Poster: Towards Music-Assisted Intrusion Detection

Adrienne Brown, Miguel Vargas Martin,
Bill Kapralos, Mark Green
University of Ontario Institute of Technology
Oshawa, Canada
adrienne.brown@rogers.com, {miguel.vargasmartin,
bill.kapralos, mark.green}@uoit.ca

Miguel A. Garcia-Ruiz
University of Colima
Colima, Mexico
mgarcia@ucol.mx

***Abstract*—The vast majority of intrusion detection systems (IDS) and network IDS convey notifications or alarms using visual interfaces, and some use a combination of visual and sound interfaces. While automatic response is critical to counter fast spreading attacks, it is also important to notify users about the status of a system in a synthesized and concise manner. We explore the usability of sound in complementing automatic response systems. We also give directions towards the design of a more advanced sonification system that will modify well-known melodies or songs to convey useful information to users in real time.**

Keywords-intrusion detection; sonification; behaviour analysis

I. INTRODUCTION

Most of the research on multimodal interfaces to support intrusion detection systems (IDS) and network IDS (NIDS) is focused on bimodal approaches such as visual and sound, or haptic and visual, but there is a lack of studies about the integration of these modalities. Sonification refers to the use of non-speech sound to convey information or data [6]. Just as visualization can be used to provide a visual representation of some complex data, sonification can provide sound-based representation of information whereby the data are mapped to various auditory parameters such the loudness or pitch of the output sound. Sonification has long been established in the area of auditory display and is commonly used in cases where a constant awareness of some form of information is required. A typical example is the Geiger counter where radiation level is mapped to the frequency of audible clicks. Our approach takes advantage of the "cocktail party effect", i.e., the ability of humans to ignore distracting sounds and keep focused only on sounds that help them complete the task at hand. Sound can be unpleasant if it is played too loud, and can be annoying and distracting for others who are also present in the same room where the sound is played, however this situation could be mitigated if an appropriate set of sounds is used, for example music.

Usability is a branch of the area of Human-Computer Interaction (HCI). It has defined by Dumas et al. [2] as "the people who use the product can do so quickly and easily to accomplish their own tasks". Usability testing comprises in-situ studies and analyses of a computer interface made by a number of users and usability experts, based on established methods and protocols [7]. Usability tests serve to measure, among other issues, how effective and efficient is an auditory computer interface, among others, and how pleasant and easy is it to use under a specific context of use [5], for example a computer laboratory, or an IT department where network sonifications are to be analyzed.

A number of efforts have been made to effectively sonificate network activity; however, the problem of sonificating network traffic to convey useful information that assists intrusion detection is still widely unexplored. Despite the benefits of incorporating sound, when incorporated into an auditory display and when used for sonification, there are several important considerations that must be addressed. Barra et al. [1] and Gilfix and Couch [3] used sound to effectively represent web server status, in order to inform the administrator about web malfunctioning and other issues regarding email spam, high load, and excessive network traffic. Auditory display in interfaces has been studied for NIDS analysis. Varner and Knight [10] proposed an audio/visual and agent-based system for monitoring the network in real time to identify malicious attacks; however, while the authors emphasize the potential benefits of enhancing IDSs with multimodal interfaces, they do not report on prototypes or experimentation. Gopinath [4] carried out a study where data from network logs was sonified to signal malicious attacks by identifying false positives and denial of service attacks; usability studies of this approach indicated that sonification may increase user awareness in intrusion detection. Qi et al. [8] presented a sonification system that maps the activity of a particular NIDS into a number of piano sounds (the sounds can be found at http://www.hrl.uoit.ca/mvargas/IDS_sonification/SoundRecording.zip); their NIDS arranges network packets into a number of queues depending on how many times each packet has been seen during a "short" time period. The sounds generated reflect the number of packets in the queues in real time.

Contributions. (1) We explore the usability of sound in assisting and complementing NIDS. (2) We also describe the problem of designing a network sonification system that effectively maps network traffic to convey useful information that assists network administrators in their decision making. (3) Moreover, we provide directions for the design of more sophisticated sonification systems that are capable of modifying the way a musical piece is played.

II. SOUND-ASSISTED INTRUSION DETECTION

In contrast to the works reported in the literature, we focus our attention on the problem of effectively sonificating raw traffic, as opposed to sonificating the activity of a particular NIDS.

Fig. 1 depicts a summary of the possibilities that network administrators may encounter when a manual response is necessary. As the potential consequences of an attack increase, it becomes obvious that an action is required. For example, if a known signature attack is detected by the NIDS an action will definitively follow without further consideration; this action will most likely be performed by an automatic security control (put in place by the administrator). However, if the NIDS is only able to detect "suspicious" network activity then the administrator has to apply their judgement to make a decision on the course of action.

