Malicious Interface Design: Exploiting the User

Gregory Conti
United States Military Academy
West Point, New York 10996
gregory.conti@usma.edu

Edward Sobiesk
United States Military Academy
West Point, New York 10996
edward.sobiesk@usma.edu

ABSTRACT

In an ideal world, interface design is the art and science of helping users accomplish tasks in a timely, efficient, and pleasurable manner. This paper studies the inverse situation, the vast emergence of deliberately constructed malicious interfaces that violate design best practices in order to accomplish goals counter to those of the user. This has become a commonplace occurrence both on and off the desktop, particularly on the web. A primary objective of this paper is to formally define this problem, including construction of a taxonomy of malicious interface techniques and a preliminary analysis of their impact on users. Findings are presented that gauge the self-reported tolerance and expectation levels of users with regard to malicious interfaces as well as the effectiveness and ease of use of existing countermeasures. A second objective of this paper is to increase awareness, dialogue, and research in a domain that we consider largely unexplored but critical to future usability of the WWW. Our results were accomplished through significant compilation of malicious interface techniques based on review of thousands of web sites and by conducting three surveys. Ultimately, this paper concludes that malicious interfaces are a ubiquitous problem that demands intervention by the security and human computer interaction communities in order to reduce the negative impact on the global user population.

Categories and Subject Descriptors

H5.m. Information interfaces and presentation (e.g., HCI), Miscellaneous.

General Terms

Security, Human Factors.

Keywords

Malicious interfaces, adversarial interface design, evil interfaces, design principles, web usability guidelines.

1. INTRODUCTION

Usable interface design, both on or off the desktop, seeks to maximize successful task completion, eliminate errors, reduce task completion time, and create a pleasurable user experience. However, these ideals are often being ignored in practice. Some interface designers deliberately violate usable design best practices in order to manipulate, exploit, or attack the user. We define such interfaces as malicious and argue that the key difference between usable interface design and malicious interface design is the intent on the part of the designer to deliberately sacrifice the user experience in an attempt to achieve the designer's goals ahead of those of the user.

Malicious interfaces are commonplace on the web, and to a lesser degree in operating system distributions and individual software applications. They are employed for a variety of reasons that are often linked to direct or indirect acquisition of revenue. Revenue driven motivations include selling a product or service, increasing brand recognition, gathering personal information from the user, and obfuscating legally mandated but undesirable information from the user. In less common cases, the designer may not be driven by profit, and instead utilizes malicious interface techniques to shock, disgust, or otherwise attack the user. Malicious techniques include the use of blinking objects, animations, videos, or sounds to attract user attention, spoofed interface elements to trick the user into taking a desired action, forcing the user to wait and view undesired content, and navigation architectures that divert a user away from the user's objectives towards those of the designer. Malicious interfaces also abound off the desktop, particularly in settings that seek to elicit some desired asset from the user. Off the desktop examples include gas station pumps designed to subtly induce the user to purchase a car wash or premium gasoline, arcade games with deliberately loose controls, digital video recorders that lack 30 second skip functionality in order to prevent users from easily skipping commercials, and pushbutton toothpaste dispensers that dispense more than a necessary portion of toothpaste.

Notably, the problem of malicious interfaces isn't isolated to primary interface designers or organizations, but is also encountered when third parties with the power to inject or alter the user's interface attempt to exploit the user. One such case is advertising networks that distribute third-party advertisements that are embedded in web pages of cooperating webmasters. Advertising networks possess an extremely wide reach and may include hundreds of thousands or more websites in their networks. Additionally, the cooperation or tacit approval of the original webmaster isn't always necessary. There is an increasing trend by communication providers to exploit their powerful position to take advantage of users. Excellent examples are Internet Service Providers (ISPs) that modify web page content in transit or capitalize on user errors. Such attacks are not idle speculation, but occurred recently when the Canadian ISP Rogers injected unsolicited content into its users' web sessions and when the Road Runner ISP redirected mistyped URLs to advertising laden error pages [1,2]. Network neutrality researchers believe the problem of modifying network content in transit is on the rise [3].

The impact of malicious interfaces on the user is significant and detrimental. Advertising has emerged as the dominant business model for thousands of websites that cater to the millions of users who employ free online tools and services. Malicious interface

WWW 2010, April 26–30, 2010, Raleigh, North Carolina, USA.
ACM 978-1-60558-799-8/10/04.

techniques are thus central to the business practices of many online companies. The problem of malicious interfaces is exasperated both by the competitive pressures of the marketplace and by the users' tendency to become desensitized to aggressive techniques. The combination of these two forces creates an environment where malicious interface techniques become more aggressive over time, in an attempt to penetrate the users' adaptive defense mechanisms. The malicious interface techniques employed must be aggressive enough to penetrate the cognitive defenses of the user, but not so aggressive that the user decides to seek an alternative. Designers of malicious interfaces seek to operate between these two bounds. Unfortunately, the range of possibilities within this band is large and malicious interface designers continually develop new adversarial interface techniques. The end result is that many interfaces, especially those on the web, are becoming increasingly unusable, slowing task completion, encouraging errors, and creating unpleasant experiences for millions of users worldwide.

