Web-Based Risk Analysis for Home Users

R.T. Magaya and N.L. Clarke

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

Abstract

The advancement of the Internet has seen more home users becoming connected to superfast broadband. It has also provided access to a wide variety of online services such as banking, e-commerce, social networking and entertainment. The wide availability and popularity of the Internet has also led to the rise in risks and threats to users, as criminals have taken an increasingly active role in abusing innocent users, giving rise to attacks such as unauthorised access, malware attacks, denial of service attacks and identity theft.

Current risk analysis tools, techniques and methods available do not fully cater for home users but are tailored for large organisations. The tools require expertise to use them, expensive to purchase or simply provide general awareness information. As such a tool is required that can bridge the gap between bespoke risk assessment approaches that provide bespoke information and broad-spectrum approaches that simply provide all information regardless of its relevance.

The paper proposes a web-based risk analysis tool for home users that is based on well-accepted standards (such as the ISO 27002, NIST SP800 and SANS 20 Critical Security Controls guidelines). The tool assists the user in performing risk analysis in an extremely user-friendly fashion and not requiring any prior knowledge and provides tailored information indicating any controls missing, with guidance also on how to implement the recommended tools. In addition the tool will also educate the user by providing information about safe user behaviour. A prototype was developed and evaluated by a sample of home users. 93% of the participants found the tool to be easy to use helpful and very informative.

Keywords

Risk Analysis, Risk Assessment, ISO 27002:2005, NIST SP 800-30, SANS 20 Critical Security Controls, Home User, Information Security Awareness.

1 Introduction

According to the latest Ofcom report 80% (eight in ten) UK households now have access to broadband internet (Ofcom, 2012). As home users are now always connected to fast broadband internet, they have come to depend on the internet for their daily activities with at least 73 % adults in the UK spending approximately 8.3 hours per week the internet (Ofcom, 2011).

This increased dependence however exposes users to numerous risks and threats (Furnel *et al*., 2007). A computer connected to the internet without protection maybe infected with malicious software in under a minute (Postnote, 2006). Most threats

now operate without the user's knowledge, stealing personal details or using a user's computer for malicious purposes (GSO, 2010).

Several threats exist in different forms; these include but are not limited to malware, spyware, Trojans etc. These threats result in attacks such as denial of service attacks; fraud; identity, data and service theft, unauthorised access, destruction of data and systems. In UK, 1 in 5 users have been victims of phishing scams, while 40% have experienced virus attacks, and 19% have been victims of online identity theft (GSO, 2010).

There is a need for a risk analysis tool designed for home users which will provide guidance and support with the aim of identifying missing controls and assisting the user on how to implement recommended controls to reduce risks. The tool should do this in a simple, user-friendly and non-technical manner.

This paper will look at the development of a web-based risk analysis tool for home users. The next section will provide a background about risk and risk assessment. Current tools, standards and techniques available will be discussed. Section 3 describes the web-based risk analysis tool methodology. The design and appearance of the tool will be discussed section 4. Section 5 will discuss the evaluation of the tool by users. Conclusions and recommendations will be in section 6.

2 Background

2.1 Risk and Risk assessment

Risk is the likelihood of a given threat exploiting a particular vulnerability. It is a combination of threats and vulnerabilities that may have adverse impact if they occur (HIPAA, 2010). Risk can lead to a compromise in confidentiality, integrity and availability of systems and or data (Elky, 2006). Risk assessment identifies, quantifies and prioritises risks using a risk acceptance criterion. Risk assessment helps set priorities for managing risks and implementing controls to mitigate identified risks (ISO 27002). It helps focus security activities on important assets.

The tool developed in this research will use qualitative risk assessment methodology for assessing risks which involves determining the probability of an outcome using an interval scale which is represented by non-numerical labels such as High, Medium and Low. The risk rating will be based the SANS 20 Critical Security Controls, a well-recognised industry standard for control prioritisation. The tool will not use complex calculation to assess risk as the same can be achieved qualitatively with simplicity.

The web-based risk analysis tool will use a questionnaire to gather information about the assets the user has and the currently controls in place. The answers to the questionnaire will determine the user's level of risk and the tool will recommend any missing controls to reduce the risk; also providing assistance to the user in selecting and implementing the controls.

