Global Information Assurance Certification Paper

Privacy and Security Management in Internet Explorer 6:
A Consumer Guide

GIAC Security Essentials Practical Assignment
Version 1.4b, Option 1

Ken Creighton
March 6, 2004

Abstract

The founders of the Internet sought to develop a collaborative communications network capable of withstanding the devastation of nuclear war. Protocols developed were intended to enhance communication across independent diversified computing networks. The concepts of privacy and security were overshadowed by the objective to maintain communication in the face of nuclear war. Internet content such as cookies, Web Beacons, potentially inappropriate violent and/or pornographic Web content, hostile active content, and malware were beyond the initial vision of the Internet fathers.

The explosion of Internet growth in a few short years has changed the very nature of the Internet itself. No longer merely a means to facilitate communication in the midst of a nuclear war, the Internet has blossomed into a cultural phenomenon. With the booming growth of the Internet has come the inevitable exploitation of the emerging technology. Hackers, crackers, malware and Web sites are not only targeting academia and business with their nefarious activities; the home consumer is more often than not targeted for privacy and security exploitation. The home consumer can not afford to rely on others to protect privacy and security on their personal computers—proactive consumer measures are required. Internet Explorer 6 provides the home consumer with built in tools designed to layer personal defenses and protect privacy, thwart inappropriate Web content, and secure the Internet browsing experience.

"The Internet is a great way to get on the net."[1]
Senator Bob Dole

The Internet; the word rolls off the tongues of politicians, scientific and academic researchers, business users and home consumers alike. The current generation of children has never known life without the Internet; yet for many, the Internet has been an immersion in technological future shock. The humble beginnings of the Internet lie in the national paranoia fostered by the 'Cold War'. The Department of Defense sought to design a communications network which would be immune to natural and man made disaster—including nuclear war. The precursor of the Internet (ARPANet) was 'born' in 1969, when a wide area network was created by the United States Defense Advanced Research Project

Agency (ARPA).[2] UCLA and the Stanford Research Center were the first entities on ARPANet; followed by the University of Utah and UC Santa Barbara. This four node network linked academic and scientific researchers in a manner heretofore unimaginable. ARPANet allowed these pioneers to access mainframe computers not previously physically available to them due to geographic location. The concept of remote connectivity and collaboration was a reality.

In a few short years as new nodes were added, ARPANet became overused and congested. The military split off from ARPANet and created MILNet. A new means of computer communication and collaboration was sought. The National Science Foundation created NSFNet in 1985, based on the TCP/IP protocols established by ARPANet. NSFNet instituted a general purpose research network which would act as the backbone for connection of regional networks at each supercomputing site.[3] The growth of NSFNet was unexpectedly rapid, and quickly outgrew its initial research focus. The National Science Foundation began studies to plan for the transition of NSFNet to private industry. In 1994 a national commercial backbone was created by private industry. Regional NSFNet networks migrated to the newly created commercial backbone, ultimately resulting of the dissolution of NSFNet in1995.[4] With the establishment of a privately funded commercial backbone, the Internet has matured into a self supporting entity.

This abbreviated history of the genesis of the Internet demonstrates an important principle: the Internet was designed for collaborative research—not privacy or security. The modest four node ARPANet has given way to the modern Internet, with literally millions of connections being made simultaneously. With the advent of 'always on' high speed Internet connections, home consumers are now enjoying Internet access once reserved for government, military, academia and business entities. Along with the enjoyment of 'surfing the net' come the inevitable perils of utilizing an international network with limited regulations. Larger organizations have the financial ability to employ professional staff to secure their Internet presence and access. What about the home consumer? Who is protecting this large population of Internet users? High speed Internet access is a double edged sword; the convenience of instant access often fore shadows the integral need for security.

Is ignorance bliss? Certainly not when it comes to Internet security. The modern Internet is analogous to the 'wild west' frontiers of the United States in the mid to late nineteenth century. Limited regulation and laws often difficult, if not impossible to enforce across international boundaries, have shaped fertile grounds for nefarious activities and behavior. True, the Internet abounds with 'safe' surfing opportunity. However, each time the consumer connects to the Internet, you risk compromise by hackers and malware. These threats include but are not limited to: viruses, trojans, worms, hostile applets, spyware, tracking

cookies and Web bugs. Consumers have been lulled into a false sense of security through clever media presentations, advertisements and peer pressure. Consumers are often too quick to site the adage that 'attacks happen to the other guy, not me'. Unfortunately, without adequate layers of defense—defense in depth—the unprepared consumer may find he/she is the 'other guy'.

There are numerous inherent risks in utilizing an unprotected computer on the Internet. Maintaining the integrity and security of the Internet is the responsibility of each organization and /or individual who makes a connection. It is not the responsibility of the 'other guy'. This document is patterned to address the home Internet consumer, and to raise the level of awareness for the need of computer security. The principles of applying defense in depth to the home computer include:

- Application of virus protection with automatic updates
- Exercising caution with e-mail and attachments
- Maintenance of operating system patches and hot fixes
- Utilizing a firewall
- Spyware protection
- Adjusting Windows and registry settings for optimal security
- Backing up important data[5]

While these steps will not completely thwart the vast array of potential Internet attacks, they do represent integral components to securing the home computer and the Internet in entirety. There are a myriad of documents available providing a basal framework for instituting security on computers. Many of these compositions are too technical for the home consumer. It is a prerequisite of this document that the home consumer meets the minimum guidelines presented in the document: "Defense in Depth and the Home User: Securing the Home PC". (http://www.giac.org/practical/GSEC/Shauna_Munson_GSEC.pdf). The document presented here will build upon and extend the foundational principles of defense in depth, providing you the knowledge and means to protect your privacy and enhance security when browsing the Internet using Internet Explorer 6.

Microsoft Windows and the integrated Internet Explorer 6 browser are instruments commonly utilized by the home consumer when attached to the Internet. Certainly many privacy and security breaches may occur from alternate operating systems, Web browsers and applications. This document will serve to further define the principles of defense in depth, by enhancing the privacy and security knowledge of the home consumer. You will be introduced to tools allowing you to define and tighten privacy and security policies in the Microsoft Internet Explorer 6 browser. Internet Explorer 6 provides the home consumer opportunity to granularly determine the level of privacy and security desired by managing cookies; managing Internet content based on a ratings system; and

management of security zones for a safer Internet experience.

"You have zero privacy anyway. Get Over It."[6]
Scott McNealy – CEO, Sun Microsystems

An unsecured and under protected computer on the Internet provides finite to no privacy for the computer operator. The naive home consumer often gives limited thought to privacy concerns. Enthralled with the technology and fascination of the Internet, the home consumer may frolic on Web sites much as an eager child in an amusement park. The consumer may assume the Web site operator is protecting the user's privacy—if thought is given to the matter at all. The contrary is more often than not the truth. Web site operators frequently have a vested interest in tracking information concerning visitors to their Web sites. A common methodology employed by Web sites to track visitors is the use of 'cookies'. A cookie is a text file that a Web site server creates on a visitor's computer; often without the knowledge or consent of the Web site visitor. The cookie allows the Web site to store information gathered about the visit to the site, and to retrieve the information during a subsequent visit. Internet Explorer 6 gives the consumer options to manage cookies. The options range from accepting all cookies, to rejecting all cookies.[7] Accepting all cookies indiscriminately may jeopardize ones privacy, while rejecting all cookies may create difficulties in viewing select Web pages. Prior to making management choices concerning cookies, an exploration of cookie types is necessary. Cookies can take several forms including: first party cookies, third party cookies, tracking cookies, session cookies, persistent cookies and Web beacons.

- First Party Cookies: A first party cookie is generated and used by a website the consumer is currently visiting. The cookie (a simple text file) contains information about the consumer that the Web site uses while the guest remains at that Web site. Only the Web site which created the cookie can access and read the cookie. The cookie may contain logon information; once you have registered at a web site the cookie remembers the information so future registration at that site is not necessary. The cookie may store preference data. Perhaps you have set up a home page with your ISP. The cookie remembers your choices for stock quotes, news quotes, weather reports etc.—the home page looks the same every time you visit. First party cookies may be session or persistent, and are often designed with the goal of convenience for the consumer.

- Third Party Cookies: A third party cookie is used by a site other than the Web site the consumer is currently visiting. These cookies are often found in banner advertisements. Third party cookies are often designed to target advertisements to the consumer based on Web sites visited and ads clicked on when visiting Web sites. A third party cookie is frequently also a tracking cookie.

- Tracking Cookies: A tracking cookie gathers information about the consumer as you visit different pages within a Web site, or as you visit different Web sites. A first party tracking cookie gathers information from various pages within a single Web site. This allows the Web site to remember who you are as you change pages within the Web site. Only the Web server from that site may access the cookie. A third party tracking cookie has the ability to track your actions from Web site to Web site. Cookies placed on your hard drive from companies such as HitBox and Doubleclick can be read and modified from any Web site which contains an advertisement from these companies. The goal of third party tracking cookies is to target personalized advertisements to the consumer.

- Session Cookies: A session cookie is a temporary text file placed in memory, not on your hard drive.[8] The cookie is removed from your hard drive when you close the Internet Explorer browser. A session cookie allows the Web site to remember who the visitor is and may allow the Web site to modify pages as you surf within the Web site. No information about you or your visit is retained by the Web site.

- Persistent Cookies: A persistent cookie is a text file placed on your hard drive by a Web server. The cookie remains on your hard drive until it is erased or the cookie expires. Persistent cookies contain an expiration value which specifies the lifetime of that cookie.[9] The persistent cookie contains information about the consumer which can be accessed by the generating Web server every time you visit that particular Web site. The cookie is no longer available or readable by the Web server once the expiration date has been met.

- Web Beacons: Web Beacons, also known as Clear GIF's and Web Bugs, are not actually cookies. They are however used in combination with cookies. A Web beacon is often a small transparent graphic image that is placed on a Web site which is used to monitor the behavior of the consumer visiting that Web site.[10] Web Beacons, which are typically used by third parties, have the ability to send information about the Web site visitor including your IP address (a numbering system which identifies your computer on the Internet), browser type, the time and how long you visited the Web page, as well as accessing information from a previously set cookie.

The Internet Explorer 6 browser provides consumers the ability to manage cookies, delete cookies, and specify cookie handling preferences for specific Web sites based on Privacy Policies. Accepting all cookies may jeopardize your privacy and allow tracking of your surfing behavior. Rejecting all cookies may interfere with the properties of certain Web sites and how Web pages are

displayed in your browser; in certain instances the page may not be displayed at all. Proper management of Web cookies will optimize your privacy and enhance Web page viewing. Cookie management is performed from the Privacy tab in the Internet Options menu (Figure 1).

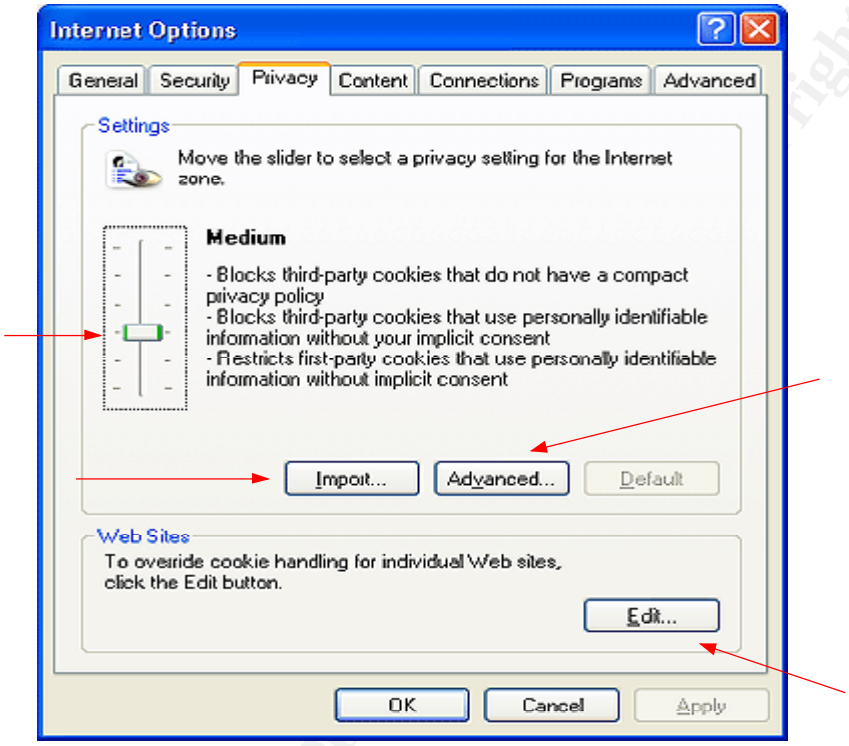

Figure 1

To navigate to the Internet Options menu:

- On your Internet Explorer browser toolbar click on the 'Tools' menu.
- Click 'Internet Options…'
- Click the tab marked 'Privacy'.
- Using the slide bar you can choose your privacy options regarding first and third party cookies. Sliding the bar to the bottom is the least restrictive (accept all cookies), while sliding the bar to the top is the most restrictive (reject all cookies).

