Web-based Risk Analysis Tool for Home users

M.Jain and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Broadband internet services are widely available in the market with high data transfer rate and attractive low prices. This feature is not only attracting organizations but a large proprtion of residential users have moved towards it. The 'always on' broadband technology comes with potential security threats and unauthorised access to information, resources and systems. The organizations hire security experts or administrators to deal with potential risks but home users have little knowledge to handle such risky situations. Various risk analysis tools, standards and techniques are available to overcome the risk problems but it has been found that these are oriented towards organizations and require expertise. Many websites are available with security risk handling guidelines for home users but they also require certain knowledge and understanding of technical terms. This research has been conducted to develop a web-based risk analysis tool specially for home users. The tool has followed controls and guidleines from ISO17799 information security standard to produce risk scores from individual user responses. The tool has covered features like using simple and accurate risk assessment method along with mitigation guidelines, userfrienliness and easy accessibility. The tool also educates users about security and threat related terminology and offers necessary protection to their systems.

Keywords

Broadband, security threats, risk assessment, home users.

1 Introduction

Majority of the people are changing from narrowband internet connection to high speed broadband connection. This broadband revolution is not only recorded in organizations but there is a large move from dialup to broadband among residential users (Ofcom, 2009). Due to immergence of internet as a part of day to day life, people and businesses cannot imagine life without it (getsafeonline, 2008). Generally people spent their time on the internet shopping, banking, social networking, dating and many otheractivities. The increasing use of broadband internet comes with a down side. As a result a large production and distribution of malicious threats have been detected in 2008 (Symantec, 2008). Online crimes such as malware, spyware, phishing, ID thefts, hacking of data and systems are extremely profitable.

This increase in internet connectivity and online applications are making home users more vulnerable (Furnell et al. 2007) and this has been observerd from the succcess of many online scams and resulting level of threat attacks on home users (Symantec, 2006). The basic requirement in order to protect home based computing is the development of web-based risk analysis tool specially for home computer users. The

tool should provide a simple and accurate risk assessment method with suitable risk mitigation guidelines applicable for individual users.

2 Current attitude towards IT security

More and more of the UK's small and large level organizations are focussing on IT systems and information secuirty. Businesses are changing their secuirty behaviour and taking regular security controls such as data backup, malware protection and encrypt network traffic to avoid any security breaches (BERR, 2008). The CSI computer crime and security survey, 2008 also recorded the average annual loss under $300,000 which shows a break down from the previous year record. The organizations are following security policies, tools and standards to promote security against illegal network access.

Survey results show that many governments and businesses are improving cybersecurity but individual computer users still lack in basic precautions against daily life cyberattacks (Gross, 2008). The home users lack the awareness, time, appropriate resources, security and risk handling skills and lack of standard risk analysis methodology (Furnell et al. 2007). Either they do not know what steps to perfom against malicious codes or they have insufficient information, tools and guidelines to follow. So this research aims to fulfil all security requirements of the home users by developing a web-based risk analysis tool.

3 Risk analysis tools and websites Evaluation

One of the important parts of the research is to analyse different risk assessment methods and their methodology whose output may guide risk analysis tool to follow suitable risk assessment methods applicable to home user environment. The famous risk assessment methods have been included in this analysis. When these methods were reviewed it was found that these are exclusively focused on the information security needs of the organizations and are used for some specific purposes. Some of them are either available at a cost or some are complex to use.

A new project CORAS, provides model-based risk asessement process which do not describe and evaluate risk assessment targets and results (Aagedal et al. 2002). The technical aspects of CORAS are human interaction and is related to organizations and society. From a case study it has been found that some components used during the process were useful and worked well but was time-consuming and required technical backing to perform the application.

The COBIT project addresses good IT security management practices for organizations. This is a very popular framework which provides necessary secuirty policy and good practice of IT controls. The implementation of the tool set consists of all important information such as IT control diagonistic, implementation guide, case studies and FAQs. The down side of this method is that it only suggests 'what' things must be done but does not explain 'how' which is necessary to know in certain things.

