AN E-TAX INTERNET FILING SYSTEM INCORPORATING SECURITY AND USABILITY BEST PRACTICES

Prototype implementation of the best practices identified in government and commercial E-tax filing websites in the USA for tax season of 2003

Aashish Sharma, William Yurcik
National Center for Supercomputing Applications,University of Illinois, Urbana-Champaign, USA

Keywords: security, usability, e-commerce, online-tax filing websites.

Abstract: We describe a prototype system we have developed that incorporates best practices identified from a 2003 study of both public and private E-tax filing websites hosted in the USA. Our motivation is to investigate the current low functionality and low penetration usage of online tax filing, an increasingly important web-application. We identify critical security and usability features in current use on E-tax filing websites (and use these features) as well as new features not found on these E-tax filing websites. We conclude that while appropriate and correctly implemented technology will make a website secure, in practice it is the website look-and-feel which has the most influence on a user's perception of usability and security.

1 INTRODUCTION

Electronic Tax (E-tax) filing adds a significant dimension to E-government initiatives by harnessing the transaction speed and cost-effectiveness of the Internet. Most of the states (38) in the U.S. have started E-tax state revenue websites and in the last few years online tax filing has experienced substantial growth.

However, the majority of the tax filing population is still reluctant to file their tax returns via a computer. In this paper we posit and seek to provide evidence that people perceive current E-tax filing websites to be difficult to use and insecure. Since average citizens are encouraged to use online E-tax filing websites (IRS plans to get as much as 80% of tax returns filled electronically by 2007) the need to make E-tax filing usable and secure for untrained users has become critical.

At present there is a disparate use of usability and security features in online E-tax filing websites. To better understand these design decisions, we studied 38 state websites and 15 private online E-tax filing portals. Most of these websites are well designed by general web standards and available usability guidelines; however, we highlight flaws that make many of these websites unusable and perceived as insecure for this specific application. domain (tax filing). We leverage previous work on security usability to derive standards based on design security usability features prevalent in these websites. Lastly, the significant contribution of this paper is taking the best practices we have identified in this application domain and implementing them in a working E-tax filing prototype for evaluation and further testing.

The remainder of this paper is organized as follows: Section 2 documents related work in security usability (we were unable to identify any previous work specifically on E-tax filing websites). We present the process of online E-tax filing in Section 3. Section 4 focuses on the security mechanisms and usability features employed by state and private websites. We discuss prototype implementation challenges in Section 5 followed by a brief discussion on future work in Section 6. We end with a summary and conclusions in Section 7.

2 RELATED LITERATURE

There has been substantial research done in the field of security usability and creating trust on the Internet [Adams, A. et al 1999] [Neilson, J. 2000]. [Whitten A, Tygar J.D., 1999] describes the usability issues with the Email encryption package PGP 5.0. While one would expect security applications would be hard to use by novices, this study shows experts also

Sharma A. and Yurcik W. (2004).
AN E-TAX INTERNET FILING SYSTEM INCORPORATING SECURITY AND USABILITY BEST PRACTICES - Prototype implementation of the best practices identified in government and commercial E-tax filing websites in the USA for tax season of 2003.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 257-262
DOI: 10.5220/0001388002570262

found security applications hard to configure and use. This study highlights a wide gap between design perspectives and usage habits.

E-tax filing website designers have tried to incorporate security features, however, users misinterpret, overlook, and/or perceive these features in unintended ways. [Princeton Survey Research Associates, 2002] describes how users on one hand desire obvious security mechanisms on the websites where they wish to transact, but on the other hand subvert these systems for usability and often give up on applications out of desperation.

We think that these problems can be avoided in the online E-tax filing websites by a balanced mixture of "visible" security mechanisms and usability features. A perceptually secure website will encourage website credibility and user trust in online E-tax filing transactions. [Fogg, B.J., 2002] reveals that unlike evaluation of other systems, Internet users do not use rigorous evaluation schemes but rather focus on general design, appearance, structure and content in the order to assess trust of websites. For instance, one way users evaluate a website is by joining together two pieces of information, one piece may be something specific that catches their attention and the second piece may be a judgment about its credibility. We believe users of online E-tax filing websites adhere to this prominence-interpretation theory.