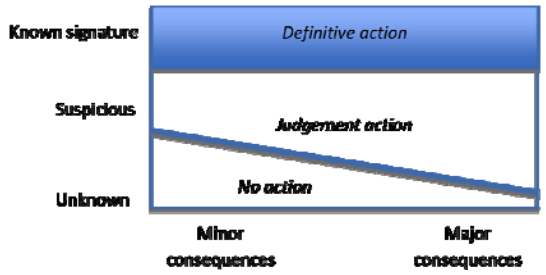

Figure 1. Sonification-based IDSs can assist in the "Judgement action" zone, depending on the certainty and consequences of the suspected attack.

III. CURRENT STATE OF OUR SYSTEM

Our system [8], in its current state, is able to play distinguishable sounds that convey meaningful information reflecting network status. To achieve this, we built a NIDS [19] that is capable of classifying disruptive traffic into a *delay queue*. By no means, this NIDS is 100% accurate, but we only used it to build our proof-of-concept (we could have also used a well-known NIDS such as Snort Inline, but our own NIDS was good enough for the purposes at hand). One modality of the sonification engine maps the byte-rate and the packet rate of the delay queue into frequency and intensity of piano notes, respectively.

IV. MUSIC-ASSISTED INTRUSION DETECTION

We are currently working on a more sophisticated version of our system which includes playing back well-known melodies or songs and introducing changes in signature tone, accented rhythm, flat and sharp notes, pitch, and volume variations depending on network activity in such a way that each traffic anomaly can effectively change the way the melody is played. To this end, we are exploring audio libraries such as STK (http://ccrma.stanford.edu/software/stk/). This system will address the challenging problem of sonificating network traffic without the support of a NIDS. A difficulty we face is to be able to collect and aggregate traffic in such a way that a NIDS would not be able to infer an attack but a trained human being would. Thus, referring to Fig. 1, our system should be able to alert the administrator about network situations in the "judgement action" zone, where automated solutions are not suitable. If we achieve this, our music-assisted system will be useful in supplementing a conventional anomaly-based NIDS, and thus the whole security system will be able to generate "suspicious" as well as "supplemented-suspicious" to allow a human begin to correlate both and infer attacks more easily and faster.

Table 1 presents a summary of traffic-to-music mapping alternatives that we are currently studying.

TABLE I. TRAFFIC-TO-MUSIC ALTERNATIVES

Traffic characteristic	Effect in play back
Prolonged increase in traffic volume	Sharp notes will be introduced and increase at an exponential rate as the period prolongs. Flat notes will override sharp ones as volume returns to "normal"
Number of TCP handshakes in progress	Pitch will shift according to the number of half-processed handshakes which are about to timeout
Number of HTTP error messages	Rhythm variations according to certain rules such as frequency of these messages

REFERENCES

[1] M. Barra, T. Cillo, A. De Santis, U.F. Petrillo, A. Negro, Scarano, "Personal webmelody: Customized sonification of web servers," in *Proceedings of the International Conference on Auditory Display*, Espoo, Finland, July 29 – August 1 2001.

[2] J.S. Dumas, J. Redish, "A practical guide to usability testing" (2nd Ed.), Intellect, Bristol, UK, 1999.

[3] M. Gilfix, A.J. Couch, "Peep (the network auraizer): Monitoring your network with sound," in *Proceedings of System Administration Conference*, Orleans, USA, December 3 – 8 2000.

[4] M.C. Gopinath, "Auralization of intrusion detection systems using Jlisten," Master's thesis, Birl Institute of Technology and Science, India, 2004.

[5] International Standardization Organization, "Ergonomic requirements for office work with visual display terminals (VDTs)," Part 11: Guidance on usability, ISO 9241-11:1998.

[6] G. Kramer (ed.), "Auditory display: Sonification, audification, and auditory interfaces. Santa Fe Institute Studies in the Sciences of Complexity," *Proceedings* Vol. XVIII, Reading, USA, Addison-Wesley, 19994.

[7] J. Nielsen, R.L. Mack, "Usability inspection methods," Wiley, Hoboken, USA, 1994.

[8] L. Qi, M. Vargas Martin, M.A. Garcia-Ruiz, M. Green, and B. Kapralos, "Toward sound-assisted intrusion detection systems," in *Proceedings of International Symposium of Information Security*, Algarve, Portugal, November 25-30 2007.

[9] L. Qi, M. Zandi, and M. Vargas Martin, "A network mitigation system against denial of service: A Linux-based prototype," in *Proceedings of Internet and Multimedia Systems and Applications (EuroIMSA)*. Chamonix, France, 2007.

[10] P.E. Varner, J.C. Knight, "Security monitoring, visualization, and system survivability," in *IEEE/SEL Information Survavibility Workshop*, 2001.