The CRAMM risk analysis methodology has been developed to provide a structured computer security management approach for large, small and home offices (Spinaellis et al. 1999). The method was successful and declared as mandatory for the UK governrnent organizations. The problems associated with CRAMM are that it is specifically designed for organizations, it is time-consuming and requires specific knowledge to implement and maintain. A product of ISO17799, COBRA specifically launched for business level security and uses very lengthy questionnaire with high level technical terms (COBRA, 2008). Same as the risk assessment and planning technique, OCTAVE fulfils the organizations' security needs and requires an analysis team to handle its 'plan-implment-monitor-control' methodology (Alberts et al. 2003).

Number of websites are available on the web to help home user computing problems and guide them appropriately. CERT-Home computer security developes and promotes appropriate techniques for different level of computer users to limit cyber attacks, damages and system failures. The home computer security part of the webiste provides certain security controls for the user to follow. Microsoft-Secuirty at home focuses on 3 main points which are protect your computer, protect yourself and protect your family by giving knowledge on security and fraud related terms.

Getsafeonline.org conducts a quiz to test the internet safety bahaviour of the user. It has multiple choice questions and results are displayed using a correct/incorrect option as and when the user answers. It does not concentrate on the individual user's computer security. Whereas Tom-cat provides basic and additional protection guidelines for family and friends computers, information on internet privacy and security programs. Staysafeonline.org asks a questionnaire to the users about the security controls they have on their system but as a result it simply counts the number of users answered particular option. It gives a comparison of different users behaviour towards computer security.

All the above discussed websites are associated with problems. Few of them are complicated, non-userfriendly and require technical knowledge to understand and access their vast data. And most importantly none of them discusses about individual user system's risk level. A risk analysis approach with nature of guaranteed accurate results is required to secure home computing.

4 Risk assessment methodology

The core part of risk analysis tool is risk assessment quiz which follows guidelines and controls associated with ISO17799 international standard. All controls do not map directly to the identification of questions, and considers only the ones which are suitable to home computing environment. The quantitative approach to analyse the risk has been used in the research, in which values are assigned to individual risk types and risk determination formula is used calculate risk as:

Risk level = Impact * Likelihood (Mazareanu, 2007)

Likelihood means probability of risk occurrance in the system and 3 cases of likelihood have been considered for risk analysis tool, as 1.0 for High, 0.5 for

Medium and 0.1 for Low level. The impact is harm or loss which occurs after any successful vulnerability incident, here quantitative impact has been used with 3 values as 100 for High, 50 for Medium and 10 for Low impact. For measurement of risk score, a simple risk model 'Jacobson's Window' has assigned quantitative values of impact and likelihood and it has used to get the accurate risk calculation (Stoneburner et al. 2002).The definition of risk score is also divided into 3 levels, 100 for High, 50 for medium and 10 for Low level risk. The risk assessment quiz has 10 categories, 2 questions in each category and each question with YES/No options. Each question has to be answered and as the user completes the quiz, the result will be shown with according to the category.

Category 1

Question 1 Do you have any anti-virus software insatlled on your computer?

Question 2 Do you regularly update the anti-virus software?

In this category, if a virus, worm or Trojan attack occurs then potential impact can be high (100) and probability of an attack can be high (1.0), medium (0.5) or low (0.1) depends on the user's answer. Here risk calculation will be applied as:

Case1: If answers to both Question1 and 2 are NO, then probability is high (1.0).

Risk level = impact (100) * likelihood (1.0) = 100 (high level)

Case2: If answers to Question1 is YES and Question2 is NO, then probability is medium (0.5).

Risk level = impact (100) * likelihood (0.5) = 50 (medium level)

Case3: If answers to both questions are YES, then probability is low (0.1)

Risk level = impact (100) * likelihood (0.1) = 100 (low level)

Depending on the level of risks, 'Best Practice' part will provide category wise suitable guidelines to follow in order to minimise the level of risk score.

5 Web-based Risk Analysis Tool

The risk analysis tool has used the platform ASP.Net with Visual basic and MS Access as database to include data tables. The application design has focused on user friendliness, consistency and user accessibility. The 'Secure Online Surfing' risk analysis tool consists of five parts which are discussed belo.

