Net-Square Security Advisory:	NS-310107-GMAIL
Date of advisory draft:	08 February, 2006
Release Date:	31 January, 2007
Affected Application:	Google Mail - Gmail
Type:	Multiple problems in server-side session handling
Severity:	Medium
Status:	Corrected by Google on 05 January, 2007
Authors:	Pallav Khandhar <pallav at net-square dot com> Saumil Shah <saumil at net-square dot com>
Publication URL:	http://net-square.com/advisory/NS-310107-GMAIL.pdf

OVERVIEW

1. Gmail fails to expire the *GX* session cookie from the server side even when the user logs off from Gmail upon clicking "Sign-Out" from the application. The cookie is cleared from the client side (browser), but is not cleared from the server side. If re-used, it provides access to the user's Gmail account.

2. Upon logging in again, a new *GX* session cookie is created, but the old session cookies still stay active on the server side. Therefore, any session cookie can be re-used to gain access to the user's Gmail account.

DETAILED DESCRIPTION

Upon successful authentication to Gmail, Gmail sets a session cookie named *GX*. The *GX* cookie is set to expire at the end of the browser session. Upon logging off from Gmail via the "Sign-Out" link, the *GX* session cookie is cleared from the browser's cookie memory.

However, the *GX* cookie entry stays active on the server side. If a valid *GX* cookie is re-used, even after logging off, Gmail allows access to that user's mail account. Net-Square has tested that *GX* session cookies stay active indefinitely. Our testing has shown that it was possible to successfully re-use a *GX* session cookie for a period of two weeks since its creation.

Secondly, Gmail does not seem to check for duplicate or multiple *GX* cookies being sent in the same HTTP request. It is possible to send a number of *GX* cookies in the same HTTP request and yet gain access to a user's Gmail account, with at least one of the *GX* cookies belonging to a valid session some time in the past.

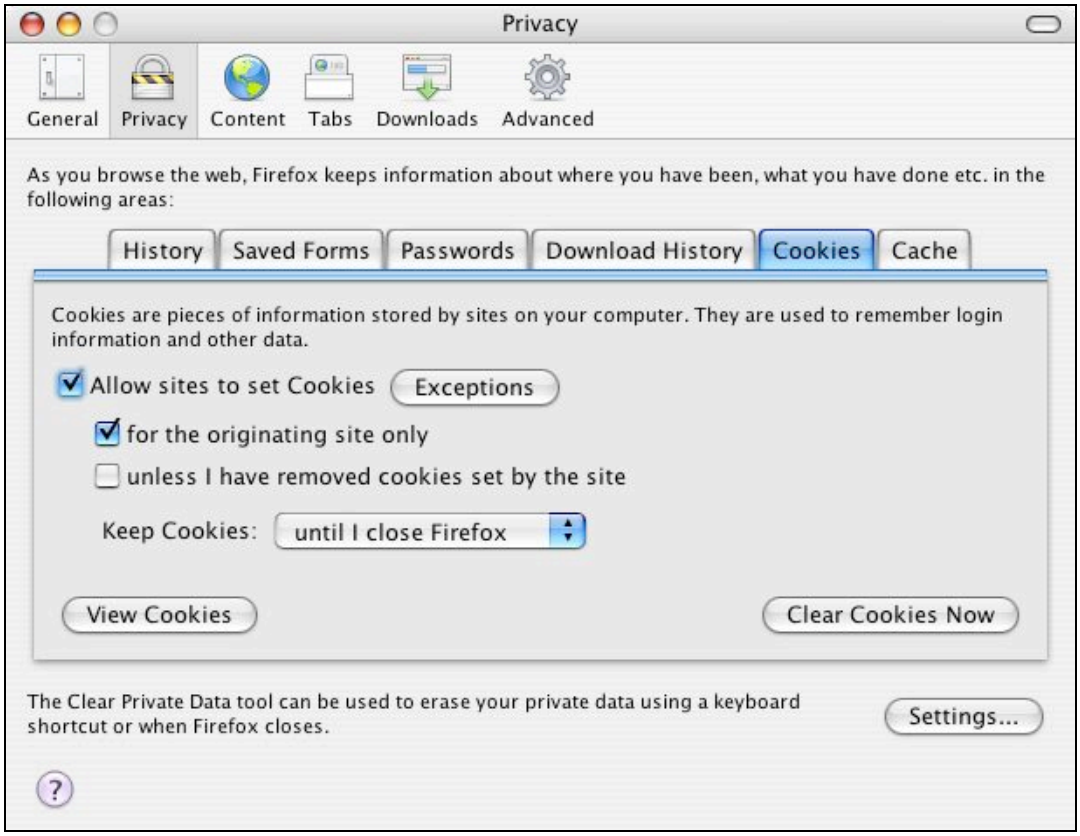
The best practices for session handling would involve expiry of all session related cookies and tokens from the server side, as well as an attempt to clear them from the client side. Server side sessions should also be checked for periods of inactivity. If there is no user activity detected for a pre-defined period of time, the application should clear the session cookie and variables.

