Design guidelines for IT security management tools

Pooya Jaferian, David Botta, Kirstie Hawkey, Konstantin Beznosov

University of British Columbia, Vancouver, Canada
{pooya, botta, hawkey, beznosov}@ece.ubc.ca

ABSTRACT

One of the most important factors that impact usability of security systems within an organization are security tools. In this paper, we report preliminary results of our survey about design guidelines for IT security management tools. We gathered guidelines and recommendations related to IT security management tool from available literature as well as result of our previous studies on IT security management. We categorized and combined these guidelines into a set of high level guidelines that can be used by tool developers in development of tools. In addition we identified the relationship between guidelines and challenges in IT security management as well as the strength of evidence for each guidelines.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*Interaction Styles*; H.5.3 [**Information Interfaces and Presentation**]: Group and Organization Interfaces—*Collaborative Computing*

General Terms

Human Factors, Security Management, Design

Keywords

IT security management, Design guidelines

1. INTRODUCTION

Today IT security is an important issue for organizations that want to protect their valuable assets from threats inside or outside the organization. Previous studies show that beside technological factors, human and organizational factors impact IT Security Management (ITSM) [17, 5, 12]. In [19], the authors classified the challenges that Security Practitioners (SPs) face in their organization into three categories: Technological, Human, and Organizational. Based on their findings, the technological challenges are: mobile access, vulnerabilities, technical complexity, human challenges are: lack of security training, lack of security culture, different perceptions of risk, communication of security issues, and organizational challenges are: distribution of ITSM, open environment and academic freedom, interaction with other organizations, control access, estimation of risks, security low priority, lack of budget, and tight schedules.

In order to improve the effectiveness of IT security in an organization one should address these challenges. One way to address the challenges is to develop effective technological solutions and tools to aid security practitioners (SPs). One important aspect of tools for IT security that determines their effectiveness is their usability [7]. In this paper, we present a set of guidelines based on the available literature and results of HOT Admin project [5] that can be used by tool developers to build usable IT security management tools. In addition, we propose a framework for classification of the guidelines. This framework can be used by tool developers to select appropriate guidelines when developing tools. For each guideline we identify the challenges that it can alleviate, and also show the strength of evidence. We argue that as a result of importance of IT security in organizations and also evolving and competitive market of IT security tools [4] developing a set of guidelines specific to IT security tools is necessary.

The rest of this paper is organized as follows: In section 2, we present methodology we used to obtain and classify guidelines. In section 3, we present our proposed framework for classification of guidelines for IT security management tools. The guidelines are presented in section 4. In section 5 we show limitations of our work and our plan for future research. The paper is concluded with section 6.

2. METHODOLOGY

Our main research questions in this work are: (1) What are the guidelines for development of tools for ITSM that help users do their job more effectively? (2) Which guidelines address which ITSM challenges (3) What is the strength of evidence for each guideline? (4) How we can classify these guidelines so they could be more useful to tool developers?

To answer the following questions, we first surveyed available literature related to tools for ITSM and network administration, and look for guidelines, or features that could be useful in ITSM and network administration tools. As a result of this survey, we found 19 useful sources and extracted

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
SOUPS Workshop on Usable IT Security Management (USM) 2008, July 23, 2008, Pittsburgh, PA USA.

164 guidelines and features from them. Consequently, we started coding and classifying guidelines. After two rounds of coding, we used card sorting exercise to combine similar guidelines, and also to have a categorization that facilitate using guidelines by tool developers. As a result of this exercise, we developed the framework presented in the next section as well as 21 general guidelines that can be classified in this framework. Consequently, we identified the relationship between the guidelines and our existing classification of ITSM challenges [19].

