Toward Sound-Assisted Intrusion Detection Systems

Lei Qi, Miguel Vargas Martin, Bill Kapralos,
Mark Green, and Miguel García-Ruiz

[1] University of Ontario Institute of Technology, Oshawa, Canada
lei@navdriver.com, {miguel.vargasmartin,bill.kapralos,mark.green}@uoit.ca
[2] University of Colima, Mexico
mgarcia@ucol.mx

Abstract. Network intrusion detection has been generally dealt with using sophisticated software and statistical analysis, although sometimes it has to be done by administrators, either by detecting the intruders in real time or by revising network logs, making this a tedious and time-consuming task. To support this, intrusion detection analysis has been carried out using visual, auditory or tactile sensory information in computer interfaces. However, little is known about how to best integrate the sensory channels for analyzing intrusion detection alarms. In the past, we proposed a set of ideas outlining the benefits of enhancing intrusion detection alarms with multimodal interfaces. In this paper, we present a simplified sound-assisted attack mitigation system enhanced with auditory channels. Results indicate that the resulting intrusion detection system effectively generates distinctive sounds upon a series of simple attack scenarios consisting of denial-of-service and port scanning.

Keywords: Intrusion detection, computer networks, computer forensics, human-computer interfaces, multimodal interfaces.

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 (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 takes time to decide on what action should be taken, when disconnecting or shutting down services are not viable solutions [26].

A multimodal interface consists of the integration of multiple human sensory modalities in a computer interface that allows the human and the computer

R. Meersman and Z. Tari et al. (Eds.): OTM 2007, Part II, LNCS 4804, pp. 1634–1645, 2007.

to exchange information, that is, to interact [2,20]. Multimodal interfaces involve human input modalities (gaze, head movements, gestures, speech, etc.) and computer output modalities (mainly the visual, auditory, and tactile display of information) that need to be adequately integrated to have a useful application.

Several proactive and reactive defence approaches have been proposed. Some of these are signature and anomaly-based, and some of them use self-learning techniques, ranging from probabilistic analysis [31] to neural networks [12]. The reaction techniques can vary from raising an alarm or delaying traffic to complex auto-configurable mechanisms [25] or automatic generation of signatures [17]. Typical IDS rely on the presence of common attacks' characteristics such as performing "many" similar actions in a "short" period of time [29], spoofing IP addresses [22], attempting connections to or from non-existing hosts or services [27], etc. Intrusion attacks are becoming clever in the ability to hide or attenuate any identifiable characteristics by protecting themselves against reverse engineering, implementing polymorphic techniques [4], or by propagating to a pre-defined set of hosts taken from a pre-computed hit-list [5].

A number of IDSs have been proposed (e.g., [13,14,32]), and some have been advanced commercially [25]. One way to assess the efficiency of IDSs is based on the number of false positives and false negatives generated. A false positive is an alarm generated under the absence of any intrusion, whereas a false negative is an intrusion that goes undetected. An ideal IDS would produce no false positives while having no false negatives; however such IDS is yet to exist. Therefore, analyzing IDS logs is a challenging task due to the large number of entries representing false positives or false negatives [29].

We have previously reported on the benefits and pitfalls of multimodal (i.e., visual, auditive, gustatory, olfactory, and tactile) interfaces to enhancing intrusion detection systems [6]. One disadvantage of auditory interfaces is that sound is volatile, and thus exists for a limited time (i.e., humans may dismiss alarms without noticing). Even though sound may be annoying if poorly designed and/or played, audible alarms are useful for driving attention on particular tasks of the IDS (e.g., notifying the user that packets are being dropped). Furthermore, while different individuals have different pitches, auditory interfaces can be useful for detecting information patterns of malicious software (e.g., worms) because they allow humans to identify particular sounds from a group of alarms ("cocktail party effect"). Thus, sound may complement visual-based IDSs allowing both modalities to complement each other.

To date, most of the research on human-computer interfaces to support intrusion detection has focused on bimodal applications (e.g., visual and sound, or haptic and visual) to convey intrusion information (see for example, [21]), but there is a lack of studies regarding the integration of these modalities in the domain of intrusion detection. In addition, very little research has examined three or more sensory modalities at the computer interface for the analysis of intrusion detection. It is necessary to determine which sensory combinations work best in our context. Most of the related work shows that the use of sensory channels in computer interfaces have been used as tools for the human network analyst

to gauge what has been already computed and filtered out with respect to network traffic and network logs. Multimodal interfaces can augment the capacity of the human analyst to cope with large amounts of information both online (i.e., traffic) or offline (i.e., contained in network logs) in search of malicious attacks.