The six options the privacy slider bar provides is often enough management control for the home consumer—the default setting is Medium. Internet Explorer allows greater control of cookie management. To override cookie settings selected with the slider bar, clicking on the Advanced button (Figure 1) brings you to the Advanced Privacy Settings menu (Figure 2).

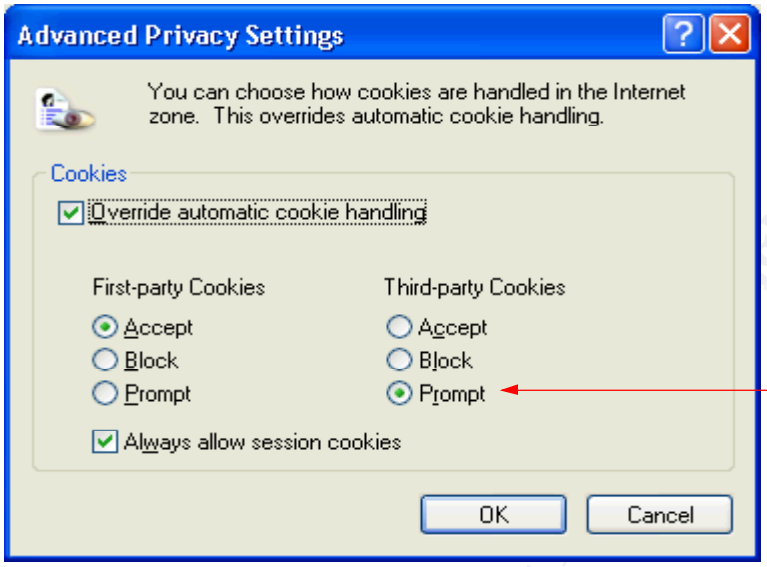

Figure 2

Selecting 'Override automatic cookie handling' allows you to specify exactly how the browser will manage cookies. Management decisions for first and third party cookies are independent of one another. You may choose to accept or block all cookies; the third alternative will prompt you with the Privacy Alert menu when a cookie is encountered by your browser (Figure 3).

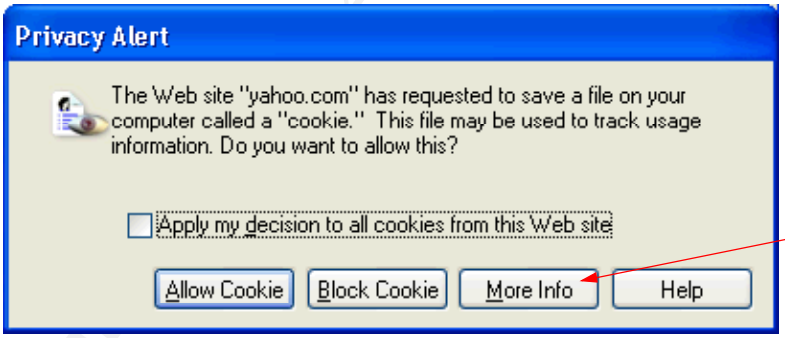

Figure 3

You may choose to Allow Cookie or Block Cookie, as well as apply your choice to all cookies from the particular Web site. Alternatively, you may request more Information about the cookie. By clicking the More Info button (Figure 3), a wealth of information regarding the cookie is obtained (Figure 4).

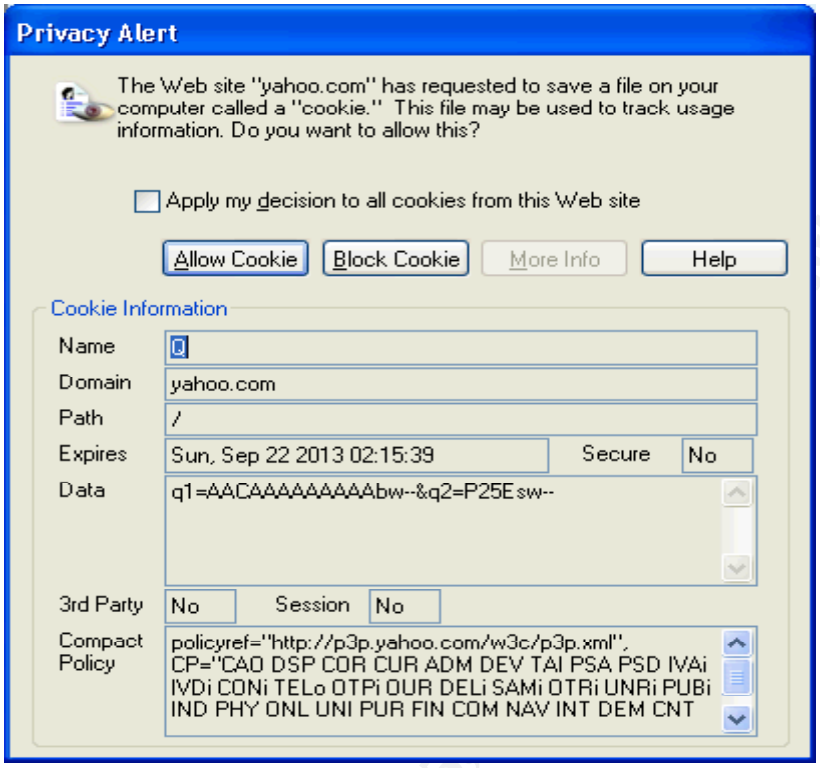

Figure 4

The Privacy Alert popup menu provides specific information about the cookie. This information enables the consumer to make an informed decision before allowing or blocking the cookie. The data in the Cookie Information field (Figure 4) includes: Name, which is simply the name the cookie was given by the programmer. The Domain indicates who (what Web server) the cookie is coming from. The Path refers to folders and files on the Web server, and tells the browser to transfer the cookie data to the Web server whenever the browser accesses one of these folders or files. Secure tells you if the information in the cookie will be sent encrypted when the cookie is accessed. Expires tells you when the cookie on your hard drive is no longer readable by the Web site. The Data field most often contains code only readable by the Web server. The information in this field may include personal data, user name and password, date and time, etc. The 3rd Party entry indicates if the cookie is from a 3rd Party. If No is in the box, the cookie is a First Party cookie; if Yes is in the box, the cookie is a 3rd Party cookie. The Session field indicates if the cookie is a Session cookie (box indicates Yes), or if the cookie is Persistent (box indicates No). Finally, the Compact Policy field contains a sequence of browser readable tags which identify the privacy policy in effect.

This information provides the consumer the ability to make informed decisions before blocking or allowing a cookie. Choosing Prompt from the Advanced Privacy Settings menu (Figure 2) comes with a price: many consumers find the pop up boxes to be an annoyance. One way to limit the pop up boxes is to accept all first party cookies (often designed for consumer

convenience), while blocking or being prompted for third party cookies (often designed for targeted advertisement and/or consumer tracking). Choosing to block third party cookies will also block Web Beacons. The Web Beacon will still record an anonymous visit to the Web site; however no personal information will be transmitted.[11]

The Privacy tab of the Internet Options menu (Figure 1) also allows the importing of an Internet Explorer privacy preferences file. This file is a template predefining the privacy options for the browser, overriding all default and custom privacy choices. This option is most often utilized by Administrators responsible for managing privacy options on a large numbers of browsers, and is not recommended for use by the home consumer.

A persistent cookie is a text file stored on your hard drive, which remains on the hard drive even after the browser has been closed. A cookie may contain any information you provided to a web site, including: your name and address, credit and bank card numbers etc. Cookies may be viewed by anyone with access to your computer with an editor program such as Notepad.exe. Managing the cookies on your computer provides an added layer of privacy defense when online. How about those persistent cookies? What about protecting the private data that may be stored in one or more cookies? Internet Explorer 6 gives you the means to delete all cookies from the hard drive. This option provides even greater defense in depth by protecting your confidential information when you are offline. Cookie deletion is performed from the General tab in the Internet Options menu (Figure 5).

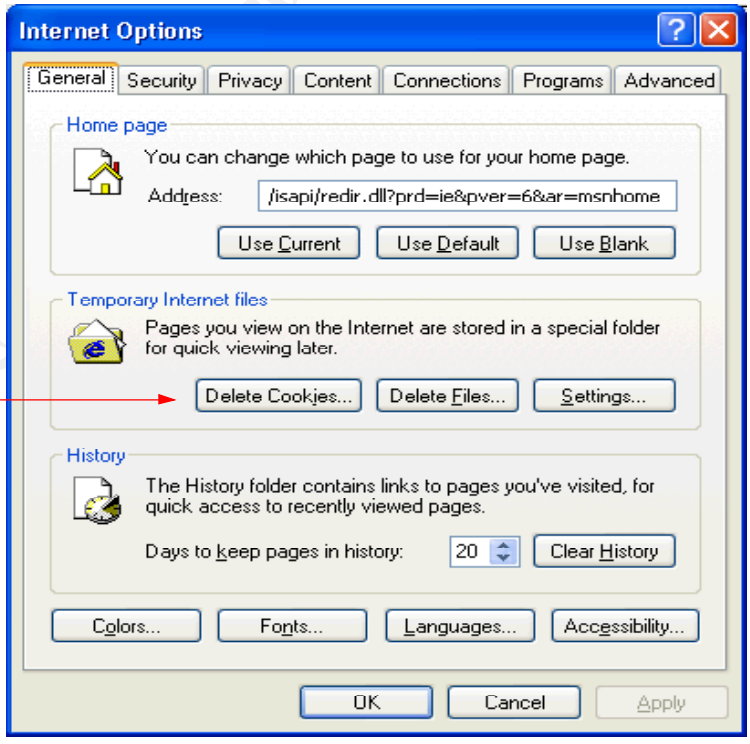

Figure 5 Cookies are stored in a folder on your hard drive called Temporary Internet Files. Choosing the Delete Cookies… button will erase the cookies stored in the Temporary

Internet Files directory (Figure 6).

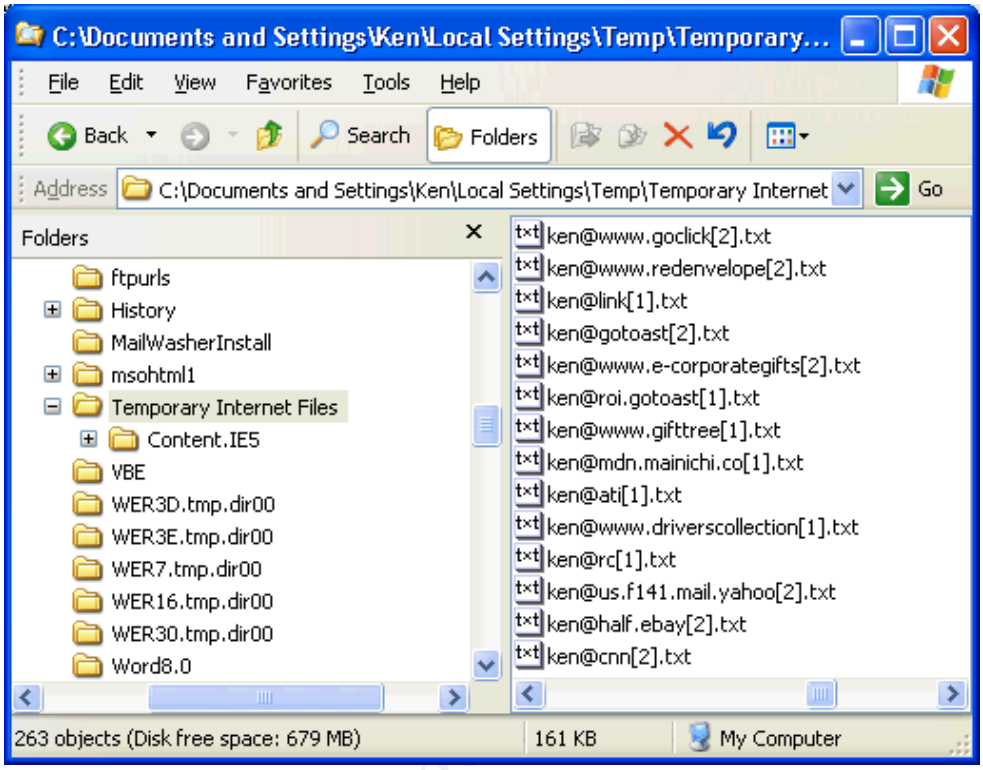

Figure 6

Remember, deleting the cookies from your hard drive may require entering usernames, account numbers etc when visiting Web sites which previously stored this information in a persistent cookie on your hard drive. Does this minor inconvenience outweigh your desire for privacy? You be the judge.