3. FRAMEWORK FOR CLASSIFICATION OF GUIDELINES

In this section we provide a framework for classification of design guidelines for ITSM tools. This framework is presented in Figure. 1. The framework classifies guidelines in different layers. The lower layers in the framework contain the guidelines that are applicable to different sets of tools, and the upper layers show guidelines that are more specific to a certain set of tools. For example, the lowest layer in the framework is general usability guidelines of ITSM tools. This general usability guidelines are applicable to all ITSM tools as well as other tools. The next layer is guidelines to help ITSM addresses technological and organizational complexity. The guidelines in this layer are the guidelines that their main goal is to address complexity in ITSM. As most of the ITSM tools should work in a complex technological and organizational environment, these guidelines are applicable to most of the ITSM tools (But not security tools for end-users as an example). The next layer in our framework contains two sets of guidelines that depend on the type of task security practitioners perform. We divided tasks that SPs perform into "security analysis" and "configuration and maintenance". The next layer contains guidelines to provide communication with different stakeholder. This set of guidelines addresses the need for communication of security issues with different stakeholders in the organization and is applicable for the tools that require this communication. The last layer in our framework contains guidelines that is recommended for tools that should work in an environment with distributed ITSM model [13]. These guidelines will help communication and collaboration of security practitioners in this environment.

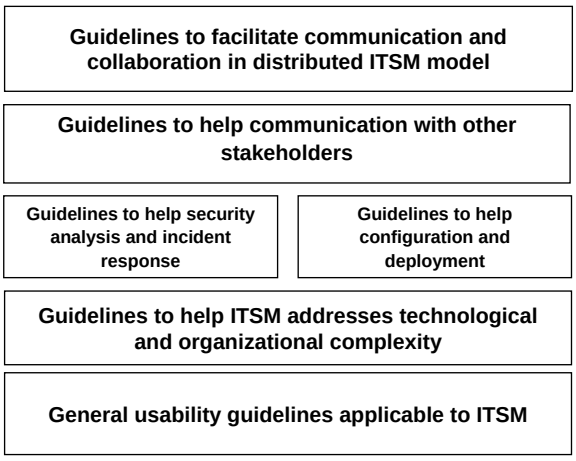

Figure 1: Framework for classification of design guidelines for ITSM tools

4. GUIDELINES

In this section we present the guidelines for IT security management tools. The guidelines are presented in the following format. First, the name of the guideline is presented followed by a discussion about the challenges in ITSM that the guideline can address. Whenever possible, we show more detailed examples or alternatives of the guideline. We also cite the references that the guideline is extracted from. To determine the strength of evidence of each guideline. the reader can use Table. 1. In this table we present methodology used in each paper.

Table 1: Used references and methodology

Ref	Methodology
[7]	Survey Literature for interface design principles for security tools
[6]	Designing a tool, user study the tool using 20 undergrads, and interview with network managers about the tool.
[8]	Implementation of technique without evaluation
[7]	User Study to became aware of the problem, But there is no study for the recommendations
[20]	Cognitive Walkthrough + User study of the problems with 12 participants, for a password manager.
[11]	Field study of system administrators + interviews, surveys, collection of different artifacts.
[18]	User study with 12 students for intrusion detection UI.
[16]	Interview and User study of low/med/high fidelity prototype with 2 to 3 managers.
[5]	Field Study + Interview of 14 security practitioners
[1]	22 Interviews, prototype design, and a user study
[21]	Survey literature, development of tool
[14]	Survey literature.
[2, 3]	Field study (200 Hours) + 12 Interviews + Diary studies + 101 Surveys of system administrators.
[9]	Survey of 160 administrators
[15]	Cognitive walkthrough of different security tools in VOIP systems.
[19, 12, 10]	Field Study + Interview of 27 security practitioners.

4.1 Guidelines to help ITSM addresses technological and organizational complexity

The main goal of this set of guidelines is to address technological and organizational complexity of ITSM. As security tools mostly work in a complex and evolving technological landscape as well as large organizations with a complex structure, these guidelines could address these problems.

4.1.1 Combinable tools

The goal of this guideline is to address *technical complexity* challenge. Because SPs deal with situations and scenarios that can't be predicted by tool designers, they frequently have to combine different tools to do their tasks. One way to facilitate combining different tools is to support interchange standards and also to read and write a great variety of file formats. Also, security practitioners prefer tools that can be combined with their existing tool set [5].

