Securing the Gmail Notifier

By
Ramece Cave

Introduction

Gmail is quite possibly becoming one the most widely used free web-based email systems. Google is consistently innovating new methods to push the technology envelope. A widely used add-on to Gmail is the Gmail Notifier.; this application periodically checks the inbox of your account for new messages. If a new message arrives a pop-up will display in the right corner of your screen. Though this feature is useful it does not encrypt the communication between your PC and the Gmail account, potentially allowing your data to be intercepted.

After noticing this I wanted to resolve the issue and began confirming and investigating methods to remedy this situation. I decided to begin investigating this at it simplest level the binary. I suspected there might be a clue to point me in the right direction, to my amazement the problem has a very simple solution that did not warrant any further investigation.

How Notifier Works

The application sits resident in the system tray and periodically checks your Gmail account for new messages in the Inbox. When a new message is found a pop-up appears in the lower right corner of your screen with the name of the person sending the email, subject and a few characters of the message. This process begins by you logging into the application, a prompt for your Gmail login credentials will appear, this information is sent securely to the Gmail.
Figure 1 displays the Notifier login; Figure 2 displays the secured communication.

Gmail Notifier Login

Figure 1

Secured Communication to Gmail

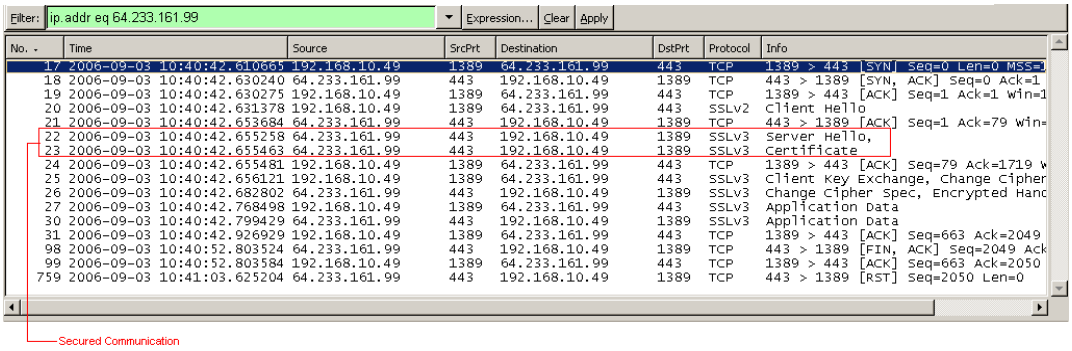

Figure 2

Identifying the Problem

The login portion is secured, but the mailbox query for new messages is not. This allows mail content to be viewed encrypted across the wire. Figures 3 and 4 display an unencrypted Gmail Notifier mailbox query and the contents of a recovered message.

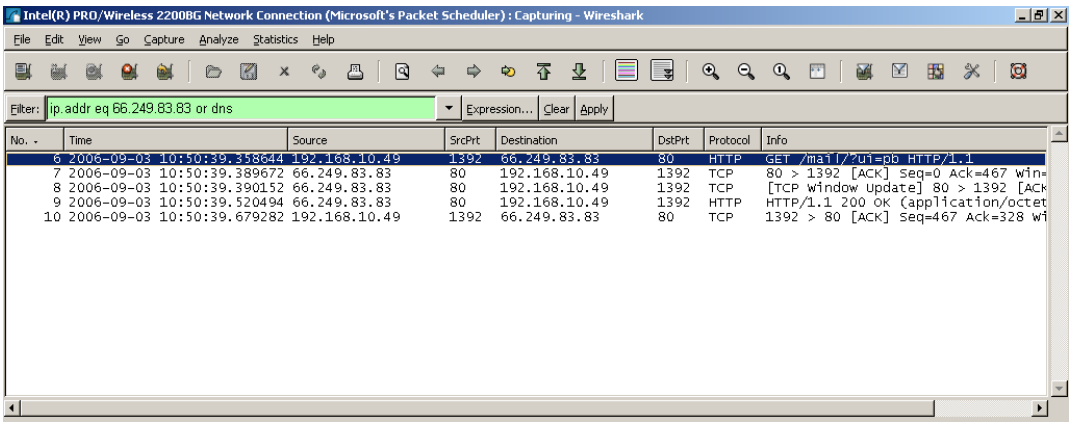

Figure 3

Gmail New Mail Notification

Figure 4

Sender	*Ramece Cave*
Subject	*The Cult of The Pink Bunny Slippers …*

Recovered Message Content

```
.
.ramece@yahoo.com..Ramece Cave.........8The Cult of The Pink Bunny Slippers - Bi Monthly
Meeting..gGentlemen, It is time for our meeting once again, who is on refreshment
detail? Also who&#39;s &hellip;......
```

Figure 5

In the recovered message we see a message arriving from "Ramece Cave" with an email address of ramece@yahoo.com. The message talks about a bi-monthly meeting called the "Cult of the Pink Bunny Slippers" and refreshments for the event

Correcting the Problem

To enable secured mail checks we must modify gnotify.exe with a hex editor, the file is located in c:\Program Files\Google\gnotify.exe. Using a hex editor search for "http" or go to offset: 00386352. In order for this modification to be successful, we must over-write into free-space because modifying a previous value may produce undesired results or cause the application to not function. Figures 4 and 5 display the modification process and location.