Cookies may also be managed by Web site: you may choose to allow or block all cookies from a particular Web site. Web sites which comply with the P3P (Privacy Preferences Platform) standards for data privacy provide the browser with a machine readable Privacy Policy. (A human readable privacy policy is typically provided by P3P enabled Web sites. To view the privacy policy for a particular Web site you will need to visit the site and find the link to their privacy policy.) A privacy policy discloses how a Web site will manage and utilize data it has collected from consumers. A P3P enabled browser—Internet Explorer 6 is P3P enabled—is able to read the Web sites privacy policy and compare your privacy preferences with the privacy policy of the Web site[12]. If there is a match, the contents of the Web page will be displayed. If there is not a match, you will be prompted to decide whether or not to proceed.[13]

If there is a Web site you implicitly trust, or one you implicitly do not trust, you can choose to accept or block all cookies from a particular Web site by overriding your defined privacy preferences. To override how cookies are handled by individual Web sites, choose the Edit… button on the Privacy tab

page of Internet Options (Figure 1). This will display the Per Site Privacy Actions menu (Figure 7).

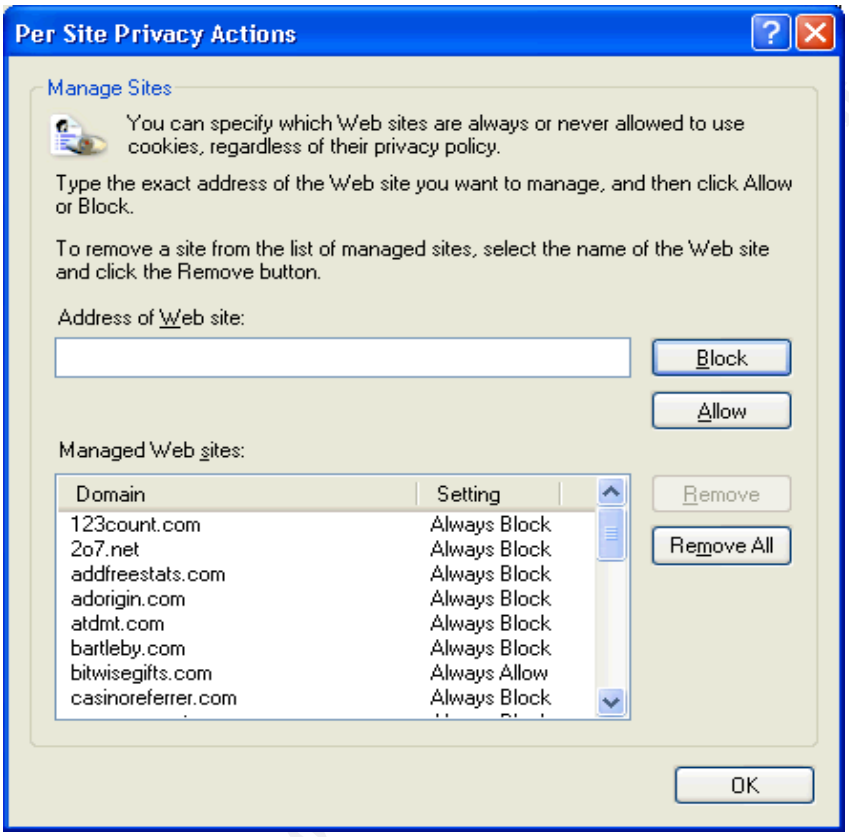

Figure 7

To add a Web site type in the exact address, then choose to Block or Allow all cookies by choosing the appropriate button. Managed Web sites may be removed by highlighting the Domain name and choosing the Remove button; the Remove All button will remove all Managed Web sites without highlighting the Domain names.

Managing privacy on the Internet is up to the individual consumer. As you have seen, Web sites will not manage privacy for you. Many Web sites developed poor reputations for the manner in which they handled data collected on consumers. The data privacy standards set forth by the P3P is designed to protect consumers while allowing the Web site to gather consumer information and effectively conduct commerce. Web sites use a variety of cookies including Web Beacons to gather your data. Keep in mind that a cookie is not a program or an application that can read your hard drive or e-mail. A cookie is simply a text file containing information provided by you or your browser. Effective cookie management provides another layer in the practice of defense in depth. While cookie management enhances your privacy, Internet Explorer allows you to extend your privacy enhancements with Content Ratings.

"Never trust a computer you can't throw out a window."[14]
Steve Wozniak – Apple Computer Co-founder

Cookie management allows you to control one aspect of your online privacy. Many consumers find Web content with raw language, nudity, sex and violence is not only inappropriate for their children and personally offensive, but is also an invasion of their privacy. Internet Explorer provides a mechanism for filtering potentially offensive and privacy invading content. The Content Advisor menu of Internet Explorer 6 allows you to modify content rating settings; establish and change the Supervisor password to protect these modified settings; modify select user options; select an alternate ratings system organization; and approve or disapprove of specific Web sites regardless of content rating. To navigate to the Internet Options menu (Figure 8):

- On your Internet Explorer browser toolbar click on the 'Tools' menu.
- Click 'Internet Options…'
- Click the tab marked 'Content'.

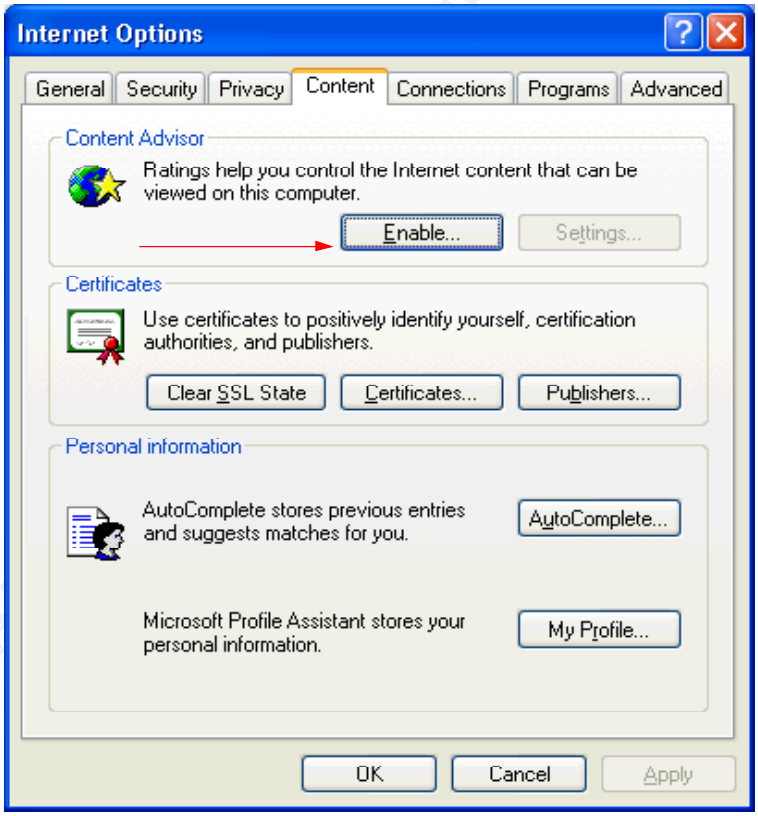

Figure 8

Clicking the Enable…button (Figure 8) will spawn the Content Advisor menu (Figure 9). The Content Advisor menu allows you to determine content ratings, set the supervisor password, and approve or disapprove specific Web sites regardless of content rating.

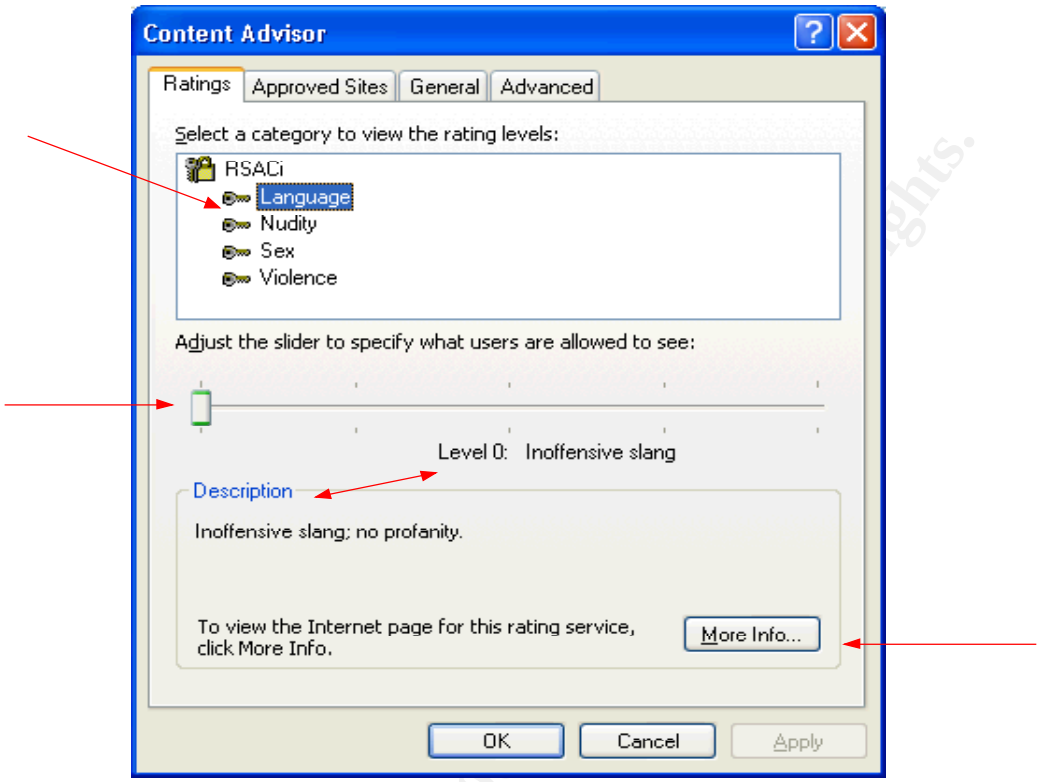

Figure 9

The Ratings tab of the Content Advisor menu allows you to set the ratings level for content containing Language, Nudity, Sex, and Violence. To set the rating level, highlight the category you wish to modify, and then move the slider bar from Level 0 to Level 4, then click OK. As the levels change, a description of each level is provided (Figure 9). The following table identifies the permissions of each Level, for each content option (Table 1):

Ratings Levels	
Language	This Level Permits
Level 0: Inoffensive slang	Inoffensive slang; no profanity.
Level 1: Mild expletives	Mild expletives or mild terms for body functions.
Level 2: Moderate expletives	Expletives; non-sexual anatomical references.
Level 3: Obscene gestures	Strong, vulgar language; obscene gestures. Use of epithets.
Level 4: Explicit or crude language	Extreme hate speech or crude language. Explicit sexual references.
Nudity	This Level Permits
Level 0: None	No nudity.
Level 1: Revealing attire	Revealing attire.

Level 2: Partial nudity	Partial nudity.
Level 3: Frontal nudity	Frontal nudity.
Level 4: Provocative frontal nudity	Provocative display of frontal nudity.
Sex	This Level Permits
Level 0: None	No sexual activity portrayed. Romance.
Level 1: Passionate kissing	Passionate kissing.
Level 2: Clothed sexual touching	Clothed sexual touching.
Level 3: Non-explicit sexual touching	Non-explicit sexual touching.
Level 4: Explicit sexual activity	Explicit sexual activity.
Violence	This Level Permits
Level 0: No Violence	No aggressive violence; no natural or accidental violence.
Level 1: Fighting	Creatures injured or killed; damage to realistic objects.
Level 2: Killing	Humans or creatures injured or killed. Rewards injuring non-threatening creatures.
Level 3: Killing with blood and gore	Humans injured or killed.
Level 4: Wanton and gratuitous violence	Wanton and gratuitous violence.