In this paper we take a step further to the corroboration of our ideas presented in [6,7] regarding the benefits of coupling intrusion detection and mitigation with auditory user inerfaces. In particular, we present a sonification-based IDS which uses a mitigation system previously reported (i.e., without sound) in [24]. Section 2 presents an overview of multimodal approaches related to network monitoring and intrusion detection systems, whereas Section 3 describes the mitigation system used in our sonification. The sonification and preliminary experiments and prototype are presented in Section 4. We close with conclusions and directions for future work in Section 5.

2 Related Work

Valdes and Fong [28] present a visualization technique of network activity. This technique allows visual detection of vertical and horizontal scanning through graphical combinations of source and destination IP addresses and ports. They indicate that appropriate entropy analysis may enable this technique for early detection of malicious traffic (see also [19]).

With the huge amount of network information that flows in a typical organization or institution nowadays, it is difficult to cope with traffic analysis using visualization alone, almost certainly causing sensory overload if one human sense alone is used to analyze that information.

Auditory display is the use of non-speech sound to present information [15]. Auditory display is currently employed in a variety of complex environments including computers, medical workstations, aircraft cockpits, and control centers in nuclear reactors (see [9,16]). Sonification is a specific type of auditory display whereby "data relations are transformed into perceived relations in an acoustical signal for the purposes of facilitating communications or interpretation" [16]. In other words, sonification is the mapping of data onto parameters of non-verbal sound such as pitch, volume, timbre, duration, frequency, amplitude, and rhythm in a computer interface [15]. Although sparse, several studies have investigated the use of sound-based interfaces for network intrusion detection.

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. 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. An alternative is to have the analyst wear headphones, especially those that are closed-cup to cover the ears and thus avoid disturbing others nearby. Barra *et al.* [1] and Gilfix and Couch [8] 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 network intrusion detection (NID) analysis. Varner and Knight [30] 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 [10] carried out a study where data from network logs was sonified to signal malicious attacks by identifying false positives and DoS attacks; usability studies of this approach indicated that sonification may increase user awareness in intrusion detection.

With respect to Human-Computer Interaction (HCI), intrusion detection analysis has been carried out using visual, auditory and haptic information channels, where most of the studies have been done with two modalities at the same time. Although visual, auditory, and tactile channels have been studied and also used separately for intrusion detection, little is known about how to best combine the sensory channels and using the senses of taste and smell in a computer interface for analyzing intrusions. In multimodal interfaces, each modality can reinforce, supplement or complement each other, with the goal of alleviating cognitive load and allowing extra information channels [18].

3 Overview of the Mitigation System Used for Sonification

The mitigation system used here is based on the typical components of traffic shaping and Bloom filters with counters (BFWC). The main idea consists of classifying packets dynamically, based on the number of times packets are forwarded. Packets found to consume disruptive amounts of bandwidth within a short time period will be classified into busier queues. This classification does not stop attack packets but limits their speed of propagation and their bandwidth consumption. In this sense, this mitigation consists of merely delaying disruptive traffic up to the point that all the applications make a more equitable use of bandwidth. The system architecture and its packet classification rules are described in the following sections. A complete description of this mitigation system (i.e., without sounification) can be found in [24].

3.1 Architecture

The system uses the three typical components of traffic shaping: classification, queuing, and scheduling. Classification consists of identifying and categorizing packets into different classes. Different classes of traffic are placed into different queues (some queues may accommodate more than one class). The scheduler decides which queue will be served next. The architecture is depicted in Fig. 1. The idea is to have an in-line BFWC which counts packet-subset (in the experiments reported in this paper, we used packet-subsets of the form [destination port, payload]) repetitions and defines classes based on this information.

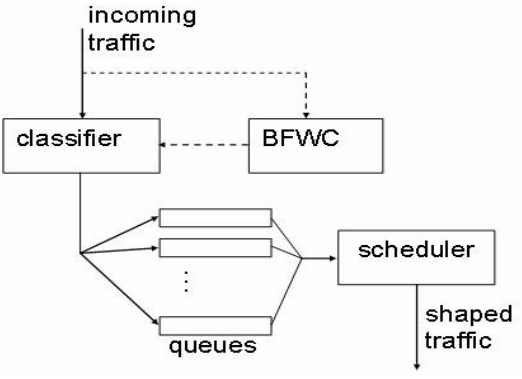

Fig. 1. Architecture of the mitigation system enhanced with sonification

3.2 Packet Classification

Packets are classified into a number of queues, q. The system's administrator sets the number of queues depending on the characteristics of the network and the fields used in the packet-subset. Packet classification takes place only upon congestion. Congestion can be detected by monitoring the rate of dropped packets. A threshold of dropped packets can be used to set on (or off) a congestion flag when congestion actually occurs. However, in our experiments, we keep the system active even under no congestion.