Before Modification

```
00386288 | 65 00 74 00 00 00 00 00  2F 61 63 63 6F 75 6E 74 | e t      /account
00386304 | 73 2F 53 65 72 76 69 63  65 43 6C 69 65 6E 74 4C | s/ServiceClientL
00386320 | 6F 67 69 6E 3F 73 65 72  76 69 63 65 3D 6D 61 69 | ogin?service=mai
00386336 | 6C 00 00 00 68 74 74 70  73 3A 2F 2F 77 77 77 2E | l    https://www.
00386352 | 67 6F 6F 67 6C 65 2E 63  6F 6D 00 00 68 74 74 70 | google.com  http
00386368 | 3A 2F 2F 6D 61 69 6C 2E  67 6F 6F 67 6C 65 2E 63 | ://mail.google.c
00386384 | 6F 6D 2F 6D 61 69 6C 2F  00 00 00 00 3F 00 75 00 | om/mail/     ? u
```

Free Space

Change "http" to "https"

Figure 4

After Modification

```
00386336 | 6C 00 00 00 68 74 74 70  73 3A 2F 2F 77 77 77 2E | l    https://www.
00386352 | 67 6F 6F 67 6C 65 2E 63  6F 6D 00 00 68 74 74 70 | google.com  http
00386368 | 73 3A 2F 2F 6D 61 69 6C  2E 67 6F 6F 67 6C 65 2E | s://mail.google.
00386384 | 63 6F 6D 2F 6D 61 69 6C  2F 00 00 00 3F 00 75 00 | com/mail/    ? u
```

Modification wrote in free space

Connecting via SSL

Figure 5

Confirming the Change

The best method to confirm the change is functioning is (primarily the application still runs) use the "Check mail now" feature in Notifier and monitor the communication. If the change was successful the query will take place over SSL using TCP port 443. Figure 8 display secure communication after the modification. Figure 9 is a new message pop-up received after the modification. Figure 10 is the recovered message context, because it was received over a secure method, the context is illegible.

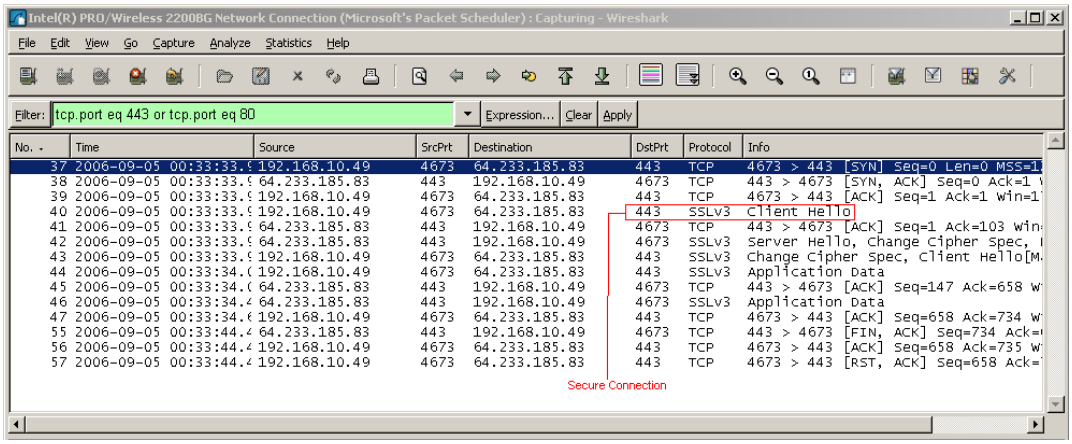

Figure 8

Gmail New Mail Notification

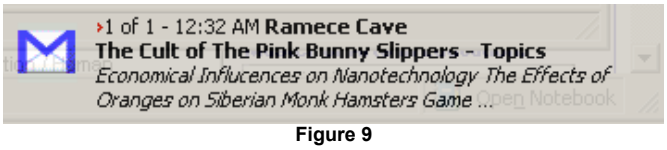

Figure 9

Sender	*Ramece Cave*
Subject	*The Cult of The Pink Bunny … Topics*

Recovered Message Content

```
..5%.i.o. ..Y...B....*......M"t....|.........h......u~.Q...W.K.
.9c. ;.2T....`...Q[@qc.......r.L..}t.s.......".pL...%.M~.Z..<..&
;.p^Y[e...Cn.....*i..D...v=.hg.>.......
X...2...0.Ry..2.1\...1..3.0p=7........I.].......Q...8'..]....U8...-.Z......'..
1.mp...'e5.=._....I6.....)L.N......::i...n...].E.%.^.RL...e.2........U..m3..-
u.e...?..W.D.;IP...@.K]op.bB....../..p.S....M.F...SqZ....x..H..=gR........0
{.Z....s....<..  ..K.......k'P...........3..T....N...........Mlm.......g.|4^.R"..O.|
```

Figure 10

Conclusion

With a simple modification to Gmail Notifier we are now able to receive message notifications and access Gmail over a secure connection. Depending on your environment and need for security this maybe an invaluable tool, or it can simply suffice as a quick hack just to see if it works. Remember this mod was achieved by following two simple rules:

Old School rules
Stay low, keep moving