2.2 Awareness

A significant number of users are still unaware of their exposure to security risks (ENISA, 2009). Lack of awareness makes users vulnerable to online threats. Awareness involves educating the user with the aim of focusing the user's attention on security by changing user behaviour and pattern (ENISA, 2010; NIST SP 800-16). Awareness is a pre-requisite for adequate protection (Spears and Barki, 2010). The effectiveness of any security measures hugely depends on users' awareness of risks and countermeasures.

Websites like Get Safe Online, Microsoft Security Centre provide awareness and security guidance information to help users stay safe online. They are however not well structured making it difficult for the user to search for and find specific information. They assume a certain level of computer security knowledge and do not provide adequate information or assistance about selecting and implementing controls.

2.3 Current state risk assessment standards and techniques

There are several tools and standards available to help identify and manage risks. They however have a number of weaknesses. The available tools such as CRAMM, OCTAVE and COBIT require expertise and are tailored for large organisations. Standards such as the ISO 27002 and NIST SP 800 act as guidelines for reference; they do not provide information on how to implement controls. Most of the processes outlined in the standards are not applicable home users. They also require a certain level of expertise making them less suitable for home users.

As Home users lack expertise and awareness, there is need for a tool that performs risk analysis for the user and provides relevant recommendations that are tailored to their assets whilst also educating them. The tool will address the weaknesses of existing websites, tools and standards

3 WEBRA tool

The web-based risk analysis (WEBRA) tool framework used the ISO 27002, NIST SP 800 – 30 standards base guidelines to identify assets and formulate questions. This was to ensure all important security areas outlined by industry accepted standards are covered.

The tool will consist of a two-part questionnaire which is tailored for a home user environment. Help will be provided throughout the tool in the form of mouse overs, links and pop up description boxes to provide guidance to the user. There will also be a full glossary page with explanations of risk and security terms. The tool unlike existing tools will cater for all home users without requiring any prior knowledge of security. The tool will have three main processes:

- **Asset selection**: the user selects assets they have, data stored on the assets, services used and controls currently implemented.
- **Control ranking**: the system analyses the missing controls and determines risk level based on a control priority ranking system.
- **Output/Recommendations**: The tool will provide an overall risk rating for each asset and will recommend missing controls that are required to mitigate the risks. Additional guidance will be provided through a description of each control and links provided to direct the user where they can get the controls or guidance on how to implement them.
- **Behavioural practice**: the user answers a series of questions regarding their use of systems. The WEBRA tool will recommend safe practice behaviour to the user such as regular updates, scanning removable media, changing passwords etc. In addition the tool will educate the user providing explanations and links to other useful websites. The information on the recommendations page is presented in a simple and comprehensive manner.

The web-based risk analysis tool will be made up of a two part questionnaire divided into section 1 (assets and controls) and section 2 (user behaviour).

3.1 Assets and countermeasures

This section forms the core part of the risk analysis tool. The questions will enable the tool to assess the user's risk level and recommend appropriate controls. Section 1 questions will help identify the user's exposure to risks based on the missing controls.

The tool begins by building an asset profile for the user by identifying the assets they have. The tool will also ask the user to provide key information about the assets such data stored on the assets, internet services used. The user will also be asked to indicate the current security controls they have in place. The system ranks all controls according to priority based on the SANS 20 Critical Security Control List (SANS, 2011); any controls missing will be highlighted as recommendations and links to relevant websites provided.

All questions in section 1 are in tabular form. This was done to simplify the user input process and for a good interface that makes navigation easier and quicker for the user.

3.2 User behaviour

The second part of the web-based risk analysis questionnaire aims to inform and educate the user about staying secure. The questionnaire evaluates user behaviour and awareness. The questions are in multiple choice form and assess existing security practices in a number of areas outlined in both the ISO 27002 and NIST SP 800 – 30 standards.

The 18 questions cover user behaviour in the home environment; for example how regularly a user updates their security software, change passwords, perform backups

etc. Several other topics are covered including security policy, authentication, encryption and privacy. See Figure 1 below for sample questionnaire.