Table 1

The Ratings Levels have been established by an independent ratings board. Internet Explorer by default uses the Recreational Software Advisory Council (RSACi) ratings guidelines. Information on the rating service may be obtained in Internet Explorer 6 by clicking on the More Info… button (Figure 9).

Once you have selected the ratings level (0 – 4) for each selected category—Language, Nudity, Sex, and Violence—click the Apply, then the OK buttons. When the OK button has been clicked, the Create Supervisor Password menu is displayed. You must enter a password, and re-enter the same password for verification before the ratings levels are applied. You may provide an optional hint in the Hint: text box. The hint should be a word, a series of words or a phrase, which will assist to remind you of the password at a later date. The Create Supervisor Password menu is illustrated in Figure 10. Once the Supervisor Password has been set, no changes are allowed to be made in the Content Advisor menu without first providing the Supervisor Password. It is advisable to close and re-open Internet Explorer once content ratings have been established to prevent viewing of recently visited Web pages which may not meet the content ratings criteria.

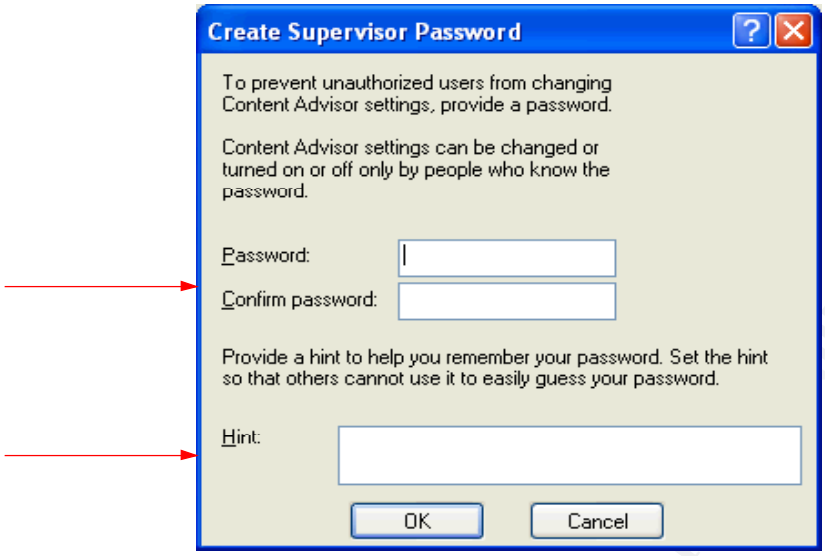

Figure 10

Note the changes to the Content tab of the Internet Options menu once the Supervisor Password has been set (Figure 11). The Enable… button has been replaced by the Disable… button. The Settings… button previously grayed out is now available.

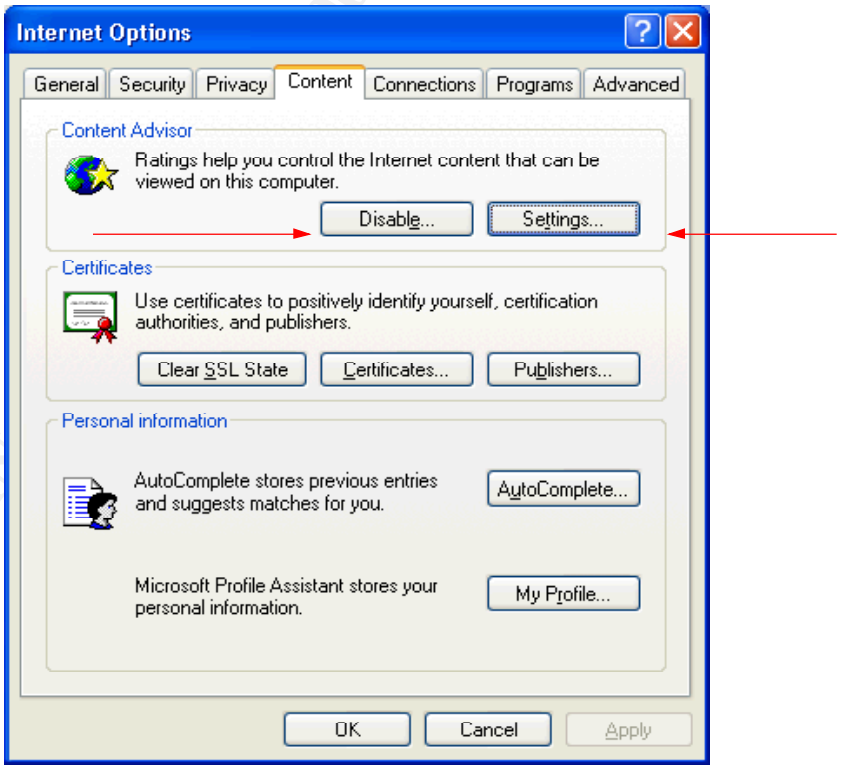

Figure 11

Keep in mind that you will be required to enter the Supervisor Password (Figure 12) if you click either the Disable… or Settings… buttons to make

modifications. Notice the hint you previously provided for the Supervisor Password is displayed.

Figure 12

If the Supervisor Password is compromised, or you desire to change the password for any reason, clicking the General tab in the Content Advisor menu, will spawn a menu providing for further modifications (Figure 13).

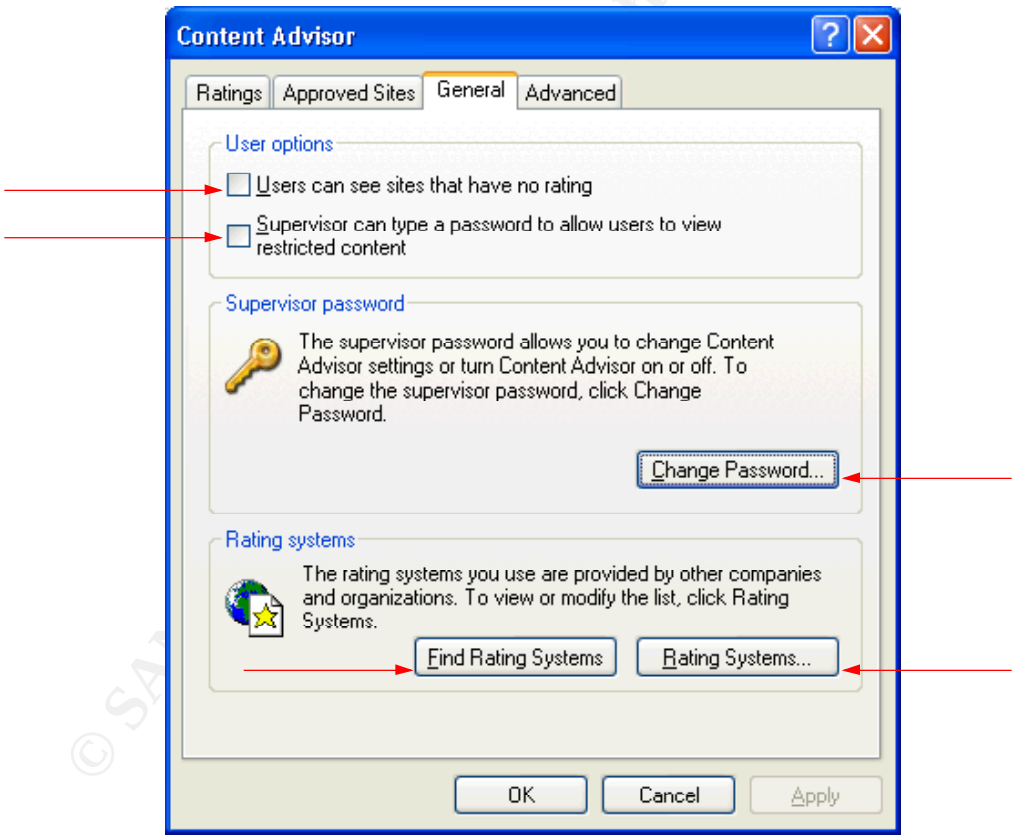

Figure 13

Clicking the Change Password… button on the General tab will open the Change Supervisor Password menu (Figure 14):

Figure 14

To change the Supervisor Password you must first supply the old password by typing the password in the Old password: text box. Enter the new Supervisor Password in the New password: text box, and retype the password in the Confirm new password: text box. If you prefer, enter a new hint which will remind you of the new password. Click the OK button. A pop-up menu will confirm the password change.

Internet Explorer 6 gives the consumer two user options that can be managed from the General tab of the Content Advisor menu (Figure 13). Web sites are not required to provide a rating for the content of the site—this is strictly voluntary. A Web site must register with a Ratings System to rate the content of the site. Internet Explorer uses the Recreational Software Advisory Council (RSACi) ratings guidelines by default. If you have defined ratings levels, Internet Explorer reads 'labels' in the HTML code to determine the rating of the content. A label is HTML code inserted by the Webmaster which defines the content rating. When you browse to a Web site, Internet Explorer reads the code and labels. If the Web site has registered with the RSACi and is using the appropriate labels, Internet Explorer will display or deny the displaying of the Web site based on the rating levels you have set.

If a Web site does not have a rating, the Web site will not be displayed. A Content Advisor pop-up menu (Figure 15) will be displayed alerting you that the page is not viewable as the page does not have a rating. The pop-up menu provides several choices for viewing the Web page. Each of these options requires the Supervisor Password to be entered to override the ratings levels. With the Supervisor Password you may elect to Always allow this Web site to be viewed; Always allow this Web page to be viewed; and Allow viewing this time only. Clicking the radio button of your choice, entering the Supervisor Password and clicking the OK button, will display the unrated Web page or site. Alternatively, clicking the Cancel button will return the user to the Web page most recently visited.

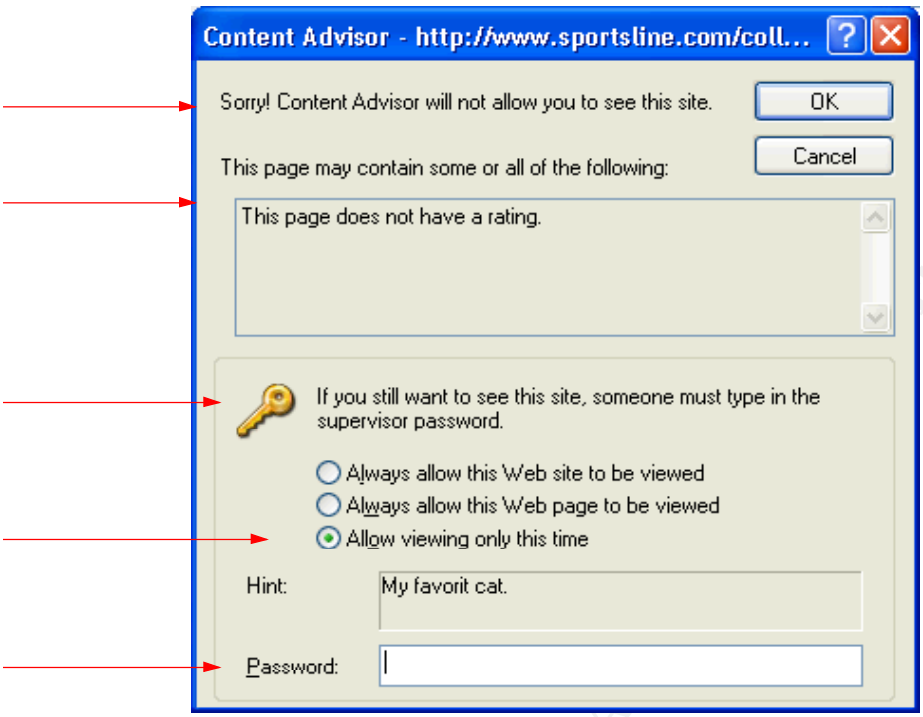

Figure 15

Clicking the OK button without providing the Supervisor Password results in a Content Advisor pop-up menu being displayed informing the user that "The password you typed in is incorrect" and Web page will not be displayed (Figure 16).

