Original-URL: http://web.inf.tu-dresden.de/~hf2/anon/aproxies/

Flaw in anonymity systems found

Hannes Federrath

TU Dresden / International Computer Science Institute, Berkeley

E-Mail: federrath@inf.tu-dresden.de

February 18, 2000, updated: May 06, 2000

I have tested a few existing anonymity proxies (A-proxies) available in the Internet. The goal was to find out whether these systems filter all dangerous contents or not. I found a security hole that is based on a mistake in the parsing algorithm.

I have tested the following systems:

System	Result
http://www.anonymizer.com	Not secure against the attack **(May 06, 2000: fixed..., now secure!)**
http://aixs.net/aixs/	Not secure against the attack
http://www.rewebber.com	secure against the attack, flaw fixed on Feb. 18, 2000
http://ikt.inf.tu-dresden.de/~feder/cgi-bin/a.cgi	secure against the attack **(Dec 03, 2001: service no longer available.)**

Deutsche Fassung (ausführlicher)

The attack described below uncovers the IP address of a client to the server.

The security hole of the systems is based on the insufficent parsing of contents of cascading style sheets.

The attack has been sucessful with Internet Explorer. Netscape Navigator does not recognize or interpret the necessary tags yet. However, the new Seamonkey (see http://www.mozilla.org) interprets the tag.

Assume the client requests a web page with the following content via an A-proxy:

```
<html>
<head>
<title>css test 2</title>
<link rel="stylesheet" type="text/css" href="style.css" title="css">
</head>
<body bgcolor="#FFFFFF">

<h1>css test 2</h1>

This is a list:
```

```
<ul>
    <li> Item 1
    <li> Item 2
    <li> Item 3
</ul>

<p>
End.

</BODY>
</HTML>
```

The A-proxy loads the content from the server, parses all nested links, and adds a prefix in order to load the nested contents via the proxy too.

Example: Anonymizer replaces the line

```
<link rel="stylesheet" type="text/css" href="style.css" title="css">
```

by

```
<link rel="stylesheet" type="text/css"
href="http://anon.free.anonymizer.com/http://www.icsi.berkeley.edu/~hannes
/atest/style.css" title="css">
```

Subsequently, the browser loads the stylesheet file via the anon proxy.

The stylesheet file `style.css` consists of the following content:

```
ul  { list-style-image:url(http://www.inf.tu-dresden.de/~hf2/dash.gif); }
```

This line contains a command that uncovers the IP address of the client. This command causes that the bullets in lists created by the `<ul>` tag are replaced with a user defined graphic image (here: `http://www.inf.tu-dresden.de/~hf2/dash.gif`).

The flaw of the A-proxies is that the stylesheet file is not sufficently parsed, and the address of the user defined image is not prefixed with the A-Proxy. The embedded image is requested directly from the client.

Thus, the client leaves his IP address to the server `www.inf.tu-dresden.de` and is uncovered.

More information on anonymity

- http://www.inf.tu-dresden.de/~hf2/anon/
- Our implementation of an A-proxy
- Links to other systems

* * *