4.1.2 Knowledge sharing

This guideline addresses three challenges: *Vulnerabilities, technical complexity, and distribution.* If ITSM tools provide knowledge sharing, SPs can seek advice from other SPs when they face a new or unknown security incident, or receive help from a community in case of a complex task that they've never done before [7]. Also, this guideline could facilitate knowledge sharing between different security practitioners in an organization that uses a distributed ITSM model. [**?**, 8] suggest the use of social navigation. Social navigation can be in form of a large knowledge base that is maintained by the tool provider or an inter-organization knowledge base that is maintained by the organization itself.

4.1.3 Multiple presentation formats

To address the *technical complexity* in ITSM, tools should offer data to the SPs by means of different presentation or visualization techniques [18, 1, 21]. This can help SPs to have a better understanding about the state of the system. For example, an intrusion detection tool can show data in both visual and textual interface. This will help SPs to find malicious patterns by analyzing different presentations of the data.

4.1.4 Different levels of abstraction

To address the *technical complexity* of IT security, tools should provide facilities to work with information at different levels of abstraction. This can broke the complex system into different levels each of which contribute in understanding the system. These levels of abstraction could be in form of a general view to a detailed view [**?**, 6, 18, 3, 12, 10, 1] or separation of different concerns [11]. This approach can address the challenge of *distribution of IT security* as well, as each practitioner or stakeholder can interact with the system from his own level of abstraction, or he/she can focus on her own part of concern. Also, by providing information at different levels of abstraction, the *communication of security issues* from hard core security practitioners to other stakeholder in the system can be facilitated.

4.1.5 Customizability

This guideline addresses *technical complexity* and *vulnerabilities* challenges. Providing and customizing ITSM tools to the specific and evolving needs of SPs is a daunting activity. Due to complexity of the IT systems, SPs usually need to add their own functionalities or settings to the tools. Also, to handle situations where a SP need to deal with a new vulnerability, tools functionalities should be customizable. Therefore, tools should be tailorable and customizable to specific need of security practitioners [5, 15]. For example SPs should be able to add new test cases to a security analysis tool. This gives them an opportunity to analyze the system for new vulnerabilities that has not been available and predicted before.

4.1.6 Provide both CLI and GUI

This guideline addresses *technical complexity* and *distribution of ITSM* challenges. The result of previous studies shows that security practitioners prefer CLI over GUI [5]. Yet, there are certain cases where security practitioners use a tool infrequently. In these cases, it is hard for the security practitioner to learn all the commands and parameters to interact with a tool using CLI. In this case, providing a GUI is helpful. Also, providing information in both GUI and CLI helps practitioners to analyze the system from different views (raw data in CLI and visualization of data in GUI) that can help addressing the technical complexity challenge [21, 18].

4.1.7 Task prioritization

Because of the *tight schedules* in organizations, *low priority of security related tasks*, and *lack of budget and resources*, tools should provide facilities to help practitioners prioritize their security related tasks [19, 12]. For example, a security analysis tool can prioritize found vulnerabilities by their level of criticality.

4.2 Guidelines to help configuration and deployment

One of the main tasks of security practitioners is to perform configuration and deployment. To support this task, the following guidelines are recommended:

4.2.1 Rehearsal and planning

Configuration and deployment in IT security is a complex task. During configuration and deployment, SPs need to configure multiple interrelated entities in the network. The complexity of configuration and deployment task in ITSM frequently leads to failure during the process. To address this challenge which is rooted in *technical complexity*, SPs prefer to first rehears the task on a test system. If the result of the operation on the test system is satisfactory, the process can be performed on the production system. This guideline can be realized in different ways. Tools can support operation on a test system with different degree of fidelity to the production system. Also, along with tools, pre-defined test cases should be provided to test the output of the operation during rehearsal, or output of the rehearsal and actual execution of the operation [11, 3, 2].