For the technically savvy, the impact of malicious interface design and the resultant adversarial interfaces is somewhat manageable, albeit annoying and inconvenient, but this isn't the case for all classes of users. One of the worst aspects of malicious interfaces is that they place the most vulnerable and most innocent at risk, sometimes effectively denying use of the web and software applications altogether. It is difficult to create usable interfaces for the elderly, young, cognitively or sensory challenged, and the less educated; deliberately (or even inadvertently) attacking these users via malicious interfaces is creating a class divide that may deny the use of information technology assets to these important and vulnerable groups. Malicious interface techniques are often in direct opposition to many accessibility guidelines and laws such as the World Wide Web Consortium's Web Accessibility Initiative, the United Kingdom's Disability Discrimination Act of 1995, the Americans with Disabilities Act, and Section 504 of the United States Rehabilitation Act of 1973 [4,5,6,7].

The purpose of this paper is to assist in defending all users by better defining the problem of malicious interface design, analyzing the impact of malicious interfaces on users, evaluating the effectiveness of current countermeasures, and presenting promising directions for future work. To this end, we make several unique contributions. We present a taxonomy of malicious interface techniques and provide the results from three surveys that offer insight into user tolerance and expectations regarding adversarial interface techniques as well as the effectiveness of current countermeasures. Our intent with this paper is to motivate and assist researchers in the interface design, advertising, and security communities in seeking solutions to the pervasive problem of malicious interfaces. Our work focuses specifically on interfaces that are *deliberately and maliciously* designed to trick, mislead, frustrate, and manipulate the user using syntactically correct, but adversarial, interface techniques. Technically, phishing emails and spoofed websites also fall into this group, but our emphasis, and the greatest source of the threat, is on mainstream websites conducting legal business on the web. We do not address attacks that employ tactics that exploit security vulnerabilities in order to subvert the user's applications, operating system, or network connectivity, or those that install adware or spyware, even if these attacks later alter the user's interface in some way. Our malicious interface designer attacks the *human user* and not their computing platform.

This paper is organized as follows. Section 2 presents our taxonomy of malicious interface techniques. Section 3 discusses results from our surveys on the impact of malicious interfaces. Section 4 addresses the effectiveness of existing countermeasures. Section 5 places our work in the field of existing research. Section 6 presents our conclusions and suggestions for future work.

2. A TAXONOMY OF MALICIOUS INTERFACE DESIGN TECHNIQUES

Malicious interface design techniques exploit virtually every facet of human computer interaction. A vulnerability exists any time the interface designer sees an opportunity to accomplish their goals ahead of the user by abusing the technology that implements the interface. The following taxonomy, see Table 1, was created based on a 12 month study involving websites, desktop software, and interfaces off the desktop. Each entry in the taxonomy exists in the wild. In some cases, a malicious interface technique may be appropriate for multiple categories, such as a thumbnail image that purports to link to a high-resolution image, but instead links to a sign-in page. This example would be appropriate for both the "Trick" and "Manipulating Navigation" categories.

A key challenge when creating taxonomies is completeness. Malicious interface design techniques are particularly problematic because they are difficult to search for using automated techniques; oftentimes malicious techniques must be encountered and identified by a human user. To address this challenge, part of the construction of our taxonomy involved a study where 22 participants, each a college undergraduate student, actively sought out malicious interface techniques, both on and off the desktop. Participants were asked to identify as many different types of malicious interface design techniques as possible. In addition, we conducted a group discussion with approximately 75 participants at the Hackers of Planet Earth (HOPE) Conference – actively soliciting missing techniques. We used the information gathered from both our student and hacker conference groups to validate the composition of our taxonomy.

A minutely detailed description of our taxonomy is beyond the scope of this paper. What follows is an abstracted version of the taxonomy that fully supports our objectives. The major categories of our malicious interfaces taxonomy are highlighted below and are more thoroughly described in Table 1:

Coercion – Threatening or mandating the user's compliance.

Confusion – Asking the user questions or providing information that they do not understand.

Distraction – Attracting the user's attention away from their current task by exploiting perception, particularly preattentive processing.

Exploiting Errors – Taking advantage of user errors to facilitate the interface designer's goals.

Forced Work – Deliberately increasing work for the user.

Interruption – Interrupting the user's task flow.

Manipulating Navigation – Creating information architectures and navigation mechanisms that guide the user toward interface designer task accomplishment.

Obfuscation – Hiding desired information and interface elements.

Restricting Functionality – Limiting or omitting controls that would facilitate user task accomplishment.

Shock – Presenting disturbing content to the user.

Trick – Misleading the user or other attempts at deception.