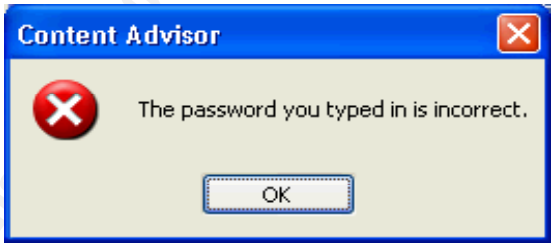

Figure 16

The setting which results in unrated Web pages and sites not to be displayed may be overridden on the General tab of the Content Advisor menu (Figure 13). To override the setting place a checkmark in the box: Users can see sites that have no rating.

The second user option which may be managed allows entering the Supervisor Password which permits viewing of restricted content. To allow the Supervisor Password to override the content restriction, navigate to the General tab of the Content Advisor menu (Figure 13). Placing a checkmark in the box: Supervisor can type a password to allow users to view restricted content will result in a Content Advisor pop-up menu being displayed. The menu explains why the content is restricted and provides for allowing the Web site or Web

page to always be viewed, or to be viewed only this time. Clicking the appropriate radio button and entering the Supervisor Password are required to override the content restrictions (Figure 17).

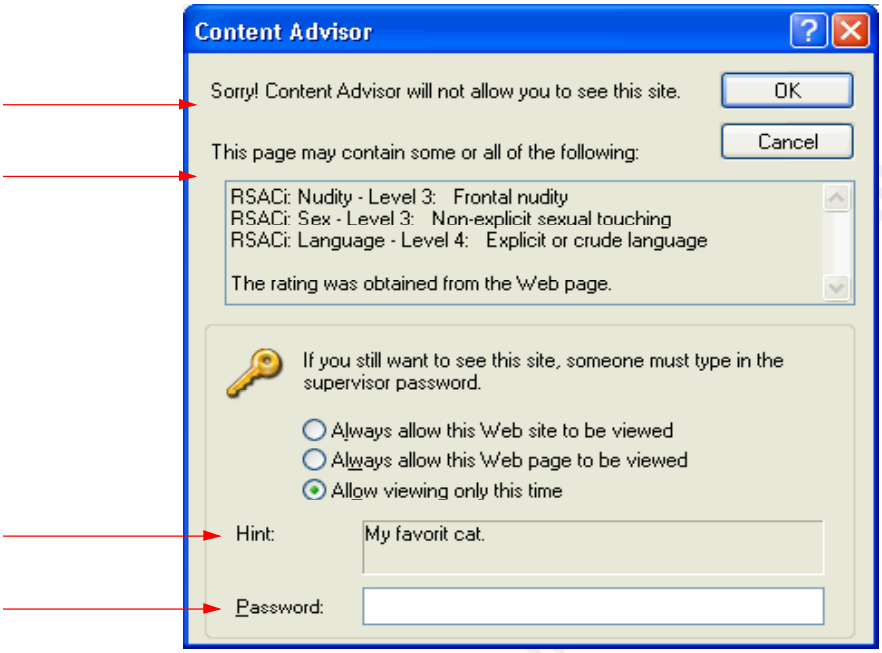

Figure 17

When you navigate to a Web site that is not rated by RSACi, a Content Advisor pop-up menu will be spawned indicating the Web page can not be displayed as the Web page has been rated by a system not installed on your computer (Figure 18).

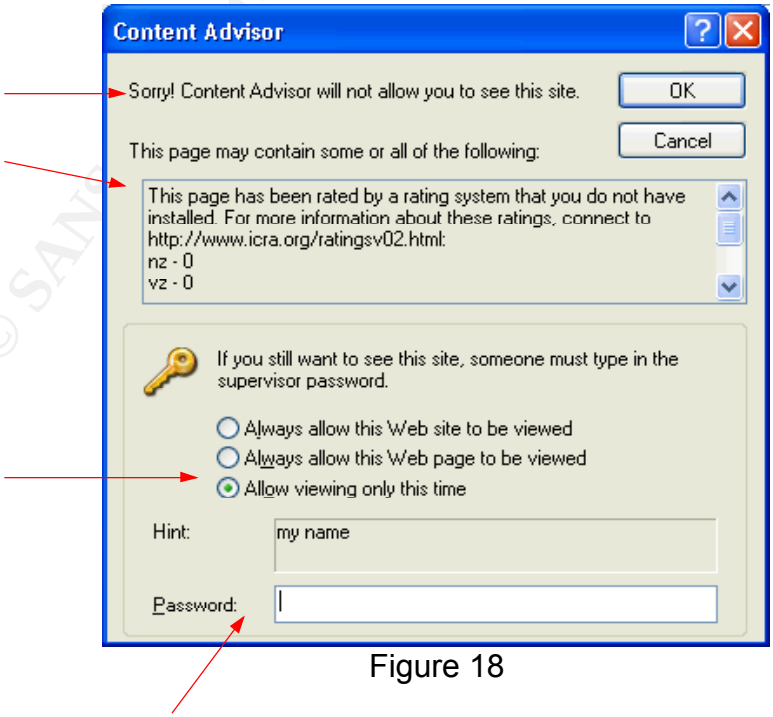

Figure 18

The consumer has the option to override the viewing restriction by clicking the appropriate radio button, entering the Supervisor Password, and clicking the OK button.

Internet Explorer supports the addition of alternate Ratings Systems in addition to the default system RSACi. Internet Explorer permits the addition of The Internet Content Rating Association (ICRA) and the SafeSurf Rating Standards.[15] Hyperlinks to these ratings organizations home pages are available by clicking the Find Rating Systems button on the General tab of the Content Advisor menu (Figure 13). To install ICRA or SafeSurf, you must download the .rat file for the ratings system you wish to add. The .rat files are available for download from ICRA and SafeSurf at their Web sites. On Windows 95, 98 and ME, save the .rat file to your C:\WINDOWS\SYSTEM folder; on Windows NT/2000/XP, save the file to C:\WINDOWS\System32[16] (Figure 19).

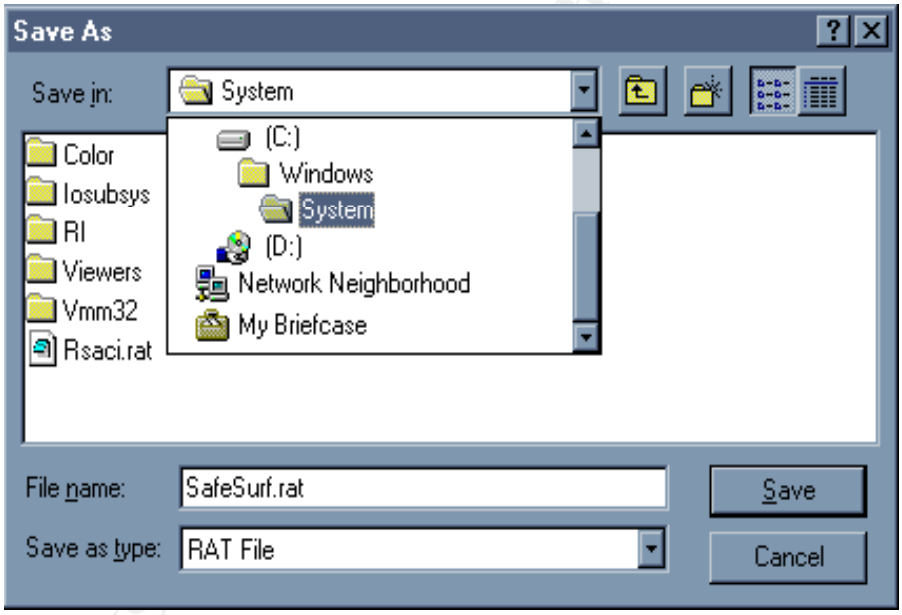

Figure 19[17]

Once you have downloaded the .rat file to your computer, you must add the ratings system to Internet Explorer. Click on the Rating Systems…button on the General tab of the Content Advisor Menu (Figure 13) to add a rating system. Clicking this button will display the Rating Systems pop-up menu (Figure 20).

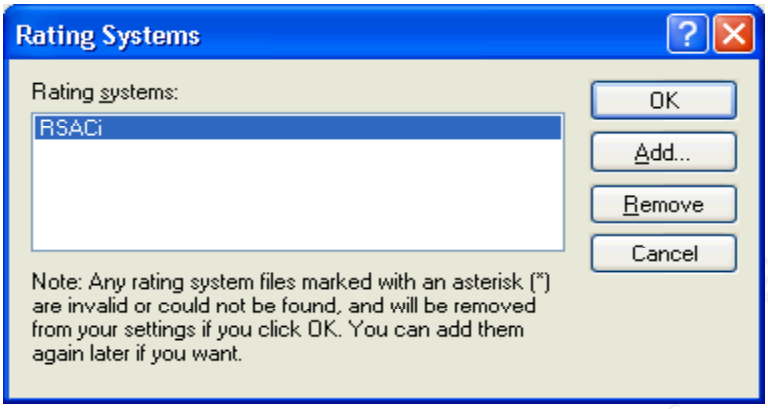

Figure 20

To add a rating system click the Add… button; this will spawn the Open ratings system file menu (Figure 21).

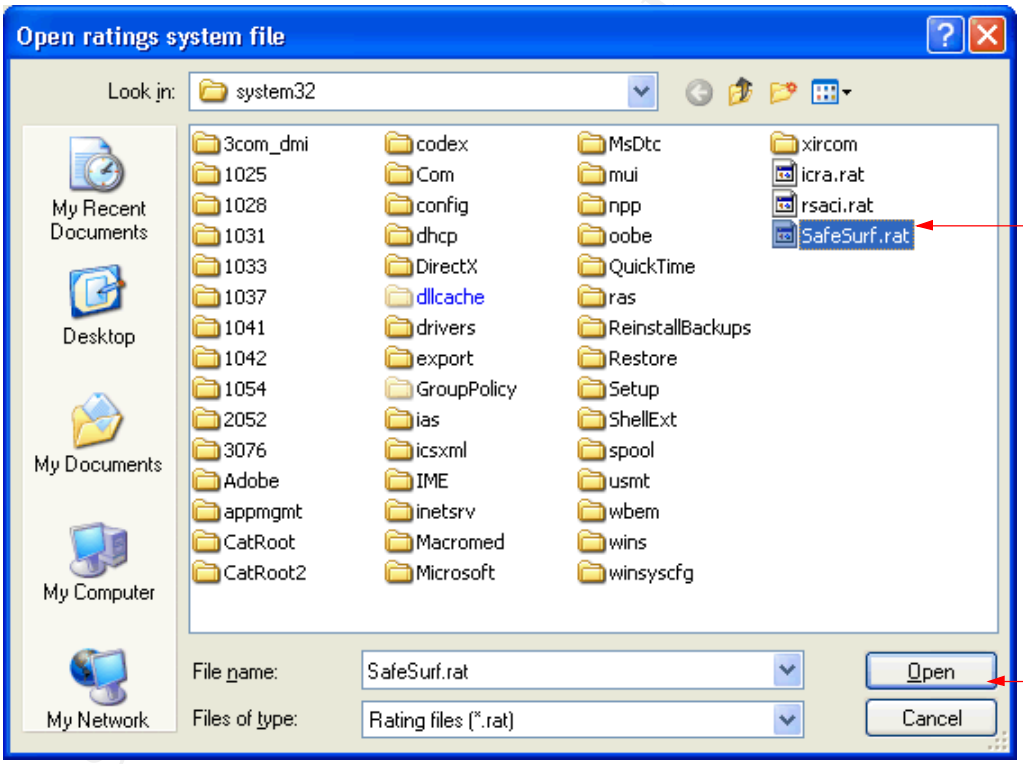

Figure 21

Click on the .rat file for the ratings system you want to add to Internet Explorer 6. The .rat file becomes highlighted. Once highlighted, click the Open button. This will add the ratings system you chose to Ratings System menu selection (Figure 22).

