Using Auditory Display to Teach Network Intrusion Detection

Miguel Angel Garcia-Ruiz, Arthur Edwards, Raul Aquino-Santos, Miguel Vargas Martin, Samir A. El-Seoud

Using Auditory Display to Teach Network Intrusion Detection

Miguel Angel Garcia-Ruiz[1], Arthur Edwards[1], Raul Aquino-Santos[1] Miguel Vargas Martin[2], Samir A. El Seoud[3]

[1]University of Colima, Colima, Mexico
[2]University of Ontario Institute of Technology, Oshawa, Canada
[3]Princess Sumaya University for Technology, Amman, Jordan

Key words: *Computer Networks, Intrusion Detection, Auditory Display*

Abstract:

Teaching network intrusion detection, or NID (the identification of violations of a security policy in a computer network) is a challenging task, because students need to analyze many data from network logs and in real time to identify patterns of network attacks, making these activities visually tiring. This paper describes an ongoing research concerned with designing and applying sounds that represent meaningful information in interfaces (sonification) to support teaching of NID. An usability test was conducted with engineering students. Natural sound effects (auditory icons) and musical sounds (earcons) were used to represent network attacks. A post-activity questionnaire showed that most students preferred auditory icons for analyzing NID, and all of them were very interested in the design and application of sonifications.

1 Introduction

The increasing threat of cybernetic attacks has become one of the major concerns of network equipment designers and administrators. An intrusion is defined as an unauthorized access to a computer system violating some security policy. One of the main problems caused by intruders is that they consume or take over resources (e.g., bandwidth, processing power, services) and compromise vulnerable systems. In some cases, even non-vulnerable systems are affected by the massive propagation of malicious software attacks such as computer worms or denial-of-service (DoS) attacks. Moreover, we can not always assume that an intrusion detection system (IDS) can discern between malicious and non-malicious traffic; and even after diagnosing the presence of an intrusion, it requires time to decide on what the reaction should be, when disconnecting or shutting down services are not viable solutions. For an overview of intrusion detection systems see [1].

The topic of network intrusion detection, or NID, is generally taught in computer security courses, either in classrooms or in computer rooms [2]. However, teaching NID is pedagogically challenging. One of the problems that students face is that they can be easily be confounded by network accesses that appear malicious (false positives) or actual threats or attacks that go undetected (false negatives). Thus, NID is critically important, but it is a time-consuming process required to distinguish between malicious and non-malicious attacks registered in network logs and in real time. The analysis of network logs and network ports by students in real time can be visually tiring and can possibly overload their visual sensory channel (and their working memory) if it is performed repeatedly, since students have to revise many text lines of network logs and have to be constantly watching in a computer monitor graphical or text reports about network ports accesses in real time. To overcome this,

in an educational setting, we propose using sound parameters to represent information on attacks and footprints present in a network log, in addition to the log visualization.

IT security specialists are typically trained (and/or certified) by trusted institutions (such as colleges, universities, or other institutions like the SysAdmin, Audit, Network, Security Institute [3]). The education of these trainees usually covers a number of areas including exploit tools, network traffic analysis (e.g., using tcpdump), incident handling, and of course IDSs (e.g., Snort). Nevertheless, this training is rather conservative, and often does not include new education paradigms such as the one proposed in this paper. We believe that auditory displays will enhance significantly the training of IT security specialists. In this paper we describe this approach, and report on a usability study conducted with individuals who declared to be non-experts on intrusion detection but to have some knowledge in the area.

2 Past Research on NID Sonification

The Computer Science branch of Auditory Display studies non-verbal sounds that represent meaningful information in a computer interface [4]. Sound is a powerful medium in Human-Computer Interaction (HCI), used mainly for helping humans discriminate data patterns and for representing alarms, as long as the sounds are correctly designed and adapted to the computer interface. However, non-verbal sounds can be annoying if they are played too loud, or distract persons who are nearby. This difficulty may be solved, by doing careful sound design and application [5]. Sonification is the action of mapping data onto parameters of non-speech sounds (i.e. volume or loudness, timbre, pitch, duration, frequency, amplitude, and rhythm) in a computer interface [4], and its use includes mapping of scientific data to support search of data trends or patterns.