Category	Example Subcategory	Representative Instances
Coercion – Threatening or mandating the user's compliance.	Mandatory form field entries	Require the user to enter contact information before allowing user to accomplish task.
	Send user threatening messages	"Register now or face punitive action" message.
Confusion – Asking the user questions or providing information that they do not understand.	Ask user questions they do not understand	Asking a novice user if they would like to change their default browser; use of double, triple, or quadruple negatives.
Distraction – Attracting the user's attention away from their current task by exploiting perception, particularly pre-attentive processing.	Video / Animation / Blinking / Motion / Audio	Advertisements commonly found on the web.
	Color	Premium gas button on pump is red to attract attention.
Exploiting Errors – Taking advantage of user errors to facilitate the interface designer's goals.	Typing errors	Mistyped URL brings up advertisement instead of assistance.
Forced Work – Deliberately increasing work for the user.	Delay user's work effort	Force the user to wait and view an advertisement for N seconds.
	Make uninstalling difficult	Removing an operating system's default instant messaging application requires a complex registry edit.
Interruption – Interrupting the user's task flow.	Force viewing	Cover user desired content, such as a news article, with designer desired content, such as an advertisement.
	Hyper-sensitive interface elements	Overly large "hot" regions for advertisements, using rollover events to trigger pop-up advertisements.
Manipulating Navigation – Information architectures and navigation mechanisms that guide the user towards interface designer's goal.	Dead end trails/Infinite trails	Asking a (near infinite) number of questions to get a "free" iPod.
	Place desired content / important information deep in navigation hierarchy	Making the free version of an application far more difficult to find than the commercial version on a consumer firewall vendor's website.
Obfuscation – Hiding desired information and interface elements.	Low contrast color scheme	Reducing contrast of close/stop buttons on video advertisements.
	Mask user warning messages	Using JavaScript to mask/rewrite browser address and status bars.
Restricting Functionality – Limiting or omitting controls that the user needs to accomplish a task.	Omit necessary controls	Removal of 30 second skip button on TiVo remote control, lack of video download option at a video sharing site, pre-checked mailing list selections (but no "unselect all" option).
	Hide desired interface elements	Place "print" hyperlink at obscure location on webpage to increase advertisement viewing times.
Shock – Presenting disturbing content to the user.	Display controversial content	Examples of this include the Internet shock site Goatese.cx and the placement of seizure-inducing graphics on the forums of the nonprofit Epilepsy Foundation [8].
Trick – Misleading the user or other attempts at deception, such as spoofed content or interface elements.	Silent/Invisible behavior	Installing additional software without user's knowledge or consent.
	Lie	"You've just won a contest" advertisement.
	Spoof content	Advertisements designed to appear as news stories.

Table 1. Taxonomy of malicious interface design techniques.

As malicious interface designers continue to "innovate," over time we expect this taxonomy will grow. In particular, we expect that attackers, could, by examining existing and emerging usable interface design techniques, subvert them in order to develop new malicious interface techniques and mechanisms to manipulate and exploit the user.

3. ASSESSING IMPACT

So far, this paper has enumerated the various types of malicious interface design techniques. In this section, we conduct some initial measurement of the dissatisfaction felt by users as they encounter such techniques. We also seek to understand the user's tradeoff between accomplishing a given task and the amount of frustration they will tolerate.

3.1 Frustration

We sought to explore user frustration with eight common malicious interface techniques by surveying 27 attendees at the HOPE Conference in New York City. The categories we chose to evaluate were techniques that *deliberately* forced users to wait and view advertisements, caused unnecessary interruptions, made content difficult to find, attempted to trick users into viewing advertisements, attempted to coerce users into registering for a user account or to pay for premium access, made advertisements appear as legitimate content (including forms and interface elements), presented blinking or animated advertisements, and installed applications without the user's permission. When constructing the survey we purposely chose categories from the taxonomy that the participants have likely encountered and were easy to understand when presented in a written survey. Participants were asked to rate their frustration on a Likert scale from 1 (No frustration) to 7 (Extreme frustration), see Table 2. Figure 1 depicts the results graphically. As you examine these results, note that respondents found every technique significantly frustrating – by rating each technique at least a five, on average. Upon analysis, including follow-up discussions with participants, we believe coerced registration and blinking/animated advertisements were rated less troublesome because solutions are readily available, via simply registering the application and using ad-blocking software, respectively.

Technique	Average	Std Dev
Coerced Registration/Payment	5.15	1.38
Blinking/Animated Advertisements	5.37	1.28
Spoofed Content or Interface Elements	5.46	1.70
Tricked into Viewing Advertisements	5.78	1.09
Forced Waiting	5.89	1.12
Difficult to Find Content	5.89	1.09
Unnecessary Interruptions	6.22	0.93
Installation of Applications Without Permission	6.96	0.20

Table 2. User frustration with eight major malicious interface techniques. (1=No frustration, 7=Extreme frustration)

The remaining malicious interface techniques ranked higher because no comprehensive countermeasure exists. We will discuss countermeasures in more detail later in the paper. We realize that these results were for advanced users, who are far more aware and sensitive to malicious techniques than an average user. We look forward to further studies that evaluate the frustration level of various diverse categories of users.

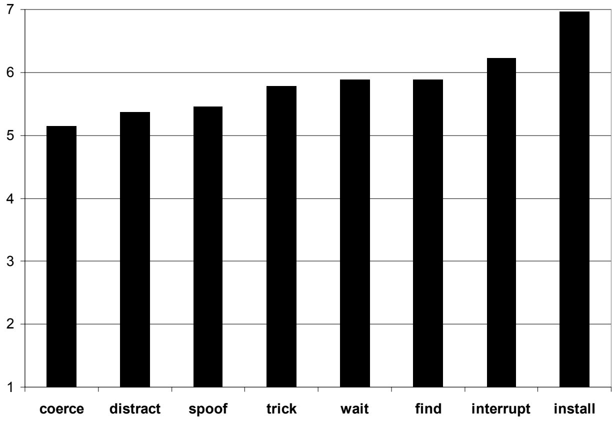

Figure 1. User frustration with eight major malicious interface techniques. (1=No frustration, 7=Extreme frustration)

3.2 Tolerance and Expectations

The previous section analyzed frustration levels caused by malicious interface techniques, but designers in most cases do not frustrate users without limit, nor without reason. Particularly in the case of the commercial web, malicious interface designers seek a balance between aggressive interface techniques (and their perceived increase in revenue) and frustrating users to the point that they leave and seek task accomplishment elsewhere.