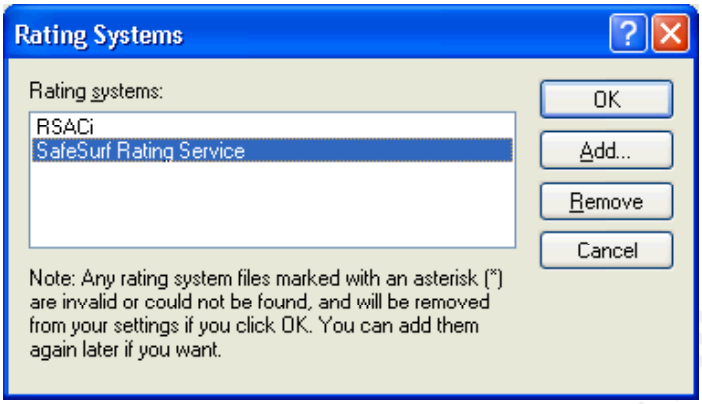

Figure 22

To complete the process of adding the ratings system, click the OK button. Alternatively, a ratings system may also be removed from Internet Explorer by highlighting the name of the ratings system on the Rating Systems menu, then click the Remove button followed by the OK button. To verify the ratings system has been added to Internet Explorer, click on the Ratings System… button on the General tab of the Content Advisor menu (Figure 23).

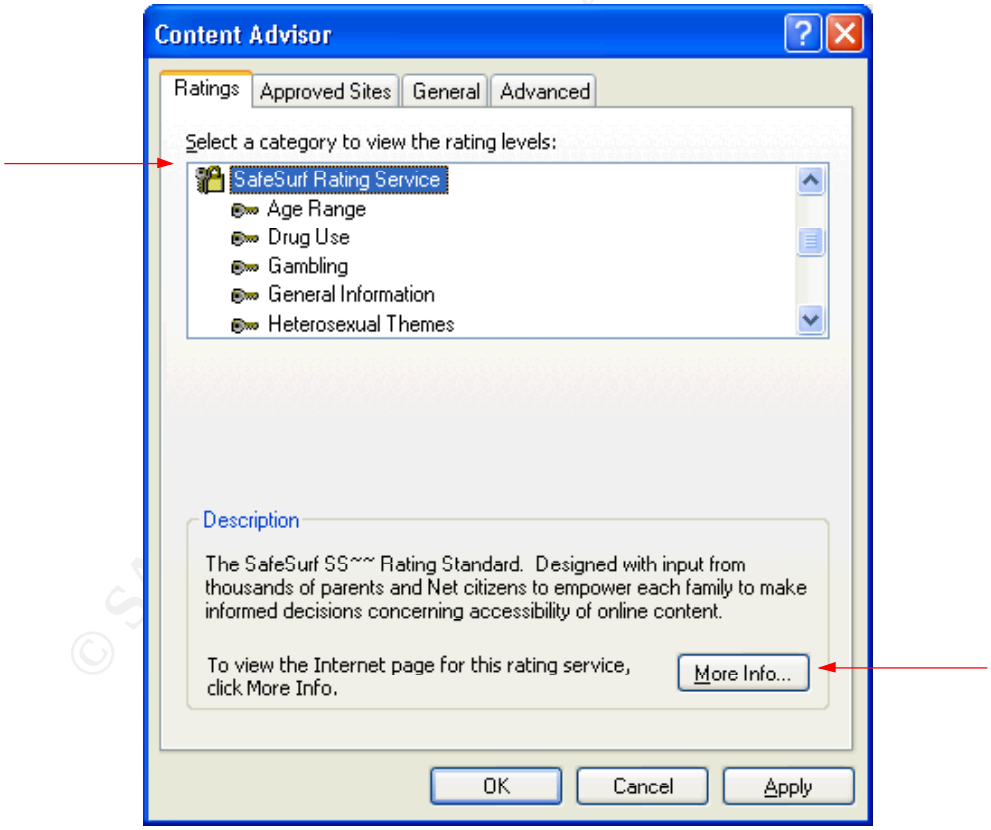

Figure 23

It is important to note that additional ratings systems beyond the default RSACi contain different rating categories and alternate means to set and

manage the ratings. Each ratings system installed must be configured independently by the consumer. Configuring additional ratings systems is an advanced topic beyond the scope of this discussion. Information on configuring additional ratings systems may be obtained by highlighting the name of the ratings system and clicking the More Info… button.

Ratings systems can be a valuable tool in providing a depth of defense to protect a consumer from potentially offensive content, and aid in protecting privacy. However, you may discover the ratings system schema is too restrictive or permissive. It is possible in Internet Explorer 6 to grant a Web site (or Web sites) permission to always be displayed, or to restrict a Web site (or Web sites) so it is never displayed, regardless of how the Web site may be rated. Individual Web site settings are made on the Approved Sites tab of the Content Advisor menu (Figure 24).

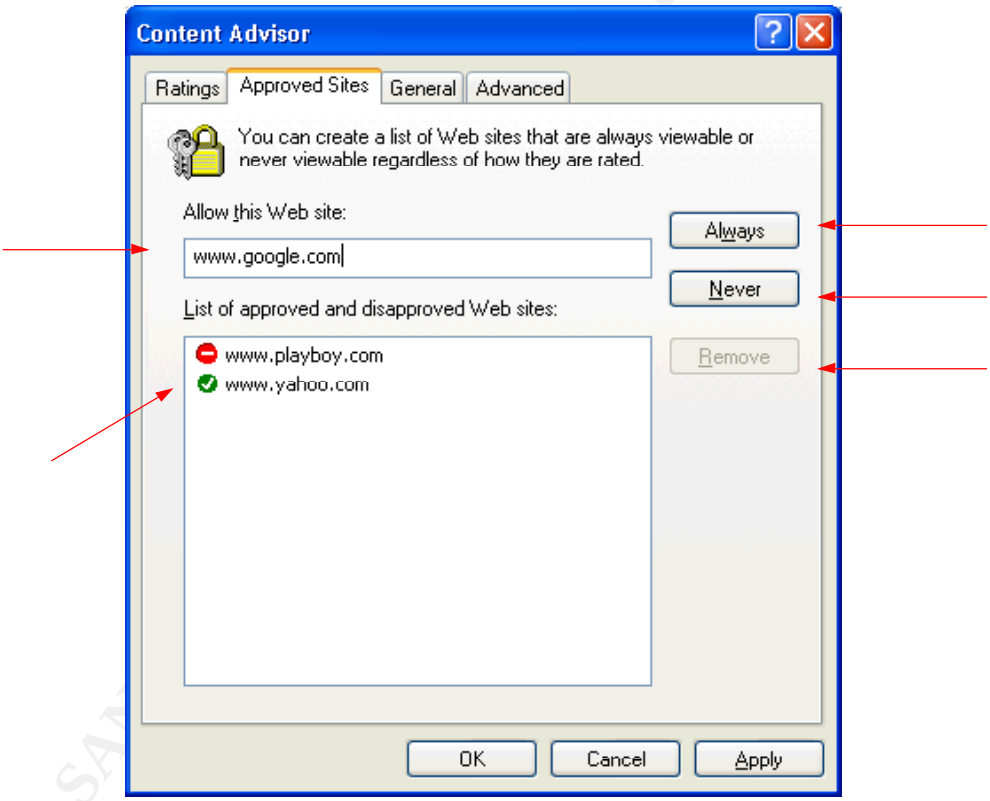

Figure 24

To add Web sites to the Approved Sites list, type the Web site address in the Allow this Web site: text box. To always allow the Web site to be viewed, click the Always button, then OK; to prevent the Web site from being displayed click the Never button, then OK (Figure 24). You will then be prompted by the Create Supervisor Password pop-up menu if not previously set; alternately you will be prompted to enter the Supervisor Password you previously established. These settings override any ratings you may have set. Web sites always and never allowed to be viewed are shown in the List of approved and disapproved Web

sites:. Approved Web sites are shown with a green circle surrounding a white check mark. Disapproved Web sites are displayed with a red circle surrounding a white dash. To remove a Web site from this list, highlight the chosen Web site and click Remove, then OK (Figure 24). The Remove button will become available once a Web site selected for removal has been highlighted.

When anyone attempts to access a disapproved Web site, the Web site will not open and a Content Advisor menu will be displayed informing the user that the Web page can not be displayed and why (Figure 25). Unlike content ratings, disapproved Web sites can not be overridden by entering the Supervisor Password.

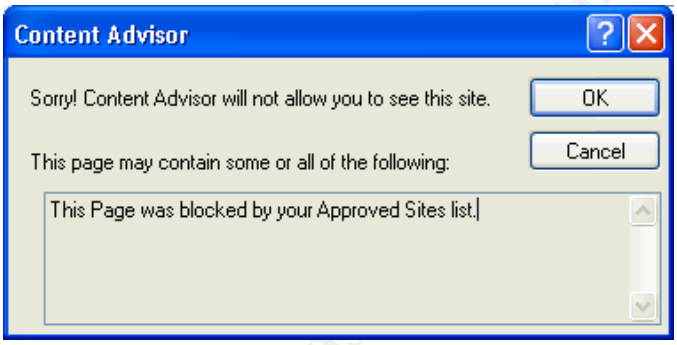

Figure 25

The Content Advisor menu provides the consumer with a variety of tools to enhance privacy and manage potentially offensive material. Internet Explorer provides the consumer another tool to enhance defense in depth and manage browser security. Internet Explorer security settings are managed by Security Zones.

"The user's going to pick dancing pigs over security every time."[18]
Bruce Schneier – Security Technologist & Author

Internet Explorer 6 provides the consumer the options to granularly manage privacy and security settings. You have been introduced to regulating privacy through cookie and content rating management. Security management is performed with Internet Explorer Security Zones. Security Zones have been designed to protect the consumer from downloading potentially harmful active content from the Internet to their hard drives. Active content is content on a Web page which is interactive; dynamic; Java script applications; embedded objects; streaming audio and video; or ActiveX applications.[19] The following offers an explanation of active content:

- Interactive content would include for example, Internet polls or opt-in features such as the ability to request email from a specified Web site.
- Dynamic content is content that changes each time it is viewed. Examples include time of day, weather or stock tickers and animated

GIF's.

- Java script is a programming language which enhances the interactive and dynamic components of a Web page. Java script allows for performing calculations, playing games, adding special effects to a Web site and more.

- Embedded objects are files that can be played, displayed, executed, or interacted with on a Web page. Examples of embedded objects include multimedia files, documents in special file formats, or small programs.

- Streaming audio and video allows the browser to play the audio or video file before it is completely downloaded. This saves considerable time as audio and video files can be quite large.

- ActiveX applications (or ActiveX controls) is a means to distribute software via the Internet. Internet Explorer can automatically download and execute ActiveX controls. Examples include scrolling marquees, pull-down menus, and interactive graphics. ActiveX controls may be signed or unsigned. When an ActiveX control is signed, the software developer certifies the software is free from viruses and other harmful components. An unsigned ActiveX control offers no such certification.

Security Zones allow you to directly control the level of security for Web content. Internet Explorer provides five predefined zones: My Computer Zone; Local Intranet Zone; Trusted Sites Zone; Restricted Sites Zone; and Internet Zone.

The My Computer Zone is hidden from you in Internet Explorer. The zone contains files from your computer. Configuring the security settings in this zone requires a special tool and is recommended only for professional administrators of large networks. These are advanced settings not applicable to the home consumer.

The Local Intranet Zone can be configured by the home consumer through the Internet Options menu of Internet Explorer; however, this zone is intended to be configured by system administrators using advanced tools. The sites in this zone, typically on a Local Area Network (LAN), should be behind a firewall and set up in conjunction with proxy servers. Though you may adjust the security settings for this zone, configuring the zone requires detailed knowledge of your network, proxy server and firewall.[20] The Local Intranet Zone contains Web sites that bypass the proxy server; the site names do not have periods; and network connections which have been established with a Universal Naming Convention (UNC) path. This security zone level is set to Medium-low by default.

The Trusted Sites Zone by default contains no Web sites and the security zone level is set to Low. You add sites to this zone with active content that are

believed to be safe. Web sites added to the Trusted Sites Zone should be established sites and companies you have confidence in, and you believe downloaded files from these sites will not harm your data or computer. Assigning a Web site to the Trusted zone allows the site to perform a wide range of options, and results in fewer prompts to the consumer for security setting decisions. It is strongly suggested that Hypertext Transmission Protocol, Secure (HTTPS:) be used, or otherwise ensure connections in this zone are secure.[21]

The Restricted Sites Zone contains no Web sites, with the security zone level set to High by default. Sites added to this zone are sites with active content you do not trust; and you believe downloaded files from these sites will harm your data or computer. This zone contains Web sites that are not in the My Computer or Local Intranet zones, or specifically assigned to another zone. Assigning a Web site to the Restricted zone constrains the site allowing for performance of a limited range of very safe options; this zone also results in more frequent prompts to the consumer for security setting decisions.

