EcomRISK.org: An E-Commerce Security Resource

Fillia Makedon, Carey Heckman, Adeel Meer, Tilmann Steinberg, Lin Wang, Song Ye, and Yan Zhao
The Dartmouth Experimental Visualization Laboratory (DEVLAB)
Department of Computer Science
Dartmouth College
6211 Sudikoff Laboratory
Hanover, NH 03755, USA
makedon@cs.dartmouth.edu

Abstract

As the Internet continues to play an increasingly important role in supporting business-to-business and business-to-customer transactions, it is crucial for the participants in these transactions to be informed about and to understand the involved risks and how to guard against them. Most websites presenting Internet and e-commerce security issues provide only specific, technical information aimed at system specialists, leaving out a more interdisciplinary audience of business professionals and entrepreneurs. The EcomRISK.org resource was created to fill this need, by providing an educational background for a more general audience, as well as the means of communicating concerns, problems, and solutions between users and experts, and research tools for future development.

1. Introduction

Electronic Commerce (e-commerce) methods and tools provide business solutions based on the use of the Internet [2, 3]. As e-commerce growth has paralleled the explosive growth of the Internet, the problems and potential for crime that are inherent with the use of the Internet have resulted in a loss of trust in e-business and consequently large-scale economic damage. [4, 5, 6] To counter this, new mechanisms are needed that will review e-commerce risks on a continuous basis and facilitate the education and involvement of the general public. The EcomRISK.org security resource [7] aims to become such a facilitator by collecting and presenting the different types of e-commerce risks, and offering contacts to experts who are producing solutions to these risks.

Aside from providing an educational resource, EcomRISK.org collects input and feedback from users and experts, which is a valuable source of information about the needs and possibilities of Internet use. By mining these data, patterns and correlations can be discovered and applied to facilitating or finding new solutions.

We describe an approach to process user inputs and queries. For different users with different understanding of the incidents they want to submit, we provide different submission forms. A flexible query interface is provided for users to search the incidents they are interested in. User activities on our website are recorded and analyzed. Based on this information, we can provide better service for users.

In this paper, we first look at several existing sites that already provide information about Internet security to specific audiences. Section 3 outlines the approach of the EcomRISK.org resource and describes the basic elements used to collect and disseminate information. In Section 4, the details about the incident classification and collection tools are given. Section 5 concludes the paper and outlines future work.

2. Related Work

There are several other websites that provide security resources to the online community. In table 1, we present a short overview of several prestigious sites and contrast their offerings with those of the EcomRISK.org site.

Proceedings of the 4th International Workshop on Computer Science and Information Technologies CSIT'2002
Patras, Greece, 2002

Web Site	Organization	Audience	Technical Level	Primary Focus	Component
EcomRISK.org	Education (.edu)	general computer users professionals & experts	low	risk incident database; discussion forum; news; tutorials; tech reports	education
CERT.org	Education (.edu)	professionals & experts system administrator	medium	risk incident database; security tutorials	technical
SANS.org	Industry (.com)	professionals & experts system administrator	high	discussing forum; vulnerabilities database	technical
SERIAS.purdue.edu	Education (.edu)	general computer users professionals & experts	low	security seminar; post-secondary education	education
neohapsis.com	Industry (.com)	clients	high	vulnerabilities database; articles; archives	consulting
securitysearch.net	Industry (.com)	professionals & experts	medium	articles & tutorials, security product reviews; software listings	technical
NIST.org	Government (.gov)	policy makers federal government agencies	medium	information on different subjects	policy
NISER.org	Government (.gov)	general computer users professionals & experts	medium	news & events; services; articles; trainings; incidents submission	consulting

Table 1. Comparison of EcomRISK.org to major, established web sites.

The following sites are tightly related to EcomRISK.org and provide additional information potentially useful to EcomRISK users.

GREeCOM.org: GREeCOM.org (the center for Global Research and Education in e-Commerce) is the parent site for the DEVLAB's e-commerce project. It handles user management, global searches, and special features.

eJETA.org: eJETA.org is the website of the Electronic Journal for E-Commerce Tools and Applications, an online-only journal hosted at the DEVLAB with articles by experts in various e-commerce issues.

ISTS: The Institute for Security Technologies Studies (ISTS) at Dartmouth is funded by the Department of Justice and "studies threats to electronic information infrastructure systems and technologies of the United States, and seeks appropriate and effective technological preparedness, response and recovery actions, as well as training and information needs" [10]. The EcomRISK.org resource is part of this program.

3. Approach

The EcomRISK.org resource is threefold: education and communication, and research. Each of these components has a clear goal by itself, but can link into relevant sections of the other components; for example, a learning module in the educational component can refer to a specific entry in the risk incident database or a discussion thread to give the user a broader context.