Consumer WebWatch [Consumer WebWatch 2004] has many examples of inconsistent user criteria for assessing websites. While users may have ideal expectations before they arrive at a website, demand for clear, specific and accurate information is often sacrificed but it does not mean that these users are always aggressive in seeking this information.

Efforts have also been made in developing community/group efforts for accessing websites by creating reliable reputation reporting mechanisms for online communities [Dellarocas, C., 2001]. [Yurcik, W. et al 2002] [Turner, C. et al 2001] have also discussed factors that affect perceptions of security of E-Commerce websites in their study.

In effort to further understand attitudes about online privacy and security AT&T conducted a study [AT&T] emphasizing categorization of some data to be of more importance than other data. For instance, users are less reluctant to provide their postal address than their active email address than their telephone numbers. This report also shows that behaviour changes according to the application domain. For example, attitudes for accepting cookies differ with the type of website

3 E-TAX FILING SYSTEMS

There are two basic approaches to E-tax filing over the Internet: (1) interactive filing and (2) batch filing. In interactive filing, the taxpayer interacts directly with a web-based application to complete the tax filing online. We have observed that in general these interactive filing websites vary from a conversational question-and-answer format customized to the taxpayer's prior filing history (pull-down selections) to a fill-in-the-blanks application where a paper tax form is simply reproduced on a web display. When the information is complete, the taxpayer submits the data for processing. Payment information, such as bank accounts for direct debit payments or direct deposit of refunds, or credit card information, may be combined with the E-tax filing application.

Within the interactive method of Internet filing, there are two alternative technologies: (1) the taxpayer interacts directly with the web server hosted by the tax authority or a third party (which is generally an IRS authorized free-file-partner), with only a web browser on the taxpayer's machine; or (2) the taxpayer downloads tax preparation software from the website to the taxpayer's machine. The taxpayer completes the filing offline, then reconnects to the host website to upload the completed filing.

In batch filing, the Internet is simply used as the network over which tax transaction is transmitted. An offline data file is created by a software program, which is either a generalized program such as a spreadsheet, or a specialized tax preparation package. Most taxing authorities also provide copies of their forms, in downloadable format, on the websites. Many offer online inquiry into the status of individual income tax refunds. The more advanced administrative uses of the Internet, however, center on the areas of account maintenance and customer service.

De facto standards for security of interactive web-based applications include the use of PINs or passwords, and the use of secured socket layer (SSL) for sender-to-receiver encrypted transmission. PINs are issued to taxpayers by an independent method (usually hardcopy postal mail) and/or are verified against a database by the Internet application. Although SSL provides some measure of security for Internet transmission, it does not authenticate the sender. PINs can be stolen from the mail or lost or compromised by the taxpayer.

4 SECURITY AND USABILITY

We used cognitive walk-through technique to review the user interface and security mechanisms directly on state and private websites and noted the security mechanisms and usability features employed by these websites. Cognitive walkthrough is a usability evaluation technique modelled after the software engineering practice of code walkthroughs. To perform cognitive walkthroughs we step through these websites as if we were novice users, attempting to simulate transactions and identifying errors, probable areas of confusion; and subjectively interpreting the security cues.

Although our analysis is most accurately described as a cognitive walkthrough, it also incorporates aspects of another technique called heuristic evaluation [Nielsen, J., 1994]. In this technique, the user interface design is evaluated against a specific list of high-priority usability principles and desirable features that we have identified on these websites. Our evaluation also draws on our experience as security researchers and additional background in educating novice computer users. Some of the features we identified by this combined process of cognitive walkthrough/ heuristic evaluation/experience of these websites are listed in the Table 1.

Table 1: E-Filing Security Mechanisms

SECURITY MECHANISMS	Percentage present	
	State (38)	Private(15)
SSL Encryption (https)	100%	100%
authentication mechanism a. IRS PIN + password b. login + password	56%	54%
third party trust symbols	0%	100%
affiliation with IRS	100%	100%
Secure and insecure zones	0%	20%
Security and Privacy policy	100%	100%
Reverse Turing Test (RTT) for protection from automated attacks	0%	0%
post submission data handling policies and acknowledgements	no mention	
statements/disclaimer on the site availability	10%	0%