PROOF OF CONCEPT

We have used an account "netsquare.test@gmail.com" for demonstrating these vulnerabilities. Testing was performed with Mozilla Firefox 1.5 with the following privacy settings, as shown in the figure below:

Options > Privacy > Cookies

"Allow sites to set cookies" is checked on.
"for the originating web site only" is checked on.
Keep cookies "until I close Firefox".



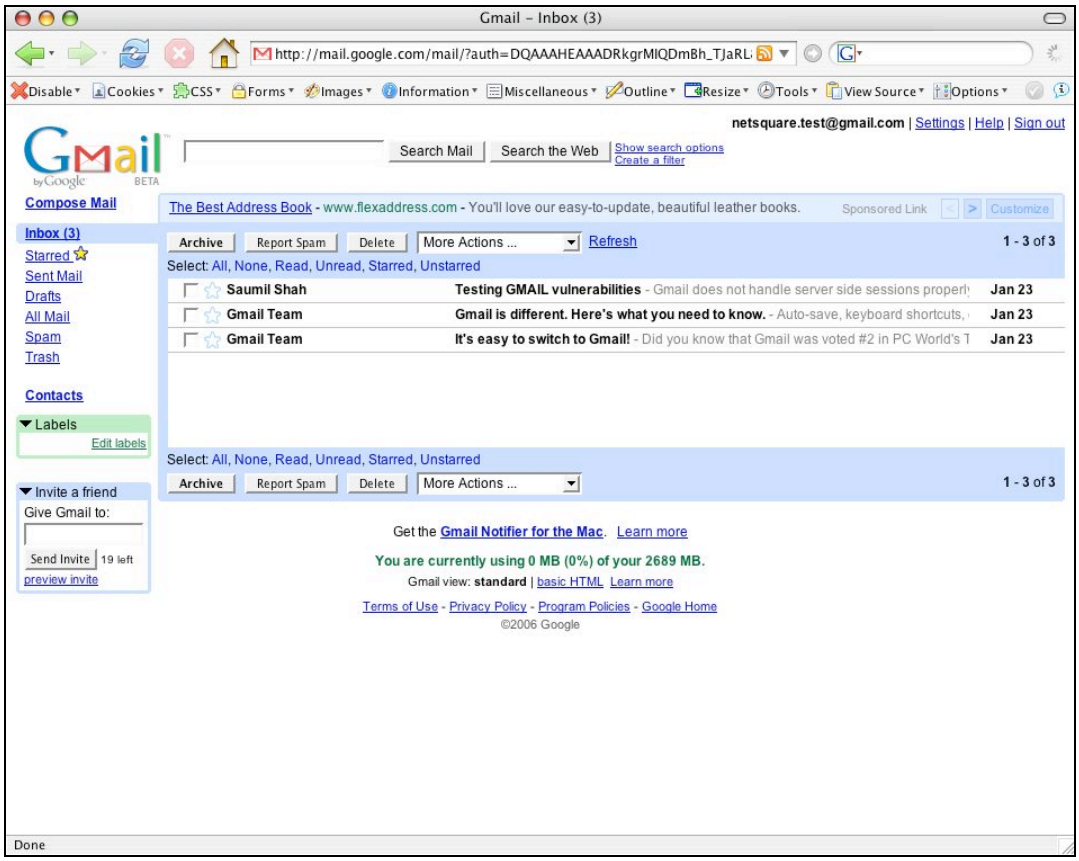
The above settings ensure that all cookies are cleared every time the browser is shut down.