The Internet Zone contains all Web sites which are not included in another zone. It is not possible to add Web sites to this zone. The Internet zone is set to the Medium security level by default. Web sites in this zone are allowed to perform a range of predefined options; a moderate number of prompts will be directed to the consumer for security setting decisions. Legitimate security concerns may prompt you to raise the security level to High. This may result in some Web pages not displaying or functioning properly. Choosing a Custom level allows you to control individual security decisions for the zone.

All the security zones come with a preselected default security level. You may accept these defaults, change the level to one of the other preconfigured default security levels, or configure your own Custom security level. These choices are available in all security zones except the My Computer zone. All security options may be modified from the Security Zones user interface in the Internet Options menu (Figure 26).

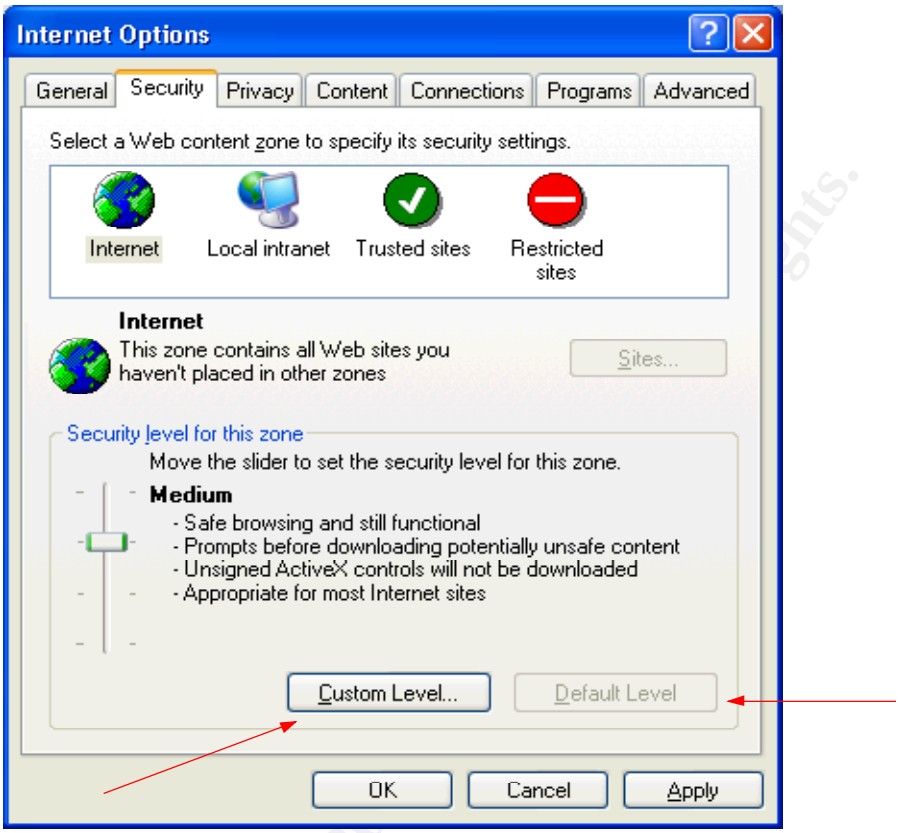

Figure 26

To navigate to the Internet Options menu (Figure 26):

- On your Internet Explorer browser toolbar click on the 'Tools' menu.
- Click 'Internet Options…'
- Click the tab marked 'Security'.
- Using the slide bar you can choose from the four preconfigured security levels. Sliding the bar to the bottom is the least restrictive (Low security level), while sliding the bar to the top is the most restrictive (High security level).

To reset any of the security zones to the default settings, click the icon of the zone you want to reset, then click the Default Level button (Figure 26) followed by OK. The Default Level button will be available once the default security setting has been modified.

Having a clear understanding of the default security levels will provide a deeper understanding of Internet Explorer security levels, and provide a foundation for the advanced settings which must be selected in a custom security level. The following table summarizes the default security levels (Table 2):

Security Level	Summary
Low	Minimal safeguards; warning prompts are provided. Most content is downloaded and run without prompts. All active content is allowed to run. Designed for Web sites you absolutely trust.
Medium-low	Same settings as Medium without the prompts. Most content will run without prompts. Unsigned ActiveX controls will not be downloaded. (A signed ActiveX control means the author certifies the control is free from malicious code.) Appropriate for sites on your local network (intranet).
Medium	Provides for safe and functional browsing. Prompts before downloading possibly unsafe content. Unsigned ActiveX controls will not be downloaded. Appropriate for most Web sites.
High	The safest way to browse though also the least functional. Less secure features are disabled. Appropriate for sites you do not trust, which may have harmful content.

Table 2[22]

Each security zone is represented by a unique icon on the Security tab of the Internet Options menu (Figure 26). To view, set or change a default security level for a particular zone:

- Click on the icon for the zone you want to configure.
- Adjust the slider bar to your choice of the four default levels.
- You may be prompted by a warning message to confirm your choice of security levels. Clicking Yes will confirm your choice.
- Click on the Apply button, and then the OK button.

The consumer may specify the security settings for individually defined Web sites. You may add specific Web sites to The Local intranet zone (designed to be modified by system administrators), Trusted sites and Restricted sites zones. The Trusted site zone is set by default to a security setting of Low—this is the most permissive zone. Only Web sites that you implicitly trust and believe to be free from potentially harmful content should be placed in this zone. Security may be enhanced in this zone by requiring server verification (https :) for all sites in this zone (Figure 27). HTTPS: transmits data in an encrypted format; keep in mind not all Web sites support HTTPS:. This setting is not available in the Restricted site zone. The Restricted site zone is set to a security setting of High by default—this is the most restrictive zone. You should only add sites to this zone that you do not trust, which you believe have a high probability of containing malicious content. All Web sites added to these zones will follow the

security settings for that designated zone.

To add a Web site to the Trusted or Restricted site zones, highlight the appropriate icon and click the Sites…button (the button will be highlighted once you choose the Trusted or Restricted site zone icons) on the Security tab of the Internet Options menu (Figure 26). Clicking the Sites… button launches the menu which allows the addition of Web sites to your chosen zone (Figure 27).

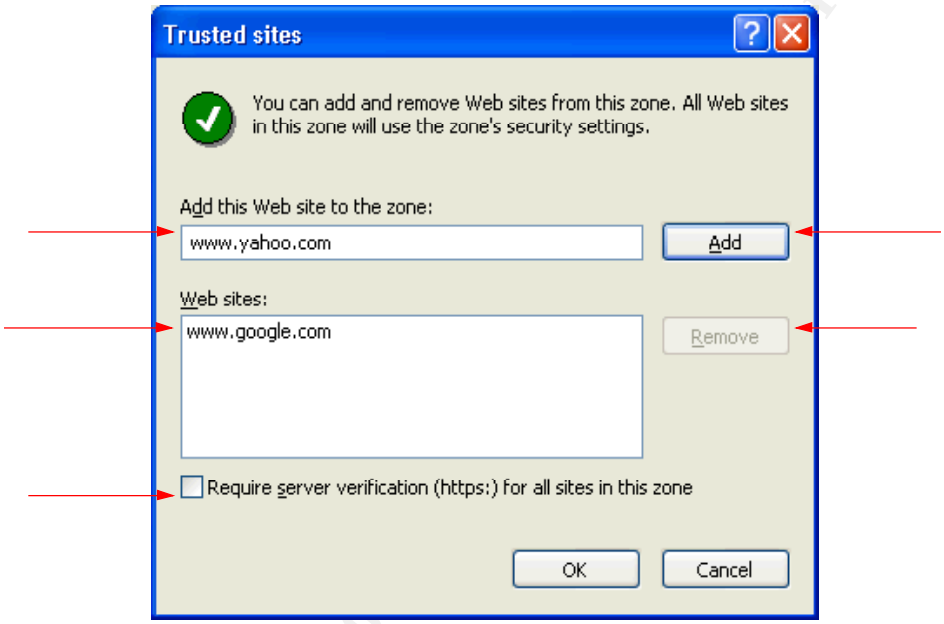

Figure 27

To add a Web site, in the Add this Web site to the zone: text box, type in the Web site address and click the Add button, then click OK. To remove a site from the zone, highlight the Web site you wish to remove in the Web sites: list. Once the Web site is highlighted, click the Remove button (the button will be highlighted once a Web site is highlighted for removal), then click OK. Figure 27 demonstrates the procedures for the Trusted site zone; follow the same process for adding and removing Web sites in the Restricted zone.

The four predefined default settings in Internet Explorer 6 offer the majority of home consumer's sufficient security for browsing the Internet. Internet Explorer provides for granular specification of security settings. These advanced settings are found and modified by clicking the icon of the zone you wish to customize and choosing the Custom Level… button (Figure 26). Choosing the Custom Level…button spawns the advanced Security Settings menu (Figure 28).

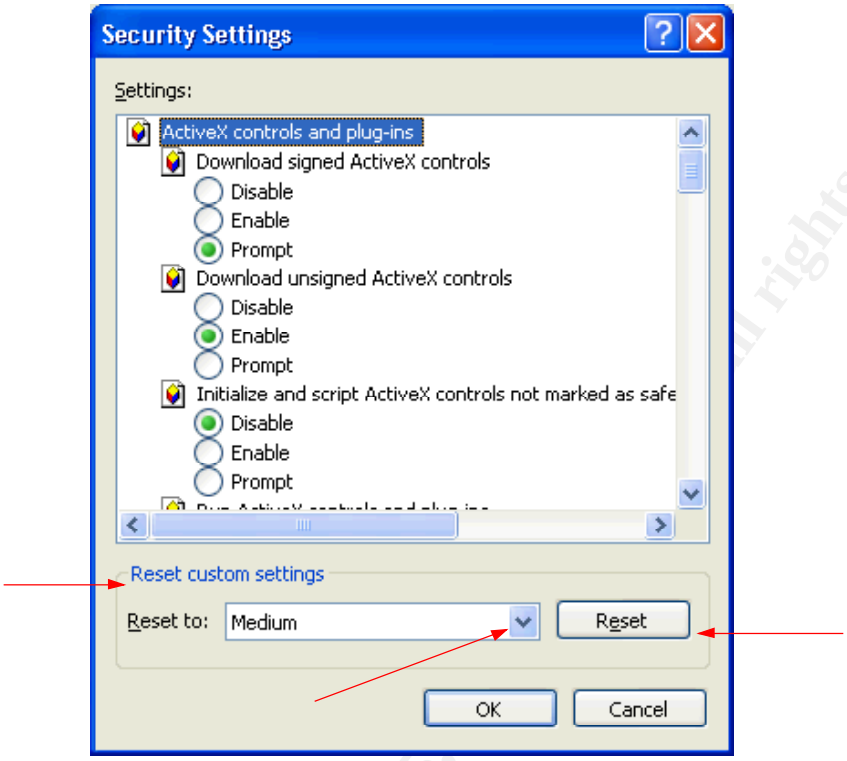

Figure 28

The custom Security Settings menu should be used with caution and care. While the home consumer may elect to modify settings in this menu, these advanced settings are designed for professional system administrators. Home consumers wishing to modify these settings are advised to do advanced research on the individual security settings before changing them. The document Setting Up Security Zones by Microsoft offers a detailed explanation of the Custom level settings. Choices made in this menu have the potential to interfere with how Web pages act and may be displayed. You have the option to Reset the chosen zone to any of the four preconfigured security settings. Choose the desired default security setting from the drop down box under the Reset custom settings portion of the menu. Once the desired default security setting is chosen, click on the Reset button followed by OK (Figure 28). To set individual security settings you must scroll in the Settings: menu and click on the radio button for each desired setting, followed by OK (Figure 28). Keep in mind that choices made in this menu only apply to the individual zone chosen from the Security tab on the Internet Options menu. Each zone must be configured independently in the Security Settings menu. Modify these settings with extreme caution. The following table identifies the default settings for each Custom security option for each security level (Table 3).