4.1 Security Mechanisms

4.1.1 Security Connections

SSL was employed on all the websites (state and private) for the secure communication and is notably highlighted on all the sites. Users invariably assume that establishing a SSL connection makes their data secure, however, it only guarantees the identity of the other machine to which the user is connecting. There have been many cases where users/browsers are fooled to connect to a malicious site. In our prototype we have also created our own certificate authority and issued our own certificates. Browsers like Microsoft Internet Explorer and Netscape Navigator show the certificate to the user. With a more sophisticated attack like DNS (domain name service) spoofing, a user is presented with a certificate for a "secure" SSL connection and yet transparently redirected to a malicious third-party server. Thus reliance only on SSL for security is dangerous – a multilevel security approach is preferred.

In our prototype we have taken the approach of creating zones to help users build a mental model for establishing secure connection.

The https protocol provides a padlock symbol (🔒) at the bottom of the browser's window but this is small and often goes unnoticed. We were unable to find any websites that encrypt cookies along with an SSL connection.

4.1.2 Authentication mechanism

In order to restrict access to an E-filing transaction to legitimate users each website employed differing authentication mechanisms. Most of these authentication mechanisms were keyed primarily on a Social Security Number However, we also observed some sites allowing a user to choose a username of choice or supply a PIN printed on their tele-file pamphlet they receive in mail (in addition to Social Security Numbers).

In our prototype we have required the users to register with the online E-tax filing program. We allow them to create their own password to log on with social security number and a pin supplied to them by IRS.

As shown in Figure 1, our prototype incorporates a Reverse Turing Test (RTT) to deter automated brute force dictionary password attacks on our authentication mechanism. RTT requires a distorted but human-recognizable word or phrase embedded in a graphic be input after supplying a wrong password a given number of times [Ahn, L. 2004] [Kavassalis, P. et al 2004]. RTT is employed by E-commerce websites such as Paypal and Yahoo mail to ensure a human user is attempting authentication as opposed to a machine. We feel strongly that E-Tax filing websites should adopt RTT as a security mechanism to stop automated brute force attacks.

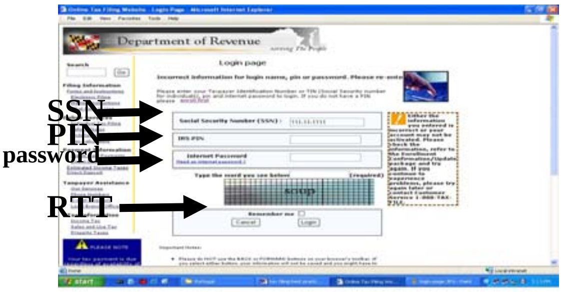

Figure 1: A Reverse Turing Test along with authentication mechanism on the prototype E-Tax Filing Website.

4.1.3 Third party trust symbols

Third party trust symbols are not an accurate security gauge for several reasons. The foremost reason is that most websites using trust symbols have placed these symbols along with advertisements that users tend to ignore. We have also found misuse of third party symbols that are completely superficial (graphic image with no verification links). Third party trust symbols are more prevalent on private tax filing websites as compared to government websites. The most logical explanation is that government websites carry credibility of their own.

In a particularly important instance, the IRS has its own *"e-file"* picture and has encouraged its partners in the free-file-alliance to use this graphic as a trust symbol. This graphic lacks the verification system and anyone can copy this image and put it on their website - there is virtually no way to determine if the IRS has approved usage of the symbol on a particular website.

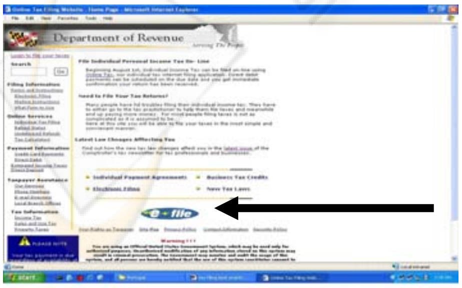

Figure 2: "e-file" 3rd party symbol issued by the IRS

We have refrained from using third party symbols on our prototype. Instead we have encouraged links to the authoritative web pages on the official IRS website which describes its free-file-alliance. This makes a cross-site verification with the IRS website. This particular system would also stop any abuse of the *"e-file"* graphic symbol issued by IRS.