Step 1: Login to Gmail

Open the URL http://mail.google.com/ and enter your username and password.

After a couple of redirections, the browser will be pointing to the main Gmail login page at:

https://www.google.com/accounts/ServiceLogin?service=mail&...

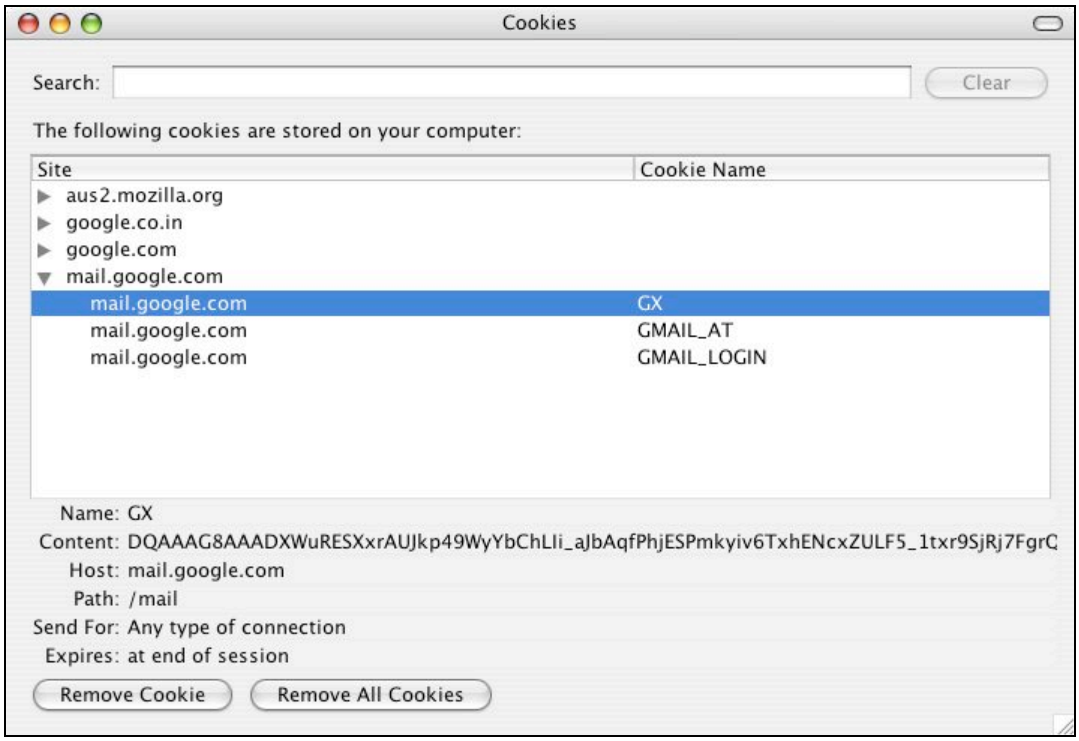


Step 2: Inspect cookies

After logging in, if we view the cookies currently set in our browser, we find the following three cookies set for "mail.google.com":

```
GX
GMAIL_AT
GMAIL_LOGIN
```

The figure below shows the cookies set in our browser:



The *GX* cookie is a session cookie, which is set to expire whenever the browser terminates.