Auditory Display, and thus sonification, employs a number and types of non-verbal sounds. The most used of these types are auditory icons and earcons. Auditory icons are defined as sound effects found in nature that map information or actions at the computer interface [10]. This type of sounds and their mappings are generally easy to recognize, but they can be difficult to design. Earcons are composed of abstract, short musical sounds made of string, wind, or percussion instruments, and represent information or activities in interfaces [9]. Earcons are relatively easy to design and create, but their users have to learn the mappings prior their use in an interface.

Sonification has been used in a number of science fields, and has also been successfully applied to computer networks, and particularly to conduct NID analysis. Non-speech sounds have been successfully designed and used, at least in experimental stages, for representing web server status to detect malfunctions and malicious attacks, especially for excessive network traffic, email spam, and denial-of-service (DoS), either in real time and applied in network logs [6, 7, 8].

3 Our Approach

Sound can be an engaging medium to motivate students, especially to maintain their attention on particular information details and relationships, ease their identification of information patterns and trends, and also to serve as a “mnemonic device” for recalling “chunks” of information, among other advantages [4]. Sonification has been researched and employed successfully in educational settings, for example, for learning molecular biology [11]. In the case of Network Intrusion Detection, sonification may alleviate students’ visual channel from

being overloaded, since they generally rely on visual information for discerning network attacks and their characteristics, making this a tedious and long task. The use of multimodal interfaces (including sonification) for NID has been proposed elsewhere by [12].

Our research approach focuses on the study of Auditory Display as an effective tool for helping students in NID analysis in an educational setting. One particularly interesting question is whether sonification can lower the cognitive load of students when associating and understanding the relationships between the types of network attacks, the network ports and the occurring times. Our research is based on the Cognitive Load Theory [13], which states that effective learning takes place when the working memory load of learners is kept to a minimum to facilitate knowledge transfer to their long term memory, in which cognitive load can be decreased by adding non-redundant auditory and visual learning materials to the working environment.

In our preliminary research, we devised, developed, and tested two sonification prototypes. We sonified a network log downloaded from the Internet [14], a declassified Defense Advanced Research Projects Agency (DARPA) log from the U.S. that is publically available for research reasons. It contains markers of five types of possible attacks that were mapped onto earcons in the first prototype, and auditory icons in the second one. Those mappings are described in detail and can be downloaded from http://docente.ucol.mx/~mgarcia/Sonificatedlog.htm..

A .WAV file with the log sonification and auditory icons was generated using our program developed in Tcl/Tk language. For the first prototype, these are the mappings of auditory icons to the five types of attacks registered in the log:

A frog sound is mapped onto “guess”
A cat sound is mapped onto “rcp”
A horse sound is mapped onto “rsh”
A cock sound is mapped onto “rlogin”
A bird sound is mapped onto “port-scan”

We generated a second sonification prototype using earcons (piano notes). These are the mappings of earcons to the five types of attacks registered in the log:

A 128Hz key note is mapped onto “guess”
A 197Hz key note is mapped onto “port-scan”
A 263Hz key note is mapped onto “rcp”
A 525Hz key note is mapped onto “rsh”
A 1056Hz key note is mapped onto “rlogin”

In an exploratory fashion, the sounds were randomly chosen and downloaded from the Internet, and were designed according to their sound parameters of pitch and timbre, following the Auditory Display design guidelines from [4]. In an attempt to facilitate recognition, all the sounds were played at different stereo positions.

4 Usability Study

Based on our research approach and using our two sonification prototypes, we conducted an informal usability test with a group of Telematics engineering students. The purpose of our preliminary usability study was to obtain initial student feedback on the delivery media and

types of sound sources to represent network attacks, and thus modify them or choose other types of sounds or sound parameters in later developments. Usability measures, among other aspects, the efficiency, efficacy, errors, and pleasantness of use of a computer interface [15]. Usability studies are important because past research has been found that educational software with high usability has a positive support for learning [16].

4.1 Test Design

We designed a usability test, which was carried out with a group of students. After the test, we administered a post questionnaire with questions to obtain subjective opinions on the sounds quality and sound sources for representing attacks in NID, as well as the pleasantness of the sounds played.