We believe there exists a spectrum of user frustration caused by the employment of malicious interface techniques. At one end of the spectrum, the value of the user's task accomplishment far outweighs the frustration caused by the interface. In this case, the user is satisfied – possibly even pleased. As interface-generated annoyance increases, however, the user will start to become dissatisfied, eventually reaching a point where the user will not accept further frustration in order to accomplish their task. We dub this point of parity the *tolerance threshold*. Below this threshold the user will remain and above the threshold the user will seek task accomplishment from a competitor, if available. We believe that malicious interface designers seek to operate in a sweet spot just below the tolerance threshold in an attempt to maximize revenue while still retaining the majority of their users.

To explore these assertions, we surveyed two categories of groups. As a group representing more common users, we surveyed 61 undergraduates at a medium sized college in the Northeast United States and asked them to evaluate the degree of frustration they would tolerate and the degree of frustration they would expect from popular classes of websites. For comparison and further understanding, we also surveyed 27 attendees of the HOPE Conference on the degree of malicious interface frustration they would expect from the same set of

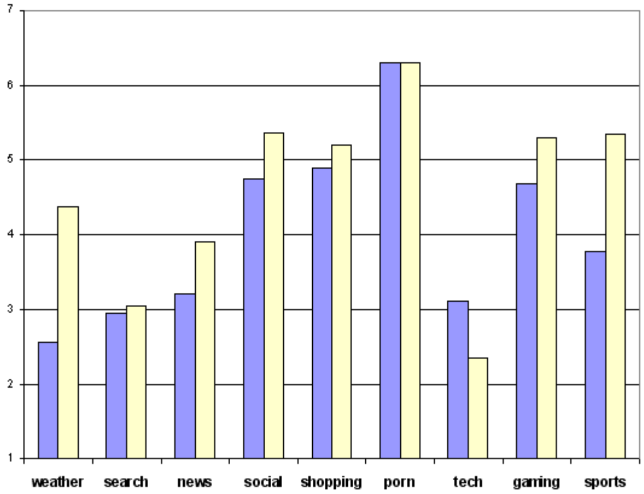

Figure 2. Comparison of undergraduate (dark) and expert (light) user expectation of malicious interface techniques by website category. (1=None, 7=Extreme)

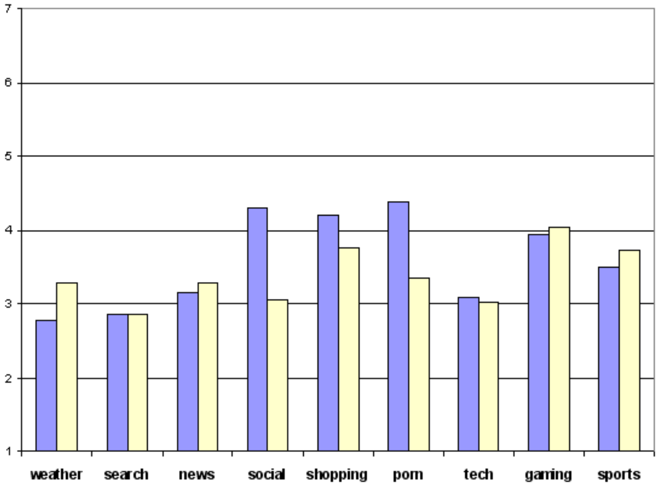

Figure 3. Comparison of undergraduate (dark) and expert (light) user tolerance of malicious interface techniques by website category. (1=None, 7=Extreme)

	Tolerate	Std Dev	Expect	Std Dev	Δ
Vendor Support	3.02	1.62	2.36	1.44	-0.66
Search Engine	2.85	1.73	3.04	1.74	0.19
News	3.29	1.36	3.89	1.67	0.60
Weather	3.29	1.50	4.38	1.86	1.09
Gaming	4.05	1.53	5.30	1.40	1.25
Shopping	3.76	1.72	5.20	1.68	1.44
Sports	3.74	1.54	5.33	1.68	1.59
Social Networking	3.05	1.66	5.36	1.29	2.31
Pornography	3.35	2.06	6.29	1.43	2.94

Table 3. Expert user expectation and tolerance for malicious interface techniques by website class. (1=None, 7=Extreme)

	Tolerate	Std Dev	Expect	Std Dev	Δ
Weather	2.77	1.32	2.56	1.07	-0.21
Vendor Support	3.08	1.50	3.11	1.54	0.03
News	3.15	1.35	3.20	1.40	0.05
Search Engine	2.85	1.29	2.95	1.47	0.10
Sports	3.50	1.40	3.77	1.23	0.27
Social Networking	4.30	1.37	4.74	1.15	0.44
Shopping	4.20	1.41	4.89	1.40	0.69
Gaming	3.93	1.49	4.67	1.22	0.74
Pornography	4.39	1.86	6.31	1.17	1.92

Table 4. Undergraduate user expectation and tolerance for malicious interface techniques by website class. (1=None, 7=Extreme)

classes as well as 47 attendees of the BlackHat and Defcon conferences on the degree of frustration they would tolerate from the same set of classes. We chose to gather data on both expectations and tolerance in order to better understand the relationship between users' perceptions regarding the prevalence of malicious interface techniques employed on popular websites and how much frustration they believe they would bear for each. We also chose to augment the responses of the college students with those of the more security savvy experts who attend HOPE, Defcon, and BlackHat to identify where there was intersection and where there were differences. The results are shown in Tables 3 and 4 as well as Figures 2, 3, and 4.