In our test, the *GX* cookie observed was:

```
GX=DQAAAG8AAADXWuRESXxrAUJkp49WyYbChLIi_aJbAqfPhjESPmkyiv6TxhENcx
   ZULF5_1txr9SjRj7FgrQRWfwLSxb2AZrpJ3brTLHiTyt7lwO_jPfHAY7oBh-sf
   xAvFbL7K41xAJX2jbkFM7ncJTp6y5yS6dvW4;
Path=/mail
```

Save this cookie for future use.

The request header (after clearing the login form) going to http://mail.google.com/mail/ is as follows:

```
GET /mail?auth=DQAAAHEAAABPqegX83ChBpo62frjGtZYXz7Cn3f_yY0T4AhSRD
    DG7Uw1_zifQf8e0IGSVfxL8a_GPoGxRRrxQZ5qx5vqlMF2FR06v09a6w2w6Nn
    BRBVkZbufEYTDcPTeoe8yy9im0aO4KWodrj52JNexcsSvfCdyeRSsQiYg5TGQ
    BCdM80XyLQ HTTP/1.1
Host: mail.google.com
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US;
    rv:1.8) Gecko/20051111 Firefox/1.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;
    =0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

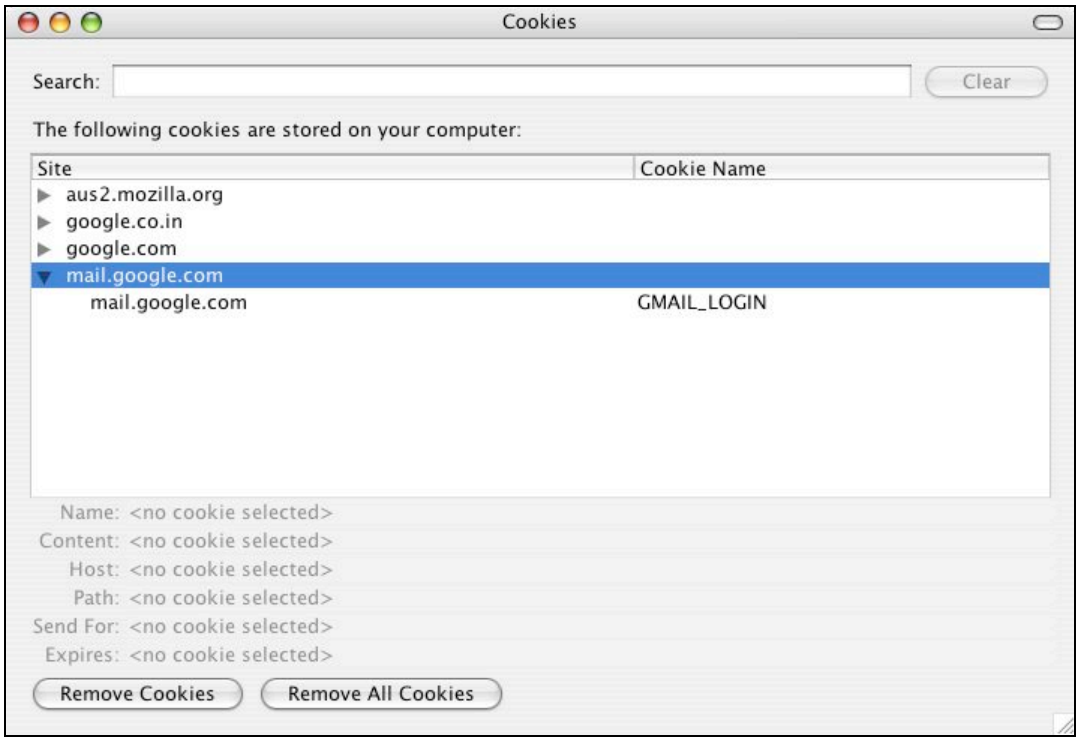
```
Keep-Alive: 300
Connection: keep-alive
Cookie: GMAIL_SU=1;
        GMAIL_LOGIN=1138660454156/1138660454156/1138660520315/1138
        660524605/1138660524981/1138660528081/1138660528610/false/
        false;
        PREF=ID=e6655de35f218248:CR=1:TM=1120584839:LM=1138660528:
        GM=1:S=lxH1zLw4gp_wVgiV;
        TZ=300;
        GMAIL_RTT=118;
        GMAIL_LOGIN=T1138660572488/1138660572488/1138660645409;