4.2 Materials

For playing the sonifications, a set of Labtec Pulse 475 computer speakers (comprised of a pair of speakers and a subwoofer, rated at 28 Watts RMS) was used for playing the sonifications. We used this set of speakers because of its low cost, easy transport, simple set up, good audio fidelity, and loudness. The speakers were placed on tripods in front of the classroom to ensuring all students could easily listen to the sounds, and were placed at a height of approximately 1.80 meters, and had about five meters of separation. We used a laptop that was connected to a data projector to show the test objective and the log sound mappings, as well as to play the prototype sonifications. The speaker set up is shown in Figure 1. The sonification prototypes earlier described in this paper were used in the test.

Figure 1. Students participating in the usability test.

4.3 Participants of the Test

Twenty-nine Telematics Engineering students were asked to volunteer in the usability test. The students averaged 20 years (3 women and 26 men), representing both the size and the composition of a typical class at the College of Telematics of the University of Colima.

Although most of the students knew the basics of computer networks, none of them knew of network intrusion detection. Sixteen participants had received differing degrees of musical training or knew how to play a musical instrument, and none reported to suffer hearing problems. Although none of them have designed auditory icons or earcons before, most of them are competent in computer programming.

4.4 Procedure

To assure ecological validity to the usability test, it was conducted in one of the classrooms of the College of Telematics. The purpose of the test and its sound mappings were explained to the students using a Powerpoint projection. The students listened to the sound mappings (earcons and auditory icons) and read their corresponding network values on the projection four times. After that, students listened to the two sonification prototypes only; the Powerpoint projection was turned off. The auditory icons' sonification was played first. After playing the sonification, a number of questions were asked, including: How many auditory icons could you identify? What is the auditory icon mapping to "port-scan" and "rlogin"? Next, the earcons sonification was played, and the same questions again asked. After playing the sonifications, a usability questionnaire was administered to the students, which included questions with Likert scales, as shown in Table 2.

5 Results

Table 1 summarizes a list of earcons and auditory icons that students suggested in the questionnaire for making new non-speech sounds to represent network attacks. We found that most of the suggested auditory icons are of violent nature. Eight students preferred to use guitar sounds for developing earcons. Similarly, a different set of eight students suggested drums for earcons. The other students listed diverse musical instruments. Table 2 depicts some of the questions with Likert scales about the sound usability.

Sounds for creating earcons	Sounds for creating auditory icons
Guitar	Breaking glass
Electric guitar	Breaking china (plates)
Drums	Water stream
Trumpets	Thunder
Violin	Nature sounds
Bass	Rain
Cello	Beach waves
Piano	Cars crashing
Flute	Screams
	Dog barking

Table 1. A summary of the sounds suggested by students for representing network attacks.

Likert scales	Average scale value
The sounds volume level (loudness) was perceived as adequate	1
The sounds were clearly heard	2

The auditory icons were useful for recalling the attacks	1
The earcons were useful for recalling the attacks	5
Both earcons and auditory icons can be useful for learning NID	2

Table 2. Opinion scales of the questionnaire
(1=strongly agree, 5=strongly disagree)

6 Conclusions

This paper described an exploratory research concerned with designing and applying sounds that represent meaningful information in interfaces (sonification) to support teaching of NID. An usability test was conducted with Telematics students, where natural sound effects (auditory icons) and musical sounds (earcons) were used to represent network attacks. A post-activity questionnaire showed that most students preferred auditory icons for analyzing NID, and all of them were very interested in the design and application of sonifications.

The previous musical training of some students did not affect their outcome in the post-questionnaire; their answers were consistent with the rest of the group. Men and women reached almost the same conclusions on their usability opinions. In addition, none of the students complained about the speakers' sound quality. This means that even modest sound equipment can be effective for delivering sonifications in classrooms. Most of the students showed enthusiastic in the test, and wished to continue on participating in testing NID sonifications. As this usability test was informal, further usability studies are needed to study the sonifications in controlled experiments and in different educational settings, for example, in a computer room.

However, there was no student consensus on which sounds would best represent software or hacker attacks in a network using auditory icons and earcons. Interestingly, one student suggested using Morse code to represent NID. Auditory icons appeared to perform better in identifying attacks, although more formal usability tests are needed to confirm this. Earcons did have a flaw in their design; the piano notes, although were distinctive from one another in terms of pitch, all of them were made of piano notes. They should be made of different musical instruments to ease mappings learning.

The students' comments indicate that the auditory icons and earcons played at different stereo positions helped them to better identify the mappings of the network attacks. Also, the speaker separation was very effective for conveying a stereo sound effect.