Our results clearly indicate that users expect and tolerate varying degrees of malicious interface techniques based on content category. Expert users will tolerate the greatest frustration on gaming, shopping, pornographic, and sports websites. Undergraduate users will tolerate the greatest frustration from gaming, shopping, pornographic, and social networking sites. Note the marked similarity between the two groups, which differ in only one category each: social networking (undergraduates) and sports (experts). The two groups also indicated that they had the lowest toleration for search, news, weather, and vendor support sites, with experts also indicating they would tolerate little frustration from social networking sites.

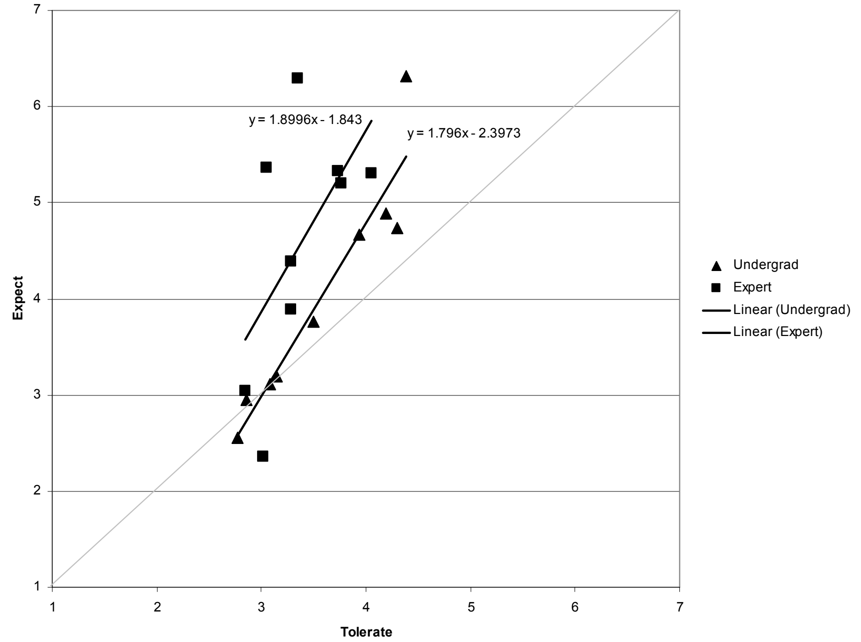

Figure 4. User expectations and tolerance levels for malicious interface techniques for two survey groups: undergraduates and experts. The long diagonal line indicates the point where toleration equals expectation. The smaller diagonal lines indicate the linear regression (and associated equation) for each group. Note that for the vast majority of site categories the degree of frustration the user expects from a site exceeds the self-reported tolerance. (1=None, 7=Extreme)

It is important to stress, however, the difference between survey participants' self-reported tolerance and expectations. The diagonal line in Figure 4 indicates the point where tolerance equals expectation. Tables 3 and 4 are sorted by the delta between expectation and tolerance. We expected results where tolerance would exceed expectation for most, if not all sites. However, in eight of the nine categories, for both groups, expectations exceeded tolerance. We believe this is because user desires do not equal the reality of the web where the most desirable content commands a significantly higher tolerance threshold, which interface designers exploit to their advantage. The most significant outliers, where expectation significantly exceeded tolerance, are the pornographic (expert and undergraduate) and social networking (expert only) categories, possibly because pornographic materials and social networking content is very desirable to many users and hence they will tolerate a higher level of annoyance. More routine content such as search and news commands less of a premium. An additional factor in the low toleration involving search may occur because Google has set an industry standard for a clean interface and unintrusive advertising, raising the bar for other search competitors. Also note that vendor support (experts) and weather (undergraduates) are the only categories with negative deltas which may indicate users would tolerate more annoyance than they currently receive. The actual tolerance thresholds are shown in Figure 4 using linear regression. Note that for both groups the slopes are very similar to each other, but steeper than the line formed when expectation equals tolerance. It is important to stress, however, that these lines indicate the tolerance thresholds for each group, on average. We believe tolerance thresholds vary from person to person.

An important future area of study is to gather data based on monitoring user actions vice self reported beliefs. In one possible scenario, users might be monitored during day-to-day activities and wouldn't know they were being tracked for tolerance and frustration levels.

4. COUNTERMEASURES

Malicious interface design has not gone unnoticed by end users, who employ a wide range of techniques in order to counter their effectiveness. This section explores these countermeasures by studying the techniques employed by expert users and presents results from a survey of 47 attendees of the BlackHat and DEFCON conferences. We chose these two events to solicit participants because of the high density of security and privacy aware subjects. Both venues attract early adopters of security countermeasures, and we believe this group should be surveyed in order to predict future trends as well as to evaluate effectiveness of existing countermeasures, including the establishment of an upper bound on their ease of use.

The survey asked participants to rate the ease of use (1=Very difficult to use, 7=Very easy to use) and the effectiveness (1=Not effective, 7=Very effective) of seven commonly available malicious interface countermeasures: pop-up blockers (such as those included in web browsers), text-only browsers (e.g. Lynx), personal proxies (e.g. Privoxy), third-party ad-blocking software, firewalls, browser plug-ins (e.g. NoScript, NoHistory, Greasemonkey) and anonymization networks (e.g Tor). In addition, survey participants were asked to list, and similarly rate, additional countermeasures that they employed, but were not explicitly listed on the survey. Table 5 summarizes the popularity of the various countermeasures as calculated from the survey results.

Technique	Number of Users	Percentage Usage
Personal Proxy	29	61.7%
Anonymization Network	33	70.2%
Firewall	35	74.5%
Text-only Browser	35	74.5%
Ad-Blocking Software	36	76.6%
Browser Plug-in	36	76.6%
Pop-up Blocker	45	95.7%

Table 5. Popularity of malicious interface countermeasures employed by 47 security experts.