4.2.2 Manageable configuration process

Security practitioners frequently need to apply configuration and deployment process on hundreds of nodes in a network. This process is considered to be a complex and long-running process. Therefore, to address the *technical complexity* and *tight schedules* challenges, tools should enable security practitioners to manage this process and have control on details of it. To realize this guideline in ITSM tools, they should provide forecasting of the operation length and amount of time remaining, pause and undo for the operations, logging of all parameters or settings that have been changed during the process, history and detailed steps of the executed operation, asynchronous operations, and single operation on multiple entities [11, 19].

4.2.3 Safe operation

Because *security is low priority* in many organizations, they can't tolerate their systems going off-line for security related configuration and maintenance. Therefore, tools should avoid requiring system to go off-line for these tasks. Also, as configuration and maintenance tasks usually make changes in system's settings, it is possible that it broke the existing security of the system. To address this challenge tools should avoid this as much as possible [11].

4.2.4 Easy to change configuration

Security practitioners frequently need to make changes in configuration of their tools. Due to *technical complexity* and *lack of security training*, in many cases changing configuration requires dealing with very many of parameters, to the extent that many of them are unknown to the security practitioner. Therefore, tools should provide facilities that help SPs change configuration of the system easily. To realize this, tools should provide commented configuration files and/or group related parameters together in high level profiles. When a SP wants to change the configuration of the system he or she can just change the profile, and all related parameters will be changed automatically [11].

4.2.5 Meaningful Errors

During configuration and deployment processes errors are inevitable. Due to *technical complexity* of ITSM and *lack of security training*, one shouldn't expect a security practitioner to be aware of the meaning of different errors. The situation is getting worse when the errors are stated with just a code or a cryptic message. To address this problem, tools should provide help in case of errors or alerts. In addition, tools should indicate which portion of the operation had been completed before error happened [11, 19].

4.3 Guidelines to help security analysis and incident response

Security analysis and diagnosis is an important task for security practitioners. To support the process of diagnosis, the following guidelines are recommended:

4.3.1 Customizable alerting

Security tools that monitor and generate alarms are frequently used by security practitioners. To address *vulnerabilities* challenge, these tools should reduce the number of false positive and negatives as many as possible. One way to realize this is to provide customizable thresholds for generating alarms. Also, due to *distribution of ITSM*, tools should be able to send alarms to multiple SPs. Therefore, the destination for sending the alarms and the communication channel through which alarms are sent should be selectable. Another challenge in using alerting tools is the number of alarms that are generated by these tools. Due to *tight schedules* challenge, SPs are unable to handle all the alarms all the time. Therefore, it will be helpful if they can suppress alarms that have lower priority or known by the SP as a false positive [11].

4.3.2 Automatic detection

To address *vulnerabilities* and *tight schedules* challenges, security tools shouldn't put the burden of finding attacks, malicious patterns, etc. on the SPs. This could be realized through using intelligent tools that use pattern recognition techniques or learn the normal behavior of the network to find abnormal patterns or behaviors [18].

4.3.3 Data correlation and filtering

Security practitioners frequently need to analyze different sources of data to find malicious behaviors. To facilitate this, tools should provide facilities to combine different sources of data into a single source of information and also provide required filtering and search features. To realize this, tools should provide correlating data from different sources by aggregating log files, combining security logs with application logs, and making a set of effective filters available [9, 19].

4.4 Guidelines to help communication with other stakeholders

Security practitioners need to communicate with other stakeholders during many of their tasks. To support this communication, we recommend the following guidelines:

4.4.1 Flexible Reporting

This guideline addresses several challenges. First, by generating reports in Web format, they can be easily distributed across the organization and be used by different security practitioners and stakeholders. This addresses *Distributed nature of ITSM* challenge. In addition, providing well-designed and easy to read reports will address *Technical complexity* challenge. Another aspect of flexible reporting is providing reports that is customized for a particular stakeholder. For example, a report about security analysis should give a manager high-level risks in the organization or the result of the investment in IT security. But another report from the same analysis that aims for a security practitioners should contain technical information about vulnerabilities. This kind of flexible reporting can address *Communication of security issues* and *Different perceptions of risks* challenges. Another facet of flexible reporting is to provide reports that are mandated by certain security standard. These reports usually show the degree of compliance with the standard and they can be demonstrated to other organizations as a proof of compliance. Therefore, providing this kind of reports can address *Interaction with other organizations* challenge [5, 15, 12].