4.1.4 Privacy Policies

[Fogg B.J., 2002] in their study also note that users tend to aggressively look for a privacy policy on a website, however, this does not necessarily mean that users also read them. All of the states and private tax websites have stated privacy and security policies. We have, however, found some discrepancies in the system of privacy policies. In certain E-tax filing websites, multiple subcontractors are handling tax-data collection, tax data submission, and help desk responsibilities - with each subcontractor having their own privacy policies.

In our prototype we have provided a direct link to both a privacy and security policy. We have also provided a link to the applicable privacy/security laws for the appropriate jurisdiction. We feel that government websites have an opportunity to leverage on access to legislation in order to distinguish themselves from private contractors and thus attract more people to use their website.

Figure 3. US Federal Privacy Act along with privacy/security policies of local site

4.1.4 Post tax-filing procedures

It is mandatory by US Federal law for the IRS and other tax filing websites to acknowledge the receipt of the returns filed by the taxpayer. If the taxpayer does not get a receipt, taxes are not officially considered as "filed". The standard way of acknowledging receipt of the tax data is via Email but in our prototype we supplement an acknowledgment Email with additional information including links to important FAQs and contact information. Email sent should not be flashy or give the feel of a spam to the users. The purpose is to provide feedback in order to facilitate taxpayer confidence in the system.

4.2 Usability features on the websites

Table 2. E-Tax Usability Features

USABILITY FEATURES	Percentage present	
	State (38)	Private (15)
eligibility criteria	100%	vague
hw/sw requirements detailed	100%	100%
usage guidance provided	50%	10%
demonstration present	30%	20%
FAQ listed	80%	50%
contact information listed	100%	100%
post-submission data handling policies	0%	0%
site availability statement	20%	0%
all prices quoted with no hidden costs	100%	10%

4.2.1 Application usage and eligibility criteria

The tax system in the United States is one of the most complex and hence it is difficult to provide universal GUI interfaces for E-Tax filing – there are multiple categories a taxpayer may use. Eligibility criteria, thus, becomes important. Taxpayers would reject a website that would not notify the user about eligibility before inputting a substantial amount of data. We found that eligibility criteria has not always been placed at visible locations, with some websites putting it in an FAQ section assuming that everyone accessing the website reads the FAQs first before starting.

In our prototype we have emphasize eligibility criteria. The most visible place seems to be the initial user enrollment forms and the login screen.

4.2.2 Demonstration Present

It is common for humans to loose sense of direction or location in a hypertext environment due to additional effort and concentration necessary to maintain several tasks simultaneously - cognitive overload. A demonstration is an important part of E-Tax filing websites since this application is new to most of users. In addition, users have a general curiosity about how exactly the system works. Some people want to find out how the system works before deciding to use it.

The advantage of a demonstration is that it facilitates mental models about the application. It helps users create a mental navigation map and supports an ability to keep conscious track of the links. Upon seeing a demonstration a user can become aware of what to expect when actually using the online E-Tax website to file taxes.

4.2.3 FAQs

Users, especially first time users, have questions about the entire system process. FAQs on the website helps bolster confidence by providing answers to anticipated questions. Another advantage is the reduction in customer support calls. Most E-Tax websites have an FAQ section. Often the information is available elsewhere on the website but the redundancy is outweighed by the benefit of answers to common questions in one place. As a warning of what to avoid, we have observed some websites with detailed FAQs in one large html file with no subsections or categorization such that it is virtually unsearchable.

The FAQ section is an important component of an E-Tax website (similar to an address book is for an email application), however, the FAQ should be designed based on topical relevance. A proper categorization of information with an effective search mechanism is required. Lastly, the FAQ link should be placed prominently.

5 IMPLEMENTATION CHALLENGES

Due to a heterogeneous user base, creating user awareness and training are difficult tasks. The same effect can be accomplished by standardizing the E-Tax filing mechanisms, content organization, and GUI look-and-feel. Our prototype is a first attempt in this direction.

Another challenge is the capability of supporting a variety of user hardware/software configurations, as well as the capability to update the host application at will without concern for what version is on the taxpayer’s machine.

Availability is another big challenge for the E-Tax filing websites. As the deadline for submission nears, the number of people trying to access these websites is going to increase exponentially.