	Ease of Use	Std Dev	Effectiveness	Std Dev
Personal Proxy	3.66	1.14	4.66	1.04
Anonymization Network	3.94	1.58	4.27	1.74
Firewall	4.29	1.72	4.54	1.48
Text-only Browser	3.23	1.93	4.60	2.09
Ad-Blocking Software	4.83	1.52	4.75	1.23
Browser Plug-in	4.61	1.17	4.88	1.08
Pop-up Blocker	6.50	0.75	4.73	1.27

Table 6. Countermeasure ease of use (1=Very difficult to use, 7=Very easy to use) and effectiveness (1=Not effective, 7=Very effective) as reported by security experts surveyed

While we anticipated the usage of the countermeasures we included on the survey, we were surprised by the range of write-in responses we received. Techniques included blocking JavaScript code, Flash objects and Java Applets, making use of cookie management software, employing WebSense web filtering, running anti-Spyware applications, editing host files to block DNS resolution of known ad serving sites, and using less popular browsers (Opera was specifically named). In addition, participants listed several anonymous browsing techniques including anonymous surfing live CD distributions, anonymizing proxies (e.g. Anonymizer.com), the utilization of public use terminals (such as those found in a library), and the (illegal) use of unsecured wireless access points. Informal discussions following the survey indicated participants believed that anonymous browsing helped reduce the effectiveness of targeted malicious interface techniques. In addition, participants suggested that webmasters and bloggers could help reduce the propagation of malicious interfaces by avoiding aggregating known malicious interface content providers in their websites and blogs.

Results for ease of use and effectiveness are shown in Table 6. Note that the average effectiveness rating for each countermeasure ranged from a low of 4.27 to a high of 4.88 on a scale of 1 to 7. We believe this tight grouping underscores the need for future study into more effective countermeasures, as no techniques was judged by the group as being very effective, even when employed by advanced users. There was however a much wider spread regarding ease of use, with personal proxies, text-only browsers, and anonymization networks receiving the worst scores. The clear ease of use winner was the pop-up blocker. This is probably because pop-up blockers are seamlessly integrated into popular web browsers and enabled by default. Because the survey studied an expert group, we believe these results indicate an upper bound on ease of use. Ease of use statistics for typical end users will likely be significantly lower due to lesser levels of technological expertise.

Figure 5 graphically compares the ease of use and effectiveness of each countermeasure. Note the relatively tight clustering of most techniques with the exception of the pop-up blocker outlier. The most effective countermeasure, by a slight margin, was the browser plug-in. We believe this is because of the wide range of security and privacy plug-ins that are available for browsers. This leads us to conclude that, in the context of the web, the best protection is seamlessly integrated, by default, into the browser. Ad-Blocking Software is a close second, because some browsers, such as the Firefox browser, allow easy integration of third-party ad-blocking software. It is important to note that the development of malicious interfaces and their respective countermeasures is a continual game of one-upmanship, both in terms of technological and non-technical solutions, so we regard these results as a snapshot in time.

We chose to focus the survey specifically on the web because the user is able to exert considerable control over their interface, both at the network level and at the application (i.e. browser) level. In many ways, this combination provides the user the greatest opportunity to employ countermeasures, as they are in control of many aspects of the information flow and the applications that generate the interface. In other, less advantageous domains, the user's ability to defend themselves is reduced, sometimes drastically, as is the case of traditional application software where the user controls very little of the interface. Off the desktop interfaces are often a more difficult problem, where the user may choose only to abstain from using a given fixed interface (e.g. avoid using a slot machine in a casino) or choose to frequent a competitor (e.g. choosing to visit a different gas station chain).

5. RELATED WORK

The primary focus of the human computer interaction community has been on creating usable, rewarding, efficient, and effective interfaces. The literature contains well established guidelines, models, heuristics, and evaluation techniques toward these ends. Representative examples include texts by Cooper [9], Dix [10], Nielsen [11], Norman [12], Shneiderman [13], and Tidwell [14]. The texts provide great coverage on how to properly design interfaces for the good of the user, but none provide more than anecdotal coverage of deliberately malicious interfaces. Some work focuses on educating novice designers by illustrating bad design such as Flanders [15], Johnson [16], and Nielsen [17], but the key distinction is that poor design is not malicious design.

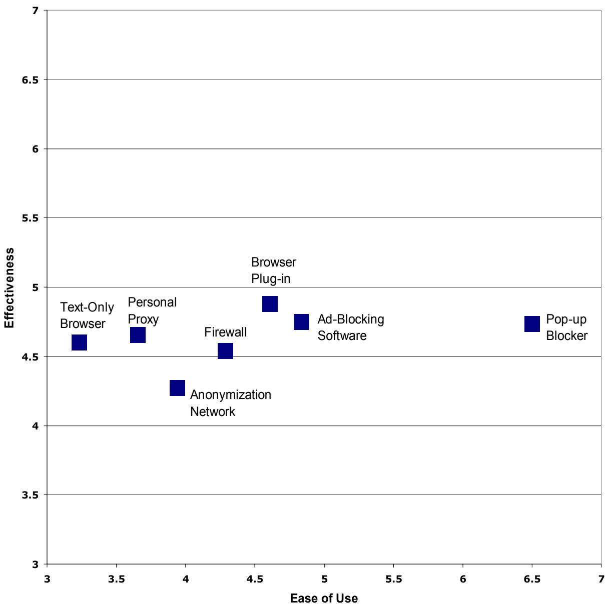

Figure 5. Comparison of ease of use (1=Very difficult to use, 7=Very easy to use) versus effectiveness (1=Not effective, 7=Very effective) as reported by surveyed security experts.