4.4.2 UI for different stakeholders

The goal of this guideline is to address *communication of security issues* and *tight schedules* challenges. Since some security related tools are used by different people within the organization, the tool users should be able to individually customize the information that is provided by the tool. For example, a manager may not be interested in technical details, but rather an overview of the information that is relevant for business [5, 15, 19].

4.4.3 Archiving

Tools should provide facilities for keeping track of communication and critical information related to the tool. The goal of this guideline is to first keep record of the communication between different stakeholders. Frequently, multiple stakeholders are involved in critical IT security decisions in an organization. By keeping record of the communication, future tracking about who is responsible for the decision is possible. This addresses the challenges related to *control access* and *interaction with other organizations*, because it makes managers as well as security practitioners more aware

about the decisions they make. Also, keeping record of security critical information, enable future analysis on the information. This could be helpful to analyze trends in the network, estimate risks, and find unusual behaviors. This will address *estimation of risk* and *vulnerabilities* challenges [12, 10].

4.5 Guidelines to facilitate communication and collaboration in distributed ITSM model

In many organizations ITSM is distributed [5]. Practitioners of various expertise cooperate with each other to solve problems. The following guidelines are recommended to support such cooperation.

4.5.1 Work in a large workflow

This guideline addresses *distributed nature of ITSM, interaction with other organizations, and tight schedules.* In order to distribute a task to different security practitioners across the organization, tools should be able to work in a large workflow. To realize this, tools can provide support for workflow internally, or they can provide API or Plug-ins for integration with meta-tools [5, 11, 4].

4.5.2 Integration with a communication media

To address *distributed nature of ITSM* and *communication of security issues*, tools should provide a media for communication. This media can be in form of text, voice or video and it can provide computer-to-human, or human-to-human communication. Also, the communication channels can provide communication between two or more security practitioners or between security practitioners and other stakeholders [19, 12, 3, 2].

4.5.3 Sharing

To address *distributed nature of ITSM* and *communication of security issues* challenges, tools should provide sharing of state, information and assets across the organization. When two or more security practitioners work on a problem, they need to understand the state of the system they are working on. Therefore, tools should be able to share the current state of the system between the practitioners. In addition, tools should provide facilities to share reusable assets(like scripts, helps, etc.) with other security practitioners in the organization [3, 2].

5. LIMITATIONS AND FUTURE WORK

First, we show the relationship between guidelines and challenges to ITSM. While this relationship can help security practitioners to decide about the importance of each guideline, more studies should be done to identify importance of each guideline. One possible way to do this is to survey security practitioners to see what is the importance of each guideline from their point of view. Second, although we have indicated which software development guidelines are most beneficial to ITSM, each guideline warrants deeper study into how it is already practiced, and how it could be practiced.

6. CONCLUSIONS

In this paper, we provided the result of our preliminary survey on design guidelines for IT security management tools. The source of the guidelines are recommendations about ITSM tools available in the literature. In this work, we gathered different recommendations and combine them in high-level design guidelines for ITSM tools. We also proposed a framework for classification of these guidelines that can be used by tool developers while using guidelines in their tool development. In addition, we identified relation between the guidelines and the challenges in ITSM. This relationship can help tool developers to determine the importance of each guideline for their tools. We also identified the methodology used in each cited source for stating the guidelines. This information can be used to determine the strength of evidence for the guidelines. Despite our guidelines can be very useful in development of ITSM tools, they have a certain limitation that are stated in the limitations section. We allege that to make the guidelines more concrete further research is required.