Home page: This main page consists of a brief introduction to the tool, so that the user will et an idea about the tool upfront. All five parts are accessible from the top of the home page and is as shown in Figure 1.

Figure 1: Home Page - Web-based Risk Analysis Tool

As discussed earlier, very few home users are familiar with computer security related terminology. To achieve the objective of educating the user on the various terminologies associated with internet security the tool has introduced two sections: 'Beginner's guide' and 'Resources'.

Beginner's guide: This section provides knowledge on malicious threats, freeware and shareware programs, firewall and its different types. This also includes password selection and protection guidelines, information on digital signatures and Microsoft's automatic updates.

Resources: This section of the tool enhances the knowledge of the user by providing additional information on computer security, information security, risk assessment websites and latest news and updates in related field.

Risk Assessment Quiz: This part is a questionnaire of 10 different categories with 2 questions in each category. First of all the quiz section will ask for user identification at login page to be stored in database to show the reference on the result page. This page consists of a brief introduction about number of categories, questions and final result page format.

If the user logins successfully, then only he is allowed to see the question web pages. The question page will look like Figure 2, each question with YES/NO options and user's answers will be stored in database table to calculte risk scores using risk determination function. The web pages consist of validation checks on answering each question and on navigating from one section to another.

Figure 2: Question page - Risk Assessment Quiz

Many users may be sure of the answer to the questions and if they are not, they are provided with a help link such as 'Anti-virus Information-Click here' shown in Figure 3, to help them answer correctly. The tool is suitable for the Windows operating system; similarly help links are provided for windows system. When the user clicks on the link, it will open a web page as shown in Figure 3. The page has some steps with the system's window pictures which the user has to simply follow on his computer system and then he will be able to answer appropriately. The help links are given on selected categories which are most likely to confuse the user. In this way the tool is best suitable from novice users to advanced computer users.

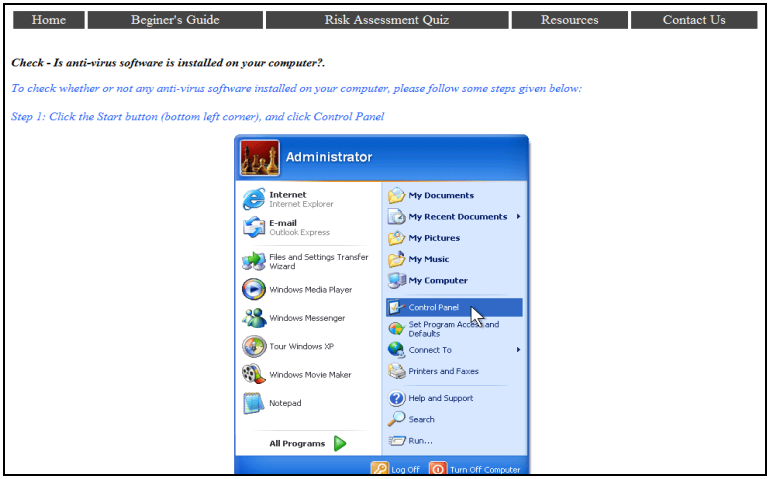

Figure 3: Helping Link Webpage – Category1

The user will be directed to the 'Result page' once he has answered all the questions. This page is divided into two types of views, one a table with user identification and category wise risk scores. The second with the five most important categories are shown in traffic signal system. The result page will look like Figure 4, with risk scores as high level risk (100) – 'Red colour box', medium level risk (50) – 'Orange colour box' and low level risk (10) – 'Green colour box'.