Early forms of malicious software interfaces manifested themselves in software applications as attempts to coerce users into upgrading, purchasing or registering shareware applications. Parberry categorized these applications as nagware (an application that frequently reminds the user to register), crippleware (an application in which key functionality is disabled), and heroinware (an application that includes enough functionality to get the user hooked, but lacks the full features of the complete application, as in a game that only provides the first three levels) [18].

The usable security research community, which studies the usability of security tools and the security implications of interfaces has covered three instantiations of malicious interface design: Spam, Spyware, and Phishing (both website and email based), but with primary emphasis on seeking countermeasures, principally by educating users, enhancing web browser interfaces with more intuitive interface techniques, and seeking attack resistant communication protocols. Representative examples include Good [19], Jagatic [20], and Sheng [21]. The literature does not focus on the broader problem of malicious interface design.

Other related work includes Conti [22], who demonstrated that information visualization systems may be manipulated if an attacker has the ability to inject information into a set of data being visualized and that even a small amount of such information allows non-trivial attacks against the user. Malicious interfaces differ in that the attacker is the creator of the interface, not a third-party who can influence data displayed by an information visualization system. Ahamad examined the notion of denial of information attacks, attacks that attempt to "intentionally or unintentionally consume human resources or mislead, confuse, or trick users into acting inappropriately or not acting when they should." [23,24] This work, however, did not consider the possibility of an attacker as the creator of the user's interface.

The phenomenon of banner blindness is related to our work in malicious interfaces because it illustrates a significant driving factor behind the increasingly aggressive interfaces users encounter. Benway first studied the topic in 1998 and demonstrated that users would accomplish tasks less well when required information was placed in a conspicuous banner on a web page [25]. Later work, involving eye-tracking tests, confirmed that users only focus on information they believe to be relevant and ignore content that appears to be an advertisement [26,27,28]. Nielsen explored the subject of banner blindness and, notably, observed that unethical design often pays off, ultimately drawing the conclusion that there are no secrets of usability and that one should not attempt to hide usability findings even if the result might encourage unethical behavior [29].

In the context of advertising, the need to penetrate a user's developed desensitized viewing techniques and divert him or her to make a purchase has led to study of "intrusive advertising." Unfortunately there is little publicly available information on the subject as almost all large online companies and advertising firms consider such information proprietary. One notable exception is Yahoo!'s Rohrer and Boyd who reported that Yahoo!'s User Experience Research Group is conducting research on both the effectiveness of its online advertising and on the impact that the advertising has on a user's experience [30]. The results of this research, which are effectively summarized by Nielsen in [31], are fairly startling. We commend Yahoo! for its described efforts to consider the user experience, but the fact the their reported data so strongly supports our premise leads us to conclude that many online companies that are dependent on advertising for revenue understand the negative impact of what they are doing and yet, they still continue to escalate the offensive and frustrating techniques that they employ in order to maximize their advertising click-throughs.

6. CONCLUSIONS AND FUTURE WORK

We recommend future work in a number of areas. Metrics, with data preferably gathered by automated means, are important in order to measure and rank the malicious content found in websites. Researchers should also consider developing more effective and easy to use countermeasure tools that can detect the presence of malicious interface elements and help reduce or eliminate their impact. Gathering data on user tolerance and frustration levels, both from further surveys as well as monitoring user actions, is another important line of research. Additionally, a promising area is to explore and measure the impact of malicious interfaces in person-to-person interactions. In other words, are users injured by malicious interfaces in ways that reduce their ability to interact with other humans. For example, are sensory gating techniques employed while using the web impacting face-to-face human communication? Finally, we intend to continue our study into the privacy implications of malicious interfaces and online information disclosure [32].

Malicious interface techniques are commonplace both on and off the desktop, and are in direct contradiction to usable interface design best practices as well as several laws and statutes. Techniques include: coercion, distraction, exploiting errors, forced work, obfuscating desired content, restricting or masking functionality, and deception or misrepresentation, among others.

In particular, web users are subjected to a wide range of malicious interfaces on a near-continuous basis, drastically degrading the usability of the web. In some cases, the reduction in usability is so severe that some of the most vulnerable users may be effectively barred from using parts of the web. We believe the motivation for malicious interface designers is predominantly to maximize profit, and they execute this intent by putting their goals ahead of the user.

Users will not tolerate malicious interfaces without bound, but instead make a cost benefit analysis, where they weigh the value of accomplishing their goal against the pain the interface designer inflicts upon them. If the pain exceeds the perceived value of task accomplishment, the user will be driven to find other means to accomplish their task, usually by visiting an entirely different website, using a different software application, or another service provider. The degree of annoyance a user will tolerate varies significantly based on content, ranging from very little tolerance when conducting web searches or seeking vendor technical support to very high tolerance when visiting gaming, shopping, sporting, and pornographic sites. We believe the malicious interface designer seeks to understand and operate just under a user's tolerance threshold, approaching it asymptotically in a belief that doing so maximizes profit.

