical insight, sophistication, and work.

```
/* Brian Rogers -- tech admin, coffee achiever -- brogers @
 integctr .
 com  */
/* The Integrity Center    --   "objective risk management information" */
/*           http://www.integctr.com/    --   info @
 integctr .
 com         */
/*  (214)484-6140  (800)456-1811  FAX (214)484-6381  FOD (214)484-2147  */
```

Follow-Ups:

- **Re: Java and HotJava security issues (fwd)**
  From: Martin Hepworth <max @ airtechsms . co . uk>
- **Re: Java and HotJava security issues (fwd)**
  From: peter @ nmti . com (Peter da Silva)

References:

- **Re: Java and HotJava security issues (fwd)**
  From: Ken Hardy <ken @ bridge . com>

Indexed By Date	Previous:	Re: UNSCRIBE From: kac @ gasco . com (Casey Canby X5530)
	Next:	Re: Notes from CERT BOF in SLC From: martin @ wsmr . emh91 . army . mil (Gary L Martin)
		Re: Java and HotJava security issues (fwd)

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Thread	Next:	Re: Java and HotJava security issues (fwd) From: peter @ nmti . com (Peter da Silva)

Google [ ] Google Search

○ Search Internet ● Search www.greatcircle.com

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.