In further sonification prototypes, we will let students choose their own sounds (auditory icons and earcons) from a repertoire. This certainly will help them to remember the mappings between the types of attacks and the sounds. In addition, we will test new forms of mapping the network attacks with non-speech sounds, as well as other types of sound delivery media, such as headphones or more powerful speakers.

References:

[1] van Oorschot, P.C., Robert, J.M., Vargas Martin, M.: A Monitoring System for Detecting Repeated Packets with Applications to Computer Worms. International Journal of Information Security. Springer. Vol. 5, No. 3, pp. 186-169, 2006.

[2] Frank , C.E. and Wells, G.A. Tutorial on laboratory exercises for a computer security course. Consortium for Computing in Small Colleges, 2006.

[3] SysAdmin, Audit, Network, Security (SANS) Institute: URL: http://www.sans.org [last visited: July 25 2007].

[4] Kramer, G., ed. Auditory display: Sonification, audification, and auditory interfaces. Santa Fe Institute Studies in the Sciences of Complexity, Proc. Vol. XVIII. Reading, MA: Addison-Wesley, 1994.

[5] Shneiderman, B., Plaisant, C. Designing the User Interface: Strategies for Effective Human-Computer Interaction. Fourth edition. Boston, MA: Addison-Wesley, 2006.

[6] Barra, M., Cillo, T:, De Santis, A., Petrillo, U.F., Negro, A. and Scarano, V., Personal WebMelody: Customized sonification of web servers. Proceedings of the International Conference on Auditory Display (ICAD), Espoo, Finland, 2001.

[7] Gilfix, M. and Couch, A., Peep (The network auralizer): Monitoring your network with sound. Proceedings of 14th System Administration Conference (LISA XIV), New Orleans (LA) USA, 2000.

[8] Gopinath, M.C., Auralization of intrusion detection system using Jlisten. Unpublished thesis, Birla Institute of Technology and Science, India, 2004.

[9] Blattner, M. M., Sumikawa, D. A., and Greenberg, R. M. , Earcons and icons: their structure and common design principles," Human–Computer Interaction, vol. 4, pp. 11–44, 1989.

[10] Gaver, W. W., Auditory icons, using sound in computer interfaces. *Human– Computer Interaction*, vol. 2, pp. 167–177, 1986.

[11] Garcia-Ruiz, M.A. and Gutierrez-Pulido, J.R., An overview of auditory display to assist comprehension of molecular information. Interacting with Computers, 18(4), pp 853-868, 2006.

[12] Garcia-Ruiz, M.A., Vargas Martin, M., Green, M., Towards a Multimodal Human-Computer Interaction to Analyze Intrusion Detection in Computer Networks. In Proceedings of the First Human-Computer Interaction Workshop (MexIHC), University of the Americas, Puebla, Mexico, 2006.

[13] Chandler,P. and Sweller, J., Cognitive load theory and the format of instruction. Cognition and Instruction, 8(4), 293-332, 1991.

[14] MIT Lincoln Laboratory (1999). DARPA intrusion detection evaluation: Data sets. Available at: http://www.ll.mit.edu/IST/ideval/data/data_index.html.

[15] Dumas, J.S., and Redish, J.C.., A practical guide to usability testing. Exter, England: Intellect, Ltd; Revised edition, 1999.

[16] MacFarlane S, Sim G, Horton M., Assessing usability and fun in educational software. In Proceeding of the 2005 Conference on interaction Design and Children. Boulder, Colorado, 2005.

Authors:

Miguel Angel Garcia-Ruiz, Ph.D.
University of Colima, College of Telematics.
Ave. Universidad 333, Colima, 28040, Mexico
Email: mgarcia@ucol.mx

Arthur Edwards, M.Sc.
University of Colima, College of Telematics.
Ave. Universidad 333, Colima, 28040, Mexico
Email: arted@ucol.mx

Raul Aquino-Santos, Ph. D.

University of Colima, College of Telematics.
Ave. Universidad 333, Colima, 28040, Mexico
Email: aquinor@ucol.mx

Miguel Vargas Martin, Ph.D.
University of Ontario Institute of Technology,
Faculty of Business and Information Technology and
Faculty of Engineering and Applied Science
Oshawa, Canada
Email: miguel.vargasmartin@uoit.ca

Samir A. El-Seoud, Ph. D.
Princess Sumaya University for Technology, Amman, Jordan
Email: selseoud@yahoo.com