3.1 Educational Component

The main goal of the educational component is to raise awareness of problems and dangers of e-commerce, and to provide answers to common and specific answers. While the EcomRISK.org website does not contain all the answers, it is designed as a launching pad and can refer the user to other sites that contain more specific information. Within the site, a variety of features are designed to enable the user to become more familiar with the issues involving security in e-commerce, to stay on top of recent developments (e.g. the introduction of new security protocol for web browsers), and to read all this information in an understandable language with references for the technical terms.

Link Library: The link library is a collection of important or interesting websites that contain additional or specific information about e-commerce security. Grouped by topic and level of importance, the library is searchable by keywords.

Newsfeed: The Institute of Security Technology Studies (ISTS) [10, 11] features a Newsfeed of security, technology, and policy news. EcomRISK.org archives this Newsfeed and allows for searching and browsing these news items by topic, keyword, date, or source.

Technical Reports: EcomRISK.org maintains a set of papers written by experts and students on a variety of topics, ranging from overviews of given areas (such as copy protection) to specific research of a single item of interest (?).

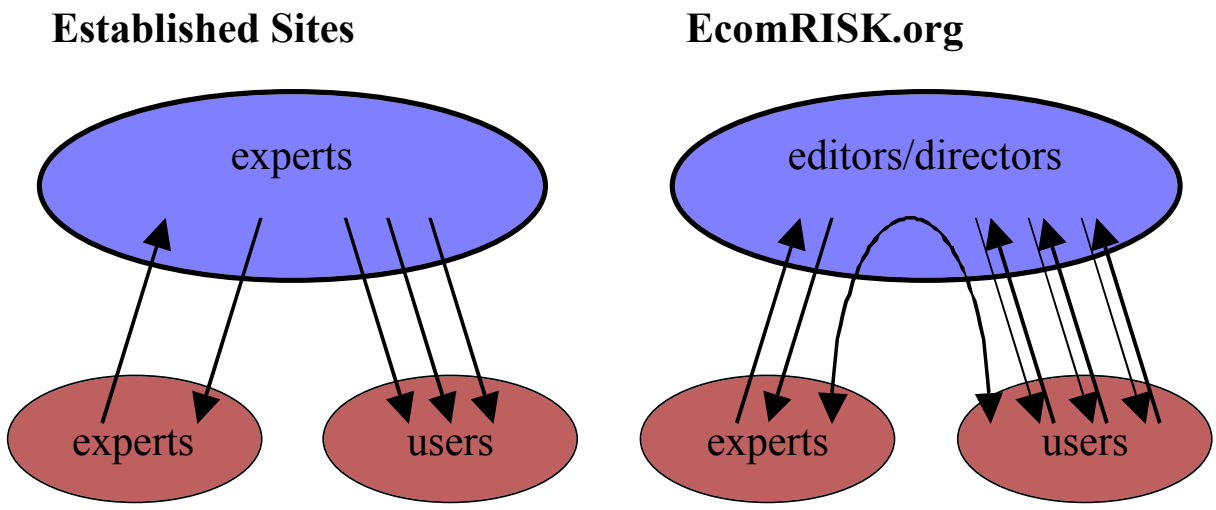

Figure 1. Difference in information flow between established sites and EcomRISK.org: while most sites facilitate traffic *to* users only, EcomRISK.org encourages contributions from users and forwards these to participating experts.

Course Guide: This part of the EcomRISK.org website aims to provide a list of available courses matching the needs of the user. By selecting parameters such as length of course or topic area, the user can find the right course.

3.2 Communication Component

The communication component facilitates the exchange of ideas between users and experts in a manner beneficial to both sides (see Figure 1). Rather than merely establishing contact between users and experts, the site handles all communication so as to shield the experts from too much user input, maintaining a high level of quality in conversation and exchange. Furthermore, this allows us to catch developments and shifts in focus and act accordingly, and make past communication available for future reference through archiving.

One important feature of this communication component is that information flows in both directions. Users have access to experts and can provide them with feedback for their solutions, while experts get to see what problems the users need answers for.

Announcements: This part of the EcomRISK.org site is used to provide a variety of announcements to users. These include urgent virus warnings (with references to the appropriate sites), calls for participation in research or testing, or notification of programs or courses, among others.

Forum Discussion: As the main part of the communication component, the forum discussions are initiated by EcomRISK.org moderators. In order to post, a user has to be registered; status information about the user is included with each posting to give additional credibility to the posted content.

One crucial component of good communication on an online forum is the presence of a moderator to control the quality of the content. Semi-automated systems such as Slashdot encourage quality but do not guarantee it; on the other hand, a fully moderated system (where all submissions must be approved before becoming visible) is detrimental to quick exchange of ideas.