S=gmail=aK2dc5KFU6w:gmail_yj=IQRKdEdg6e8:gmproxy=NdnxcczuPsM;
        SID=DQAAAG0AAAB9MJmUsx1ssFbSvDmseSDj4ZV2OJ18aqA9l0TKvL5dj3Pm
        W0DC1XJZ9AkClZjhums6m8BMSmLpgGcOc8JEm6670jBOoqdrA4AEYc9HD_AE
        1lzXEuMTxWVetPd8q4bMALQa7yogbPiYkauvASVHtAeO
```

The response header received is as follows:

```
HTTP/1.1 302 Moved Temporarily
Set-Cookie: GV=EXPIRED;Domain=mail.google.com;
            Path=/;Expires=Mon, 01-Jan-1990 00:00:00 GMT
Set-Cookie: GV=EXPIRED;Domain=mail.google.com;Path=/mail;
            Expires=Mon, 01-Jan-1990 00:00:00 GMT
Set-Cookie: GX=DQAAAG8AAADXWuRESXxrAUJkp49WyYbChLIi_aJbA
            qfPhjESPmkyiv6TxhENcxZULF5_1txr9SjRj7FgrQRWf
            wLSxb2AZrpJ3brTLHiTyt7lwO_jPfHAY7oBh-sfxAvFb
            L7K41xAJX2jbkFM7ncJTp6y5yS6dvW4; Path=/mail
Set-Cookie: GMAIL_AT=1be40710a00c7288-1091d769d53; Path=/mail
Set-Cookie: GMAIL_RTT=EXPIRED; Domain=.google.com;
            Expires=Sun, 29-Jan-06 22:37:26 GMT; Path=/mail
Set-Cookie: GMAIL_LOGIN=EXPIRED; Domain=.google.com;
            Expires=Sun, 29-Jan-06 22:37:26 GMT; Path=/mail
Set-Cookie: S=gmail=aK2dc5KFU6w:gmail_yj=UO2Xjdj_ZVI:
            gmproxy=NdnxcczuPsM; Domain =.google.com; Path=/
Cache-control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Location: /mail/?auth=DQAAAHEAAABPqegX83ChBpo62frjGtZYXz7Cn3f_
          yY0T4AhSRDDG7Uw1_zifQf8e0IGSVfxL8a_GPoGxRRrxQZ5qx5vq
          lMF2FR06v09a6w2w6NnBRBVkZbufEYTDcPTeoe8yy9im0aO4KWod
          rj52JNexcsSvfCdyeRSsQiYg5TGQBCdM80XyLQ&shva=1
Content-Length: 0
Server: GFE/1.3
Date: Mon, 30 Jan 2006 22:37:26 GMT
```