Due to the importance and nature of the E-Tax filing application, these websites are a high potential target for cyber attacks such as denial of service attacks and identity theft.

Finally, it should be noted that the Internet is not reliable, that is, there is no guarantee that any particular message will reach its destination. For this reason, it is imperative that the E-Tax filing websites build some form of acknowledgement mechanism into all transactions. The taxpayer should be educated to understand that the tax filing has not been completed until the confirmation number or acknowledgment is received in return.

6 FUTURE WORK

We feel that in order for an Internet E-Tax system to be successful, there is a strong need for large-scale authentication. The IRS and several states have piloted Public Key Infrastructure (PKI) applications with some success, but they have also reported concerns regarding the ability to correctly install and manage digital certificates. Some tax authorities are considering becoming certificate authorities themselves, and assigning key pairs to taxpayers at no charge. These keys may reside on a server or personal computer, or they may reside on a card or some form of token, which must be read at every transaction. Biometric forms of security and authentication, such as a fingerprint or retinal scan, will become inexpensive and widely used.

There is also a need for incorporating sophisticated logging and auditing capabilities for user feedback, error detection, error recovery, and forensic investigation.

Another approach that remains to be tested for E-Tax filing is allowing the taxpayer to download tax preparation software from a website to the taxpayer’s machine. The taxpayer completes the filing offline, then reconnects to the host website to upload the completed filing. Advantages of this method include the ability of the taxpayer to store the filing on the taxpayer’s machine for future reference. Disadvantages include the need to accommodate various versions of the software to match taxpayer hardware/software configurations, and the need for customer assistance staff to support the download and installation processes.

7 CONCLUSIONS

Online E-Tax filing is gaining acceptance in society but there is still a long way to go. Most tax filing systems are complex with traditional filing by paper through the postal mail. Internet filing is a fundamental change and the reluctance of people to use such a new system is to be expected. However, there are features that can be addressed immediately and effectively in the design of an E-Tax filing website to encourage security and usability.

In this paper we studied many Internet E-tax filing websites and identified best practices for security and usability. We highlighted the discrepancies between security and usability in E-Tax filing websites and then addressed the problems we found by building a prototype E-Tax filing application to simulate and test our solutions. We conclude with the primary observation that visible security mechanisms most effectively bolster user trust with multiple instances highlighted within our analysis and prototype.

REFERENCES

Adams, A., Sasse, M. A., December 1999, Users Are Not the Enemy, Comm. of ACM, Vol 42/No 12.

Ahn, L. V., Blum, M., Langford, J., February 2004, How Lazy Cryptographers Do AI, Comm. of the ACM, Vol 47/No.2.

AT&T Labs-Research, Beyond Concern: Understanding Net User’s Attitudes About Online Privacy, Technical Report, TR 99.4.3

Consumer WebWatch http://www.consumerwebwatch.org/

Dellarocas, C., 2001, Building Trust On-Line: The Design of Reliable Reputation Mechanisms for Online Trading Communities. http://ebusiness.mit.edu

Fogg B.J., 2002, Stanford-Makovsky Web Credibility Study 2002 Investigating What Makes Web Sites Credible Today.

Kavassalis, P., Lelis, S., Rafea, M., Haridi, S., February 2004, Telling Humans and Computers Apart Automatically, Comm. of ACM, Vol 47/No 2.

Nielsen J. Security and Human Factors. Jakob Nielsen’s Alertbox, November 2000. http://www.useit.com/alertbox/20001126.html

Nielsen, J., 1994, Heuristic Evaluation In Usability Inspection Methods, John Wiley & Sons, Inc.

Princeton Survey Research Associates, 2002, A Matter of Trust: What Users Want From Web Sites, Research Report.

Turner, C., Zavod, M., and Yurcik, W., 2001, Factors That Affect The Perception of Security and Privacy of E-Commerce WebSites, 4th Intl. Conference on Electronic Commerce Research (ICER-4), Vol 2, pp. 628-636.

Whitten A, Tygar J.D., 1999, Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0, 9th USENIX Security Symposium.

Yurcik, W., Sharma, A., Doss, D., 2002. False Impressions: Contrasting Perceptions of Security as a Major Impediment to Achieving Survivable Systems, IEEE/CERT/SEI 4th Information Survivability Workshop (ISW).