User Management & Protection: EcomRISK.org requires users to register in order to validate their identity. The basic formula dictates that the more a user's identity has been validated, the more it is taken into account when adding credibility to the user's contributions. At the same time, users are given protection from abuse of their online presence by limiting communication through the EcomRISK.org site to other users only.

3.3 Research Component

The research component aims to provide a single, uniform collection of actual e-commerce risk incidents and solutions that can be easily browsed, searched, and extended. By looking at the existing cases, the user can get an overview of what risks have been identified so far, and what tools are available to counter or protect against these risks. The goal is automatic incident analysis: collection and classification of e-commerce incidents into incident types. Finally, a survey system allows us to profile our users, identify crucial areas and main concerns, and collect demographics.

Risk Incident Database: The risk incident database captures specific cases of e-commerce problems or abuse. The categories described in [1] are used as a foundation for our classification of what flaw caused the problem, when and where it was introduced, and how it was resolved (including the costs involved). A mix of multiple

choice questions and free text answers allows for both automated classification and inclusion of case-specific information.

One major problem to overcome is that companies generally prefer not to give out information about problems with their IT infrastructure, both out of embarrassment and fear of legal repercussions. On the other hand, allowing anonymous submissions may slant results. Until a way is found to address the concerns of submitters, all anonymous submissions are marked as such and resulting graphs annotated accordingly. A key issue is providing an incentive for incident submission, which will be the focus of a future publication.

Incident classification includes cost of incident, type of industry impacted most, location, and other parameters. This results in a database of common cases as contributed by a broad range of users ranging from experienced software programmers to young entrepreneurs. The database includes cases of known crimes with previous modus operandi and thus serves as a repository of what is known about previous crimes of a similar nature. Statistical methods and stochastic analysis tools can be used to develop a prognosis model.

Solutions & Tools Database: The solutions & tools database lists information about known methods to solve e-commerce risks, such as software tools designed to counter specific flaws. The database uses a characterization scheme similar to that of risk incidents, to allow searching and matching up risks with tools (and vice versa).

New tools can be submitted via links to the tool's location (the EcomRISK.org site does not store the actual tool itself but only information and feedback about it).

Survey: The survey is one of the interactive mechanisms for eliciting user participation. While a survey relies on the user to provide information, the extracted information is invaluable: on user EC trends, user knowledge, EC-cyber-terrorism and user demographics. The survey information is combined with the incident submission to derive statistics on user backgrounds: what they already know, what they would like to know, what they would like to do (and what risks would they face), how much protection they are willing to deal with (e.g., "How complicated is your password? Would you rather type in a whole sentence if it makes it easier for you to remember?"). Similarly, experts can outline their areas and potential contributions.

Searching for Incidents & Solutions: Currently, users can search for incidents by choosing classification terms from the submission form, or specifying terms to search in free text answers.

Solutions can be browsed by type, area of employment, or keywords.

Searching for Related Information: Users have the option of searching the site globally or specific elements such as the technical reports. Searches can look for keywords in all or part of each resource.

4. Incident Collection and Classification

We have developed a suite of tools to classify incidents for the risk incident database and enable data mining. The tools are described below and they are: the incident submission interface, the synthetic incident generator, the visualization tool, the query tool, etc. These tools are designed to attract incident submission by providing interactivity and feedback.

Incident submission interface: To make submissions of new content to the site as simple as possible, EcomRISK.org distinguishes between general users and experts and offers two versions of most submission forms, each geared towards the different technical background of the submitter.

The submission form starts with questions about the user and his or her relation to the incident. While we prefer submissions of personal experiences with e-commerce risks, third hand information is useful both to obtain a wider incident range and to view incidents from different angles.

The next section deals with the introduction of the incident into the respective system. Markers such as type of incident (e.g. "denial of service") and the location of the introduction (e.g. telnet daemon) provide a simple classification; a long-text summary allows the user to point out specifics of the incident.

Next, the submitter can provide information about the solution that was employed to fix the problem (if it was fixed). This can be a pointer to the resource used (e.g. a software patch) or a description of changes in the system's use (e.g. changes in policy).

The user then has the opportunity to quantify the incident in terms of required man-hours to solve the problem, and lost revenue. These values may not be exact (especially in the case of third hand information) but provide a general idea of the severity of the problem.

Finally, the submission form asks for information about the system's owner (usually a company) such as the general area of commerce and size (in terms of annual revenue).

After the user successfully submits the incident, feedback is given to the user to provide some additional information for the submitted incident. For example, the classification information about the submitted incident is shown. If the user did not fix the incident yet, information about how to fix it will be provided.