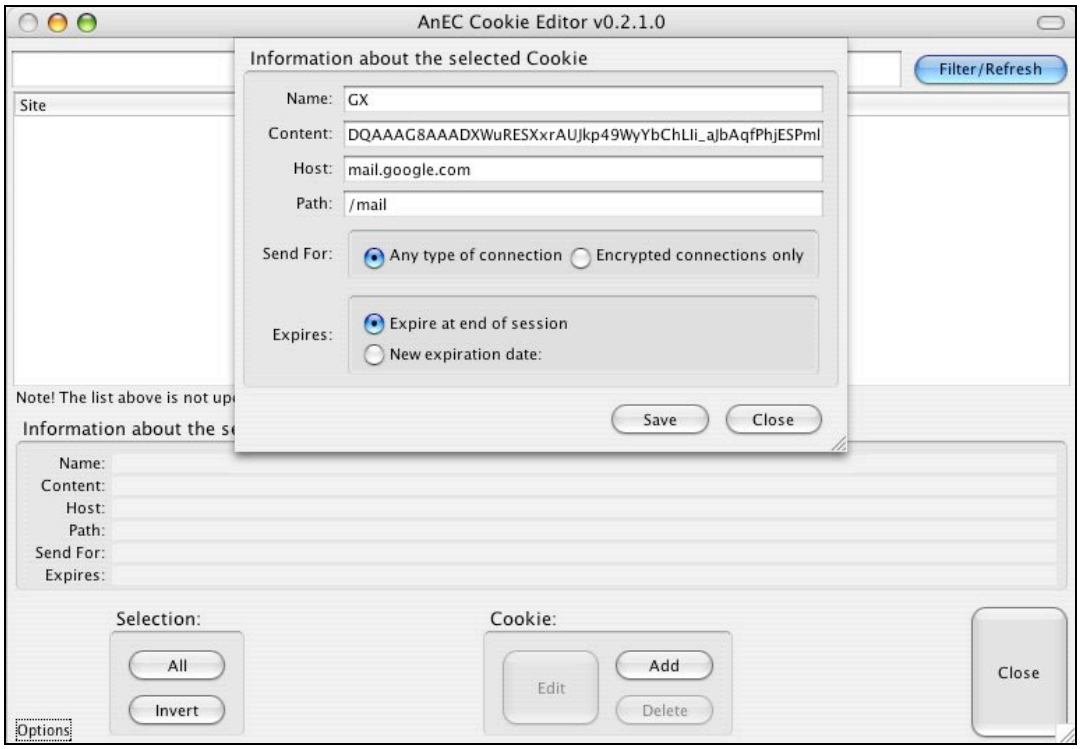
Step 3: Log out of Gmail

Use the "sign out" link to log out of Gmail. The session cookies will be cleared from the browser's memory. The following screenshot shows there are no session cookies remaining in the browser's memory.



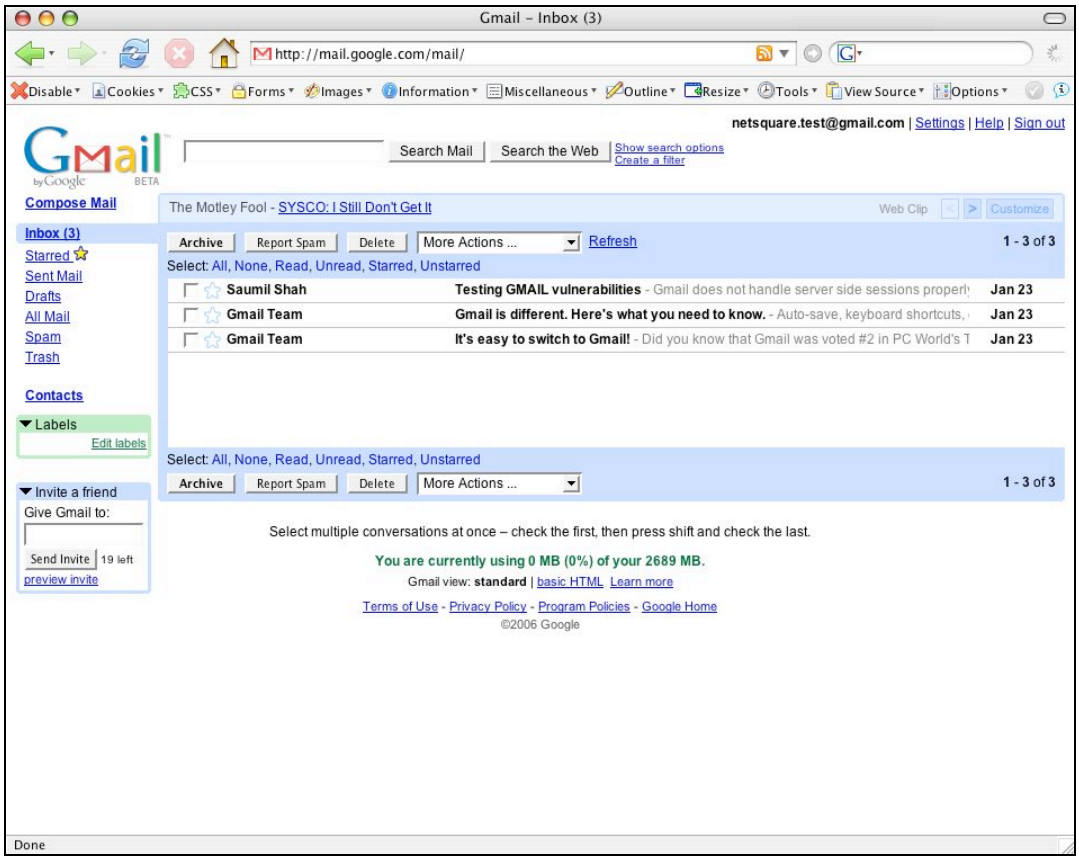
Step 4: Set the *GX* cookie back in the browser's cookie store

Use the Firefox Add n Edit Cookies extension to insert the saved *GX* cookie back into the browser's cookie store. The following screenshot demonstrates this:


AnEC Cookie Editor v0.2.1.0
Information about the selected Cookie
Name: GX
Content: DQAAAG8AAADXWuRESXxrAUJkp49WyYbChLIi_ajbAqfPhjESPml
Host: mail.google.com
Path: /mail
Send For: Any type of connection Encrypted connections only
Expires: Expire at end of session
New expiration date:
Save
Close
Filter/Refresh
Site
Note! The list above is not up
Information about the se
Name:
Content:
Host:
Path:
Send For:
Expires:
Selection:
All
Invert
Cookie:
Edit
Add
Delete
Close
Options

Step 5: Browse to http://mail.google.com/

Once the cookie is set, as described above, point the browser to http://mail.google.com/. After a few HTTP redirects, it will land you into the user's mail account. Notice that there is no "?auth=..." parameter on the URL this time.



IMPACT

Session cookies such as the *GX* cookie should be cleared at both the client side as well as the server side upon termination of the authenticated session. Gmail fails to clear the *GX* cookie from the server side. It was observed that *GX* session cookies stay active for two weeks after they are