ActiveX Controls and Plug-Ins

Security option	Low	Medium-low	Medium	High
Download signed ActiveX controls	Enable	Prompt	Prompt	Disable
Download unsigned ActiveX controls	Prompt	Disable	Disable	Disable
Initialize and script ActiveX controls not marked as safe	Prompt	Disable	Disable	Disable
Run ActiveX controls and plug-ins	Enable	Enable	Enable	Disable
Script ActiveX controls marked safe for scripting	Enable	Enable	Enable	Disable

Downloads				
Security option	Low	Medium-low	Medium	High
File download	Enable	Enable	Enable	Disable
Font download	Enable	Enable	Enable	Prompt

Miscellaneous				
Security option	Low	Medium-low	Medium	High
Access data sources across domains	Enable	Prompt	Disable	Disable
Allow META REFRESH	Enable	Enable	Enable	Disable
Display mixed content	Prompt	Prompt	Prompt	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Enable	Enable	Disable	Disable
Drag and drop or copy and paste files	Enable	Enable	Enable	Prompt
Installation of desktop items	Enable	Prompt	Prompt	Disable
Launching programs and files in an IFRAME	Enable	Prompt	Prompt	Disable
Navigate sub-frames across different domains	Enable	Enable	Enable	Disable
Software channel permissions	Low safety	Medium safety	Medium safety	High safety

Miscellaneous				
Security option	Low	Medium-low	Medium	High
Submit nonencrypted form data	Enable	Enable	Prompt	Prompt
Userdata persistence	Enable	Enable	Enable	Disable

Scripting				
Security option	Low	Medium-low	Medium	High
Active scripting	Enable	Enable	Enable	Disable
Allow paste operations via script	Enable	Enable	Enable	Disable
Scripting of Java applets	Enable	Enable	Enable	Disable

User Authentication

Security option	Low	Medium-low	Medium	High
Logon	Automatic logon with current username and password	Automatic logon only in Intranet zone	Automatic logon only in Intranet zone	Prompt for user name and password

Table 3[23]

Internet Explorer 6 Security Zones provide a granular mechanism for enhancing your security when surfing the net. It is up to you, the home consumer, to take the initiative to protect yourself. Hackers, crackers and malware are out there and seeking under protected computers to compromise. Do not unwittingly become their next victim.

"Let us not look back in anger or forward in fear, but around in awareness".[24]

James Thurber – Author & Humorist

This document does not offer a magical fix to the threats the Internet poses; nor does any other document published on the subjects of Internet privacy and/or security. It is impossible to offer a total solution to privacy and security matters. The Internet is dynamic, as are the potential threats. Awareness and education are the keys to protecting your privacy and security on the Internet. Internet privacy and security ignorance is not bliss—it is inherently dangerous. If you have been compromised by a hacker or malware, or unwittingly tracked by a Web site, you may have experienced feelings of anger and perhaps experienced feelings of fear and helplessness the next time you logged onto the Internet. Ignorance of privacy and security measures sets you up to be a victim; it is not a matter of if you will be compromised, only a matter of when. Research currently indicates that unpatched or under protected computers that have been connected to the Internet are being compromised in 3 days or less.[25] You may choose to be a victim, or you may empower yourself and take measures to enhance the layers of defense on your personal computer.

Practicing the principles of defense in depth is not a magic panacea. Layering your privacy and security postures will not thwart all attempts to invade your privacy or compromise your security. Nefarious activity and behaviors are on the rise, and the threat has never been greater in Internet history. Education of the threats in conjunction with a posture of defense in depth will provide the home consumer with a matrix of protection, and minimize the possibilities of becoming the next victim. The privacy and security measures you instill must be monitored and upgraded on a regular basis. If this sounds like a lot of work, you are right—it is. Protecting your privacy and security is your responsibility. The Internet can be, and is, a terrific educational and entertainment medium. Using

this technology wisely, and practicing the principles of defense in depth, will enhance your Internet experience. If you choose to be privacy and security ignorant, your choice amounts to practicing 'defense in shallow'; which provides limited, to no defense at all. Ultimately, the choice is yours.

List of References

All About Cookies "General Information About Cookies 1997 – 2003
URL http://www.allaboutcookies.org/cookies/cookies-the-same.html

All About Cookies "What are Web Beacons (also known as Web Bugs) and Clear GIFs?" 1997 – 2003
URL http://www.allaboutcookies.org/web-beacons/index.html

All About Cookies "What is P3P? What has it got to do with privacy?" 1997 – 2003
URL http://www.allaboutcookies.org/p3p-cookies/index.html

Aspect Security "News" 2003
URL http://www.aspectsecurity.com/news.html

BrainyQuote "James Thurber Quotes" 2004

URL http://www.brainyquote.com/quotes/quotes/j/jamesthurb106488.html

CNET Asia: IT Manager "Protect your network with Internet Explorer 6's Security Zones" 3 September 2002
URL http://asia.cnet.com/itmanager/tech/0,39006407,39075568,00.htm

Dole, Bob. "Amusing Quotes" 2003
URL http://www.amusingquotes.com/h/d/Bob_Dole_1.htm

Freeman, James "You Have Zero Privacy…Get Over It" 9 August 1999
URL http://www.usatoday.com/news/opinion/columnists/freeman/ncjf30.htm

Internet Content Rating Association "ICRA filtering using Microsoft Internet Explorer" 1999 – 2003
URL http://www.icra.org/_en/faq/contentadvisor/

Labalme, Fen "Fen's Collected Quotes: Nerdly" 1994 – 2004
URL http://www.fen.net/quotes/nerdly.shtml

LivingInternet "NSFNET" 1997 - 2003
URL http://livinginternet.com/i/ii_nsfnet.htm

Marshall, Brian "How Internet Cookies Work" 1998 – 2004
URL http://computer.howstuffworks.com/cookie1.htm

McClure, Stuart. Scambry, Joel. Kurtz, George. Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition. McGraw – Hill / Osborne: Berkeley, California: 2003 Pgs. 649 – 652

Microsoft Internet Explorer "Browse the Web with Content Advisor" 26 March 2003
URL
http://www.microsoft.com/windows/ie/evaluation/features/indepth/contentadv.asp

Microsoft Internet Explorer "Help Safeguard Your Privacy on the Web"
26 March 2003
URL
http://www.microsoft.com/windows/ie/using/howto/privacy/config.asp#cookies

Microsoft Internet Explorer "Setting Up Security Zones" 7 September 2001
URL http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

Microsoft Knowledge Base Article – 154036 "How to Disable Active Content in Internet Explorer" 15 September 2003
URL
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/s

upport/kb/articles/Q154/0/36.asp&NoWebContent=1

Munson, Shauna "Defense in Depth and the Home User: Securing the Home PC" 24 January 2003
URL http://www.giac.org/practical/GSEC/Shauna_Munson_GSEC.pdf

Netscape Support Documentation "Persistent Client State HTTP Cookies" 1999
URL http://wp.netscape.com/newsref/std/cookie_spec.html

O'Sullivan, Miko "Embedded Objects" 1997 – 2002
URL http://www.faqs.org/docs/htmltut/embeddedobjects/_EMBED.html

SafeSurf IESetup "How to Update Microsoft's Internet Explorer to Support SafeSurf Ratings" 2002
URL http://www.safesurf.com/iesetup/

SANS Institute "SANS Network Security 2003" 2002 – 2003
URL http://www.sans.org/ns2003/track8.php

Scambray, Joel and McClure, Stuart Hacking Windows 2000 Exposed: Network Security Secrets & Solutions. Osborne / McGraw – Hill: Berkeley, California 2001 Pgs. 357 – 360

Scambray, Joel and Shema, Mike Hacking Web Applications Exposed: Web Application Security Secrets & Solutions. McGraw – Hill / Osborne: Berkeley, California: 2002 Pgs. 278 – 297

ScienCentral, Inc, and The American Institute of Physics "Birth of the Internet" 1999
URL http://www.pbs.org/transistor/background1/events/arpanet.html

SearchWebServices.com Definitions 'Transient Cookie" 31 July 2001
URL
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci752450,00.html

Security Space "P3P Compact Privacy Policy Report" 1 March 2004
URL http://www.securityspace.com/s_survey/data/man.200402/p3p.html

Webopedia "Active Content" 20 February 2002
URL http://www.webopedia.com/TERM/A/active_content.html

Webopedia. "ARPANET" 2 July 2001
URL http://www.webopedia.com/TERM/A/ARPANET.html

Webopedia "The Birth of the Internet" 2004
URL http://webopedia.com/didyouknow/internet/2002/birthoftheinternet.asp

Webopedia "Web Beacon" 21 August 2003
URL http://www.webopedia.com/TERM/W/Web_beacon.html

Webteacher "JavaScript for the Total Non-Programmer" 2004
URL http://www.webteacher.com/javascript/

W3C "Platform for Privacy Preferences (P3P) Project" 19 February 2004
URL http://www.w3.org/P3P/#what

End Notes

[1] Dole, Bob. "Amusing Quotes" 2003
URL http://www.amusingquotes.com/h/d/Bob_Dole_1.htm

[2] Webopedia "ARPANET" 2 July 2001
URL http://www.webopedia.com/TERM/A/ARPANET.html

[3] LivingInternet "NSFNET" 1997 - 2003
URL http://livinginternet.com/i/ii_nsfnet.htm

[4] LivingInternet "NSFNET" 1997 - 2003
URL http://livinginternet.com/i/ii_nsfnet.htm

[5] Munson, Shauna "Defense in Depth and the Home User: Securing the Home PC" 24 January 2003

URL http://www.giac.org/practical/GSEC/Shauna_Munson_GSEC.pdf

[6] Freeman, James "You Have Zero Privacy…Get Over It" 9 August 1999
URL http://www.usatoday.com/news/opinion/columnists/freeman/ncjf30.htm

[7] Microsoft Internet Explorer "Help Safeguard Your Privacy on the Web" 26 March 2003
URL
http://www.microsoft.com/windows/ie/using/howto/privacy/config.asp#cookies

[8] SearchWebServices.com Definitions 'Transient Cookie" 31 July 2001
URL
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci752450,00.html

[9] Netscape Support Documentation "Persistent Client State HTTP Cookies" 1999
URL http://wp.netscape.com/newsref/std/cookie_spec.html

[10] Webopedia "Web Beacon" 21 August 2003
URL http://www.webopedia.com/TERM/W/Web_beacon.html

[11] All About Cookies "What are Web Beacons (also known as Web Bugs) and Clear GIFs?" 1997 – 2003
URL http://www.allaboutcookies.org/web-beacons/index.html

[12] W3C "Platform for Privacy Preferences (P3P) Project" 12 August 2003
URL http://www.w3.org/P3P/#what

[13] All About Cookies "What is P3P? What has it got to do with privacy?" 1997 – 2003
URL http://www.allaboutcookies.org/p3p-cookies/index.html

[14] Labalme, Fen "Fen's Collected Quotes: Nerdly" 1994 – 2004
URL http://www.fen.net/quotes/nerdly.shtml

[15] Microsoft Internet Explorer "Browse the Web with Content Advisor" 26 March 2003
URL
http://www.microsoft.com/windows/ie/evaluation/features/indepth/contentadv.asp

[16] Internet Content Rating Association "ICRA filtering using Microsoft Internet Explorer" 1999 – 2003
URL http://www.icra.org/_en/faq/contentadvisor/

[17] SafeSurf IESetup "How to Update Microsoft's Internet Explorer to Support SafeSurf Ratings" 2002
URL http://www.safesurf.com/iesetup/

[18] Aspect Security "News" 2003
URL http://www.aspectsecurity.com/news.html

[19] Webopedia "Active Content" 20 February 2002
URL http://www.webopedia.com/TERM/A/active_content.html

[20] Microsoft Internet Explorer "Setting Up Security Zones" 7 September 2001
URL http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

[21] Microsoft Internet Explorer "Setting Up Security Zones" 7 September 2001
URL http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

[22] CNET Asia: IT Manager "Protect your network with Internet Explorer 6's Security Zones" 9 March 2002
URL http://asia.cnet.com/itmanager/tech/0,39006407,39075568,00.htm

[23] Microsoft Internet Explorer "Setting Up Security Zones" 7 September 2001
URL http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

[24] BrainyQuote "James Thurber Quotes" 2004
URL http://www.brainyquote.com/quotes/quotes/j/jamesthurb106488.html

[25] SANS Institute "SANS Network Security 2003" 2002 – 2003
URL http://www.sans.org/ns2003/track8.php