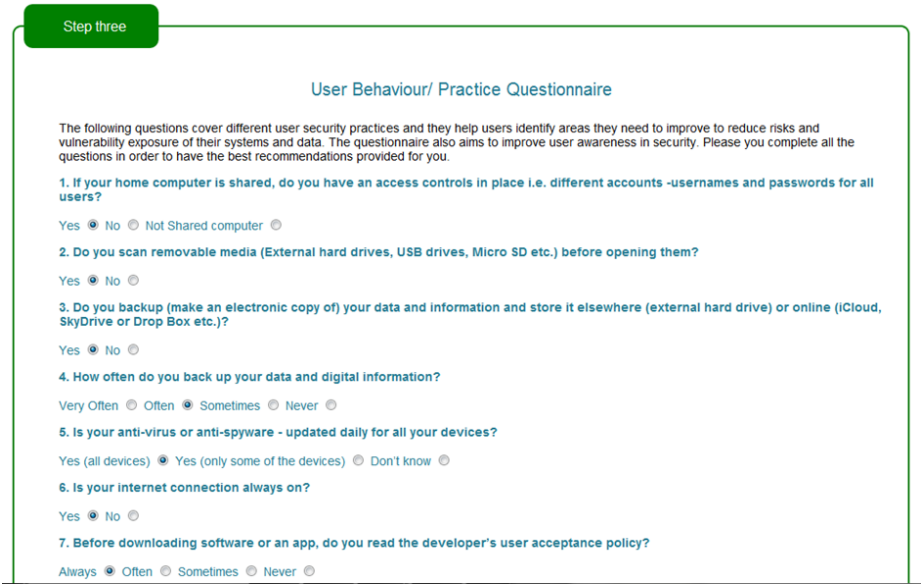

Figure 1: Behavioural Questionnaire.

Once the user has completed all the questions in this section the tool will give recommendations for best practices. Links are provided to websites that offer best practice guidelines which will address any insecure user behaviour.

3.3 Determining the risk level

The web-based risk analysis tool uses a modified control prioritisation list tailored for home users (shown in Figure 2). All controls listed apply to home users. The 20 Critical Security Controls takes into consideration the latest threats and vulnerabilities.

The process allows controls in place to be mapped to the assets and indicate areas where controls need to be implemented. The tool will rank each control in order to give a view of relative importance (IRM, 2002). The controls are ranked according to their importance in keeping assets secure.

The WEBRA will use a simple rating scale of High, Medium and Low to represent the degree of risk. The rating will be based on the prioritisation of controls in terms of their effectiveness and potential impact in reducing common threats and vulnerabilities. This will help user prioritise resources and efforts on critical areas in order to prevent attacks and intrusions. It will also help ensure that systems have the most critical baseline controls in place.

Critical Controls	WEBRA Controls	Priority
Inventory of Authorized and Unauthorized Devices	Identify the assets the user has done by the tool (Stage 1 WEBRA)	RA tool
Secure Configurations for Hardware and Software on Laptops, Workstations, and mobile devices	Secure configuration of security software and system settings.	High
Continuous Vulnerability Assessment and Remediation	Patches and updates	High
Malware Defences	Anti- Virus, Anti-Spyware	High
Controlled Use of Administrative Privileges	Passwords	High
Application Software Security	Encryption	Moderate
Data Recovery Capability	Backups	Moderate
Secure Configurations for Network Devices such as Firewalls, Routers incl. wireless, and Switches	Firewalls	Moderate
Boundary Defence	Physical security, case, pouch	Moderate
Controlled Access Based on the Need to Know	User Accounts for different users	Low
Account Monitoring and Control	Biometrics	Low
Data Loss Prevention Capability	GPS tracking	Low
Incident Response Capability	IDS	Low

Figure 2: Asset Priority List. (Adapted from SANS, 2011).

The reason for using this methodology was to eliminate the subjectivity inherent in qualitative analysis methods while ensuring the score reflects the importance of controls based on statistics (such as the SANS 20 Critical Security Controls) that reflect vulnerabilities and threats affecting users today. The result of the risk assessment questionnaire will lead to recommendations tailored to the user's assets. An overall risk rating for each, missing controls and their priority ranking will be displayed on the recommendations page.