created. If at any point during a user's Gmail session, the *GX* cookie has been intercepted or recovered, an attacker can gain unauthorized access to the Gmail account long after the user signs off. Even if the user logs in again with a new *GX* cookie, the old ones never expire, and the replay attack still works.

It has been observed by Net-Square that sending HTTP requests with multiple *GX* cookies also works, and lets the attacker gain unauthorized access to a victim's Gmail account.

Changing the password has no effect either, since a *GX* session cookie once set after proper authentication stays working.

WORKAROUNDS/FIXES

~~At this point in time, there are no workarounds that a user can use to protect his or her session. Net-Square advises Gmail users not to use their Gmail accounts from untrusted computers or networks.~~

Google has fixed this problem on their side. Session cookies are now set to expire within 24 hours from the server side, as opposed to two weeks. Net-Square was checking this vulnerability almost every week. The vulnerability seems to have been fixed around 05 January, 2007.

VULNERABILITY REPORTING AND STATUS

Date of discovery: 01 February 2006
Date of reporting to Google: 10 February 2006
Follow-up emails: 22 February 2006, 20 June 2006, 10 December 2006
Vulnerability fix from Google: January 2007

CREDITS

AnEC Cookie Editor - http://addneditcookies.mozdev.org/

CONTACT

Net-Square Solutions Pvt. Ltd.
1 Sanjivbaug, Paldi, Ahmedabad 380007, India
Tel: +91 79 2663 7090
Fax: +91 79 2663 8051
http://net-square.com/

DISCLAIMER