Synthetic incident generator: Since we have not enough real incidents data in the database so far, to help the research work based on the incidents, we design and implement a synthetic incident generator, which can generate thousands of synthetic incidents according to some specific pattern in several minutes. These synthetic incidents provide a testbed for our following research.

Visualization tool: The visualization tool is used to visualize the incidents distributions in the database. It provides a concise interface to show the status of the current risk incident database.

Query Processing: To help users use our risk incident database, we provide a flexible query interface. Users can query the risk incident database using any fields or field combinations. Since there will be always multiple incidents returned as the query result, users can assign different weights to different search fields to focus on the incidents they need. Users can also input keywords, which is used to search the summary of the incident, to help search the incident. By providing such a flexible query interface, we help users find the incidents they are interested more quickly and accurately.

Each time users employ the query functionality, the query is recorded and analysed. By analysing the query usage records, we find the pattern of how users use the query. Based on this pattern and the global search records, we can know what users want to know in a specific period. Thus we can adjust the content of our website to provide a better service for users.

5. Conclusion & Future Work

The future success of e-commerce depends on providing adequate security measures that minimize or eliminate risks such as fraud, denial of service attacks, or digital forgeries; and giving users the understanding and the means of gauging the risks involved in any particular transaction. [8, 12] The EcomRISK.org resource aims to familiarize current and future e-commerce participants with the technology and language of the trade so that they become comfortable in using the Internet with a similar ease as traditional marketplaces. At the same time, EcomRISK.org is designed as a collection point for the general participants' concerns and issues, so that experts can learn what new technologies are needed, how well existing technologies are accepted or what might need to be done to further their acceptance. Finally, by connecting users with experts and monitoring the traffic and exchange of information between them, we hope to learn of trends as they develop, create new research areas, and improve the resource continually.

One feature of the EcomRISK.org website currently under development is to provide a customized user page that allows the user to pool specifically those parts of the website that are of the most interest, such as a filtered newsfeed or direct links into selected discussion threads.

An important improvement for EcomRISK.org is to make better use of plain text that users input. For the users who cannot fill all the fields in the incident submission form accurately, they can just input incidents description in the form of plain text, from which we can extract the information for the missing fields. An incident collector is also under development to collect the incidents information from the Internet for our risk incident database.

One main problem with EcomRISK.org as a resource is that its usefulness depends on the level of use. By cooperating with other national resources such as the Institute for Security Technology Studies (ISTS), we hope that the initial exposure will help the website to become known among Internet users.

6. Acknowledgements

The authors would like to acknowledge previous work by Aidan Marcuss and Sanket Agrawal, as well as feedback from Gerry Davis from ISTS.

This work has been supported by the Department of Justice contract 2000-DT-CX-K001.

References

1. Landwehr C.E., Bull A.R., McDermott J.P., Choi W.S. "A Taxonomy of Computer Program Security Flaws." ACM Computing Survey 1994; 26:3, 211-254
2. Collins J.C., Lazier W.C. "Beyond Entrepreneurship: Turning your Business into an Enduring Great Company." Prentice Hall, Eaglewood Cliffs, 1992, pp 95-134
3. Makedon F. "E-Commerce Security Resource: ECOMRISK Data Center." Grant Report, 2000
4. Linqvist U., Kaijser P., Jonsson E. "The Remedy Dimension of Vulnerability Analysis." Proceedings of the 21st National Information Systems Security Conference, 1998, pp 91-98
5. Bishop M., Bailey B. "A Critical Analysis of Vulnerability Taxonomies." TR CSE-96-11, Dept. of Computer Science, University of California at Davis, 1996
6. Sahay A., Gould J., Barwise P. "New Interactive Media: Experts' Perceptions of Opportunities and Threats for Existing Businesses." European Journal of Marketing, 1998, Vol. 32, No. 7/8, pp. 616-628
7. Marcuss A. "EcomRISK.org The Source for E-Commerce Risk News & Assessment." TR2001-403,

Dept. of Computer Science, Dartmouth College, 2001

8. U.S. Department of Commerce. "The Emerging Digital Economy: Introduction." 1998 http://www.ecommerce.gov/emerging.htm
9. Hoffman D.L., Novak T.P., Chatterjee P. "Commercial Scenarios for the Web: Opportunities and Challenges." Journal of Computer Mediated Communications, 1995, December, Vol. 1, No. 3
10. Institute for Security Technologies Studies at Dartmouth College, http://www.ists.dartmouth.edu
11. Vatis M.A., "Cyberterrorism: The State of U.S. Preparedness." Statement before the House Committee on Governmental Reform, Wednesday, September 26, 2001.
12. Ashcroft, J., "Remarks of Attorney General John Ashcroft," First Annual Computer Privacy, Policy & Security Institute, May 22, 2001. http://www.usdoj.gov/criminal/cybercrime/AGCPPSI.htm