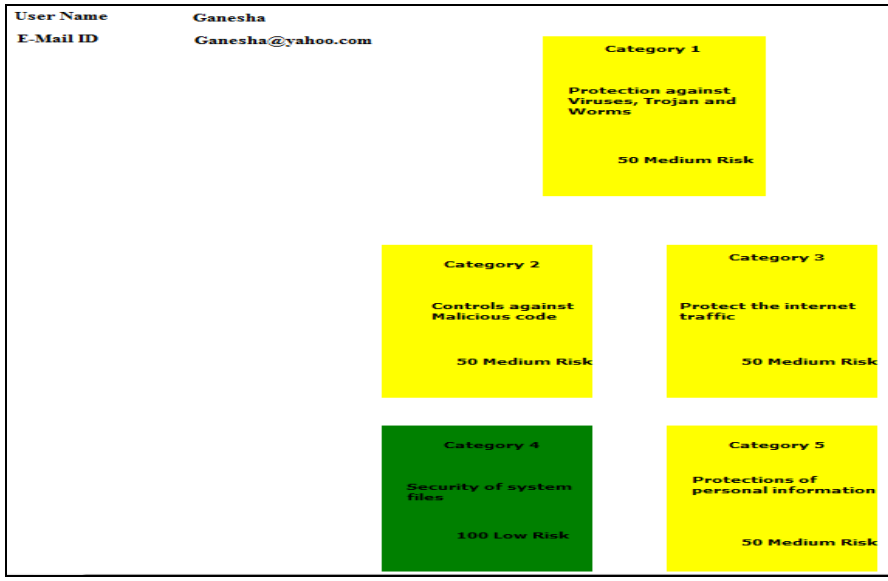

Figure 4: Result page - Traffic Signal System

6 Conclusion

The research revealed that majority of individual users and organizations are adopting broadband services due to its falling prices and unlimited connectivity. The high speed and 'always on' broadband connection comes with various security threats. The discussed survey has resulted that organizations taking care of their information security but the lack of awareness and technical skills of the home users to deal with security threats make them easy targets for hackers. The evaluation of risk analysis tools, methods and websites showed that they are suitable for businesses and organizations, require expertise and available at a cost. The guidelines are sometimes overwhelming and not structured well.

The development of web-based risk analysis tool was proposed to overcome computer security problems of the home users. A risk assessment questionnaire has been constructed by considering ISO17799 controls and guidelines best suited for home computing environment. The questionnaire used a simple and accurate risk assessment method to highlight critical risk areas in the user's system and provides suitable risk mitigation steps based on individual user's responses. The tool is considered to be user-friendly, easy to use and accessible by 20 user's reviews and on comparison with 'getsafeonline.org'. The 'Secure Online Surfing' risk analysis

tool can be launched globally to provide an accurate and trustworthy solution against internet security risks aimed at home users.

7 References

Aagedal, J., Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D. and Stolen, K. (2002), "Model-based Risk Assessment to Improve Enterprise Security", 6th International Enterprise Distributed Object Computing conference. IEEE proceeding.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), "Introduction to OCTAVE Approach", www.cert.org/octave/approach_intro.pdf, (Accessed 24 July 2008)

BERR (2008), "BERR 2008 Information Security Breaches Survey", www.berr.gov.uk/files/file45714.pdf, (Accessed 2 February 2009)

COBRA (2008), "COBRA Knowledge", http://www.riskworld.net/kbases.htm, (Accessed 10 February 2009)

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), "Assessing the Security perceptions of personal Internet users", Computer & Security, Vol. 26, No. 2006, pp 410-417.

Get safe online (2008), "Get Safe Online Report", http://www.getsafeonline.org/media/GSO_Report_2008.pdf, (Accessed 15 July 2009)

Gross, G. (2008), "Survey: many computer users lack basic security precautions", IDG new services, http://www.pcworld.com/businesscenter/article/151793/survey_many_computer_users_lack_basic_security_precautions.html (Accessed 25 August 2009)

Mazareanu, V.P. (2007), "Risk Management And Analysis: Risk Assessment (Qualitative and Quantitative)", http://www.anale.feaa.uaic.ro/.../06_Mazareanu_V__Risk_management_and_analysis-risk_assessment.pdf, (Accessed 22 August 2009)

Ofcom (2009), "The Communication Market 2009 – 4 Telecoms", http://www.ofcom.org.uk/research/cm/cmr09/cmr09.pdf, (Accessed 12 July 2009)

Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999), "Security requirements, risks and recommendations for small enterprise and home-office environments", Information Management and Computer Security, MCB university press, pp 121-128.

Symantec (2008), "Symantec Global Internet Security Threat Report", http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, (Accessed 12 June 2009)