3.4 Overall risk rating

The tool will give the overall risk rating as High (Red), Medium (Amber) and Low (Green). If one of the missing controls has a High priority ranking in the controls list then the overall risk is High. The same is true for Medium risk rating, if one of the controls missing has a Medium priority then the overall risk rating for the asset is Medium. If all missing controls are Low priority, then the overall risk rating will be Low. For example, if patches and updates (ranked High priority) are not installed the system can be easily compromised even if all other controls are in place. Patches and updates cover vulnerabilities and loopholes attackers can use to compromise the system.

4 WEBRA Design

The web-based risk analysis tool prototype was developed to demonstrate functionality, usability and the suitability of the tool to home users. The tool consists of a front-end website for the user interface, and a back-end database that stores all the input data, asset lists, countermeasures and priorities.

4.1 The interface

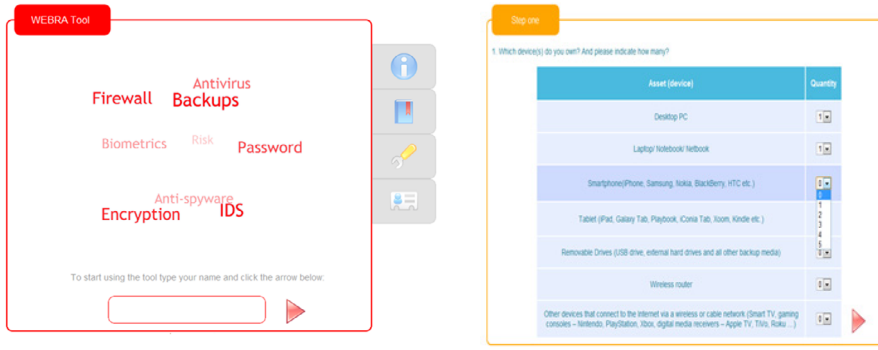

Figure 2 & 3: Main Page and Assets questions

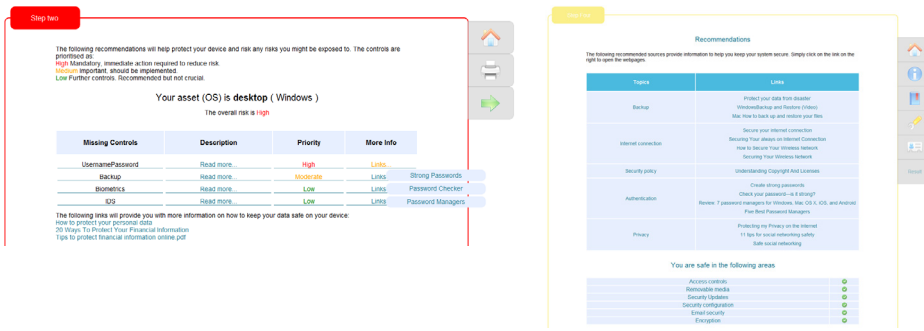

Figure 4 & 5: Recommendations for Assets and User behaviour

Usability helps users use the tool, completing the process quickly and easily. The interface determines whether the user can quickly learn to use the tool. Functionalities like navigation through menus, colours for different risk levels and priorities, mouse over and hovering makes the tool more usable and easy to follow. Figure 2 to 5 above illustrate the tool's interface.

5 Evaluation

The prototype was evaluated to test its suitability for home users and to see if it addressed the problems of existing tools. Two types of evaluations were undertaken.

The first one involved evaluation by sample of 50 home users. The aim was to gather users' perceptions, attitudes and opinions about the tool. The second evaluation involved a focus group of information security professionals. The group tested the WEBRA tool alongside a number of existing tools such as Secunia PSI, Get Safe Online, and Microsoft Baseline Security Analyser (MBSA). The usability of the tool, help provided, recommendations and links to other information were some of the criterion used to evaluate these tools.

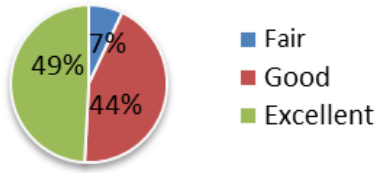

Figure 6: Usability of the tool (Ease of use)

Feedback from the users indicated that most (93%) users found the tool very easy to use and the interface was user friendly (as shown in figure 6 above).