7. REFERENCES

[1] R. Ball, G. A. Fink, and C. North. Home-centric visualization of network traffic for security administration. In *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 55–64, New York, NY, USA, 2004. ACM.

[2] R. Barrett, E. Haber, E. Kandogan, P. Maglio, M. Prabaker, and L. Takayama. Field Studies of Computer System Sdministrators: Analysis of System Management Tools and Practices. In *Proc. of the Conference on Computer Supported Collaborative Work*, pages 388–395, 2004.

[3] R. Barrett, P. P. Maglio, E. Kandogan, and J. Bailey. Usable autonomic computing systems: The system administratorsṕerspective. *Advanced Engineering Informatics*, 19(3):213–221, 2005.

[4] B. Beal. It security: the product vendor landscape. *Network Security,*, 2005(5):9–10, 5 2005.

[5] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding IT security professionals and their tools. In *SOUPS*, pages 100–111, Pittsburgh, Pennsylvania, July 18-20 2007.

[6] C. M. Burns, J. Kuo, and S. Ng. Ecological interface design: a new approach for visualizing network management. *Comput. Netw.*, 43(3):369–388, 2003.

[7] S. Chiasson, P. C. van Oorschot, and R. Biddle. Even experts deserve usable security: Design guidelines for security management systems. SOUPS USM Workshop, July 2007.

[8] P. DiGioia and P. Dourish. Social navigation as a model for usable security. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 101–108, New York, NY, USA, 2005. ACM.

[9] S. Furnell and S. Bolakis. Helping us to help ourselves assessing administratorsúse of security analysis tools. *Network Security*, 2:7–12, February 2004.

[10] A. Gagné, K. Muldner, and K. Beznosov. Identifying differences between security and other IT professionals: a qualitative analysis. In *proceedings of Human Aspects of Information Security and Assurance (HAISA)*, Plymouth, England, July 2008.

[11] E. M. Haber and J. Bailey. Design Guidelines for System Administration: Tools Developed through

Ethnographic Field Studies. In *Proc. of 2007 symposium on Computer human interaction for the management of information technology (CHIMIT), 9 pages*. ACM, 2007.

[12] K. Hawkey, D. Botta, R. Werlinger, K. Muldner, A. Gagne, and K. Beznosov. Human, organizational, and technological factors of it security. In *CHI'08 extended abstract on Human factors in computing systems*, pages 3639–3644, 2008.

[13] K. Hawkey, K. Muldner, and K. Beznosov. Searching for the Right Fit: Balancing IT Security Model Trade-offs. *Special Issue on Useful Computer Security, IEEE Internet Computing*, 12(3):22–30, 2008.

[14] A. Herzog and N. Shahmehri. User help techniques for usable security. In *CHIMIT '07: Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, page 11, New York, NY, USA, 2007. ACM.

[15] S. McGann and D. C. Sicker. An analysis of security threats and tools in sip-based voip systems. In *In 2nd Workshop on Securing Voice over IP*, June 2005.

[16] M. Nohlberg and J. Backstrom. User-centred security applied to the development of a management information system. *Information Management & Computer Security*, 15(5):372–381, 2007.

[17] R. H. Rayford B. Vaughn Jr. and K. Fox. An empirical study of industrial security-engineering practices. *The Journal of Systems and Software*, 61:225–232, 2001.

[18] R. S. Thompson, E. M. Rantanen, W. Yurcik, and B. P. Bailey. Command line or pretty lines?: comparing textual and visual interfaces for intrusion detection. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 1205–1214, New York, NY, USA, 2007. ACM.

[19] R. Werlinger, K. Hawkey, and K. Beznosov. Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. In *to appear in HAISA'08: Human Aspects of Information Security and Assurance (10 pages)*, July 2008.

[20] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium*, pages 169–184, 1999.

[21] W. Yurcik, R. S. Thompson, M. B. Twidale, and E. M. Rantanen. If you can't beat 'em, join 'em: combining text and visual interfaces for security-system administration. *interactions*, 14(1):12–14, 2007.