Users employ a wide range of countermeasures including personal proxies, pop-up blockers, text-only browsers, ad-blocking software, and browser plug-ins, among others, but expert users evaluate their effectiveness as only marginal. The end result is that a large percentage of the interfaces found on the web successfully exploit the user, and even the most technically savvy can only partially protect themselves. Less adept users are largely defenseless and must rely on default browser behavior such as integrated pop-up blocking. In some cases, particularly in traditional software applications and off the desktop physical interfaces, developing effective technological countermeasures may be extremely difficult, because the interface designer completely controls the environment. Malicious interfaces are extremely prevalent in a variety of contexts and a deeper understanding is required by human computer interaction and security professionals as well as end users in order to counter and mitigate their impact.

7. ACKNOWLEDGMENTS

We would like to thank the BlackHat, Dartmouth, DEFCON, HOPE, and West Point communities for their support and feedback regarding this research. In particular, we would like to thank Gillian "Gus" Andrews for her encouragement and valuable feedback.

8. REFERENCES

[1] Rogers accused of hijacking other web pages. Canadian Broadcasting Corporation News, 11 December 2007. http://www.cbc.ca/technology/story/2007/12/11/tech-rogers.html, last accessed 1November 2009.

[2] Road Runner Intercepting Domain Typos. Slashdot, 26 February 2008. http://slashdot.org/article.pl?sid=08/02/26/1741253&tid=95, last accessed 1 November 2009.

[3] Kaminsky, D. Black Ops 2007: Design Reviewing the Web. Black Hat USA, 2007.

[4] Web Accessibility Initiative. World Wide Web Consortium, 16 July 2008. http://www.w3.org/WAI/, last accessed 1 November 2009.

[5] Disability Discrimination Act 1995. Office of Public Sector Information, United Kingdom. http://www.opsi.gov.uk/acts/acts1995/ukpga_19950050_en_1#19, last accessed 1 November 2009.

[6] Americans with Disabilities Act Home Page. United States Department of Justice, 25 July 2008. http://www.ada.gov/, last accessed 1 November 2009.

[7] The Rehabilitation Act. United States Department of Education , 13 December 2004.

[8] Poulsen, K. Hackers Assault Epilepsy Patients via Computer. Wired, 28 March 2008. http://www.wired.com/politics/security/news/2008/03/epilepsy, last accessed 1 November 2009.

[9] Cooper, A., Reimann, R., and Cronin, D. About Face. Wiley, 2007.

[10] Dix, A., Finlay, J., Abowd, G., and Beale, R. Human-Computer Interaction. Prentice Hall, 2003.

[11] Nielsen, J. Designing Web Usability. Peachpit Press, 1999.

[12] Norman, D. The Design of Everyday Things. Basic Books, 2002.

[13] Shneiderman, B. and Plaisant, C. Designing the User Interface. Addison-Wesley, 2004.

[14] Tidwell, J. Designing Interfaces, O'Reilly, 2005.

[15] Flanders, V. and Peters, D. Son of Web Pages That Suck. Sybex, 2002.

[16] Johnson, J. GUI Bloopers 2.0. Morgan Kaufmann, 2007.

[17] Nielsen, J. and Tahir, M. Homepage Usability. New Riders Press, 2001.

[18] Parberry, I. The Internet and the Aspiring Games Programmer. Proceedings of DAGS 95, Electronic Publishing and the Information Superhighway, pp. 155-159, 1995.

[19] Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. Symposium on Usable Privacy and Security, 2005.

[20] Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. Social Phishing. Communications of the ACM, Vol. 50, Issue 10, pp. 94-100.

[21] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., and Nunge, E. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. Symposium on Usable Privacy and Security, 2007.

[22] Conti, G., Ahamad, M., and Stasko, J. Attacking Information Visualization System Usability: Overloading and Deceiving the Human. Symposium on Usable Privacy and Security, 2005.

[23] Ahamad, M., Mark, L., Lee, W., Omicienski, E., Dos Santos, A., Liu, L. and Pu, C. Guarding the Next Internet Frontier: Countering Denial of Information Attacks. New Security Paradigms Workshop, 2002.

[24] Conti, G. and Ahamad, M. A Taxonomy and Framework for Countering Denial of Information Attacks. IEEE Security and Privacy. November/December 2005.

[25] Benway, J. and Lane, D. Banner Blindness: Web Searchers Often Miss "Obvious" Links. Internetworking, Issue: 1.3, December 1998.

[26] Bayles, M. Just How 'Blind' Are We to Advertising Banners on the Web? Usability News, Vol. 2, Issue 2, July 2000.

[27] Norman, D. Commentary: Banner Blindness, Human Cognition and Web Design. Internetworking, Issue: 2.1, March 1999.

[28] Pagendarm, M. and Schaumburg, H. Why Are Users Banner-Blind? The Impact of Navigation Style on the Perception of Web Banners. Journal of Digital Information, Vol. 2, No. 1, 2001.

[29] Nielsen, J. Banner Blindness: Old and New Findings. Alertbox, 20 August 2007. http://www.useit.com/alertbox/banner-blindness.html, last accessed 1 November 2009.

[30] Rohrer, C. and Boyd, J. The Rise of Online Advertising and the Response of User Experience Research at Yahoo!. Extended Abstract. Conference on Human Factors in Computing Systems, 2004.

[31] Nielsen, J. The Most Hated Advertising Techniques. Alertbox, 6 December 2004. http://www.useit.com/alertbox/20041206.html, last accessed 27 July 2008.

[32] Conti, G. and Sobiesk, E. Malicious Interfaces and Personalization's Uninviting Future. IEEE Security and Privacy, May/June 2009.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the United States Government.