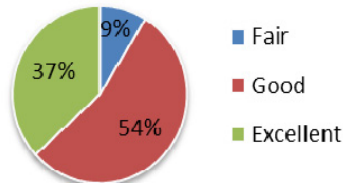

Figure 7: Provided implementation assistance

The majority of users (91%) felt the tool had provided adequate assistance and links to help them select and implement recommended controls. Users also found the recommendations to be helpful because they were tailored to their needs.

Overall the users liked the friendly user interface which made the tool easy to follow and use. Users found the questions easy to understand and the tool improved their security awareness. The tool risk analysis process took reasonable time to complete. Issues pointed out by the users included the need for more detailed explanation for terms like Intrusion detection systems and digital certificates which most users are not aware of.

Focus group feedback was the tool was comprehensive covering all aspects from risk assessment, control recommendation and implementation guidance to educating the user; unlike other tools which only covered a few areas like awareness and patches. The group also noted that WEBRA supported different devices and platforms; and had a simple and which provided a comprehensive report specific to the user's assets.

Overall the group concluded that the WEBRA tool was *"excellent and offered tailored recommendations to the user."* Tool was also easy to use for users with little experience, taking reasonable time to complete and very educational making it more suitable for home users than other tools. Areas the group felt could be improved include adding more controls and automatic detection of some controls like firewall.

6 Conclusion and Future work

This research looked at risk analysis and how it affects home users. This paper proposes a tool which is designed based on industry wide standards such as ISO 27002 and NIST SP 800. A web-based risk analysis tool was designed and developed to help users analyse and assess their security requirements; providing information in a simple manner to the user about how to solve identified security problems. In addition the tool also educated the user about risks and security.

The tool identifies missing controls and recommends them to the user together with educational information about safe practices. It also improves user behaviour by proving links to safe practices. The tool was evaluated by users who found it very easy to use, helpful and informative.

The prototype needs to be improved to include more controls and should be regularly updated to reflect latest threats, vulnerabilities and countermeasures. Detailed explanation of controls and auto detection of controls are other improvements to make the tool better.

7 References

Elky, S (2006). *An Introduction to Information System Risk Management*. SANS Institute. InfoSec Reading Room.

ENISA (2009). *Awareness Raising. European Network and Information Security Agency.* Available at: http://www.enisa.europa.eu/media/key-documents/fact-sheets/Awareness-1.pdf [Accessed: 25 August, 2012].

ENISA. (2010). *The new users' guide: How to raise information security awareness.* Available at: http://www.enisa.europa.eu/ [Accessed: 25 August, 2012].

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). *Assessing the security perceptions of personal Internet users.* Computers & Security, 26 (5). pp 410-417.

GSO. (2010). *UK Internet Security: State of the Nation. The Get Safe Online Report.* November. Available at: http://www.getsafeonline.org/media/Get_Safe_Online_Report_2010.pdf [Accessed: 26 25 August, 2012].

HIPAA. (2007). *Basics of Risk Analysis and Risk Management.* HIPAA Security Series. Volume 2: 6/2005: rev. 3/2007

IRM (2002). *A Risk Management Standard.* The Institute of Risk Management (irm). Available at: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf [Accessed: 18 August, 2012].

IS0 27002. (2005). *Information technology. Code of practice for information security management.* British Standards Institution. BS ISO/IEC 27002:2005. ISBN 0 580 46262 5.

NIST SP 800 – 30. *National Institute of Standards and Technology (NIST) Special Publication 800-30. Risk Management Guide for Information Technology Systems.* Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [Accessed: 03 January, 2012].

NIST SP 800-16. *Information technology security training requirements: A role- and performance-based model.* Available at: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf [Accessed: 25 August, 2012].

Ofcom. (2011). *Communications Market Report: UK*. Available at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf [Accessed: 03 December, 2011].

Ofcom. (2012). *Communications Market Report: UK*. Available at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf [Accessed: 25 August, 2012].

Postnote. (2006). *Computer Crime.* The Parliamentary Office of Science and Technology Available at: http://www.parliament.uk/documents/post/postpn271.pdf [Accessed: 12 July, 2012]

SANS (2011). *20 Critical Security Controls - Version 3.1*. Available at: http://www.sans.org/critical-security-controls/guidelines.php [Accessed: 25 July, 2012].

Spears, J. L. and Barki, H. (2010). *User Participation and Information Systems Security Risk Management.* MIS Quarterly. Vol. 34 No. 3, pp. 503-522/ September.