The packet-subset p of every incoming packet P is processed by the BFWC. If the congestion flag is on, P will be classified according to the following rules:

If $1 \leq t_0 \leq \lfloor z \rfloor$, P is put into queue 1;
If $\lfloor z+1 \rfloor \leq t_0 \leq \lfloor 2z \rfloor$, P is put into queue 2;
If $\lfloor 2z+1 \rfloor \leq t_0 \leq \lfloor 3z \rfloor$, P is put into queue 3;
$\vdots$
If $\lfloor (q-1)z \rfloor \leq t_0 \leq t$, P is put into queue q,

where $z = t/q$ (for $t > q$); t is the maximum possible value of every counter of the Bloom-table ($t = 2^c - 1$, cf. Fig. 2); and t_0 is the minimum value of the k corresponding counters of p in the Bloom-table (i.e., the inferred number of repetitions of p).

4 Sonification

One way of applying multimodality in intrusion detection is to integrate sensory channels in a virtual reality (VR) environment, since VR is multimodal by definition. VR can be defined as "a high end computer interface that involves real time simulation and interaction through multiple sensorial channels" [3]. Our approach is to study the benefits of a multimodal human-computer interface (using three or more sensory channels) to analyze malicious attacks during

forensic examination of network traffic or network logs (these ideas were first proposed in [6]). In this section we describe our experiments and the sonification methodology used in the experiments.

4.1 Sound Generation

The sonification here focused on the problem of mapping the input parameters from the mitigation system (represented by a number of inputs varying through time) onto the parameters controlling a synthesis algorithm. In other words, map number of inputs into sound with the intention of making this sound perceptible to humans and allow them to distinguish from different scenarios. There are 32 data series output from the mitigation system representing the continuous values for byte-rate (bytes per second) and packet-rate (packets per second) of 16 queues ($q_0 \sim q_{15}$). In particular, those mitigation output data series are generated with a resolution of 200 ms and reflect the traffic classification patterns of the mitigation system varying through time. From those traffic patterns, the picture of current network traffic passing through the mitigation system will be displayed. Particularly, traffic from the last queue (i.e., q_{15}) is expected to contain "only" disruptive/malicious traffic. These data constitute our data set input for sonification.

Two different mitigated traffic pattern-to-audio (or pattern change-to-audio) mappings were experimented with. Since most people are familiar with the notes of the musical scale (see [11]), traffic patterns were mapped to the 88 keys of the piano keyboard (52 white keys and 36 black keys). The frequencies of the piano keyboard range from 27.50Hz to 4186Hz. This follows the scale of equal temperament in which every octave (a 2:1 change in frequency), is divided into 12 equal intervals allowing for the frequency of adjacent notes to differ by a factor of $\sqrt[12]{2}$.

Mapping 1. As previously described, the last queue (i.e., q_{15}) is a direct indication of disruptive traffic. Thus a data sonification mapping that maps the byte-rate (b_{15}) and the packet-rate (p_{15}) of the last queue to frequency and intensity of the audio signal respectively is employed. The mapping is accomplished using the following relations for the frequency (f) and amplitude (a) for the output sound:

$$f_{15} = 27.5(\sqrt[12]{2})^{\lfloor (b_{15}/B_{15})N \rfloor}, \tag{1}$$

$$a_{15} = \left\lfloor \frac{p_{15}}{P_{15}} M \right\rfloor, \tag{2}$$

where $N = 88$ (number of piano keys), $M = 2^{15} - 1$ (maximum amplitud), B_{15} is the maximum byte-rate of queue 15, and P_{15} is the maximum packet-rate of queue 15. Once the frequency and amplitude of the signal are known, the corresponding audio signal (pure tone), $x(n)$, is generated as follows:

$$x(n)_{15} = a_{15} \times \cos(2\pi n f_{15}/f_s), \tag{3}$$

where $f_s = 44\,100$ is the sampling rate (in Hz), and n is the index in the discrete time domain. The generated frequency corresponding to the byte-rate of q_{15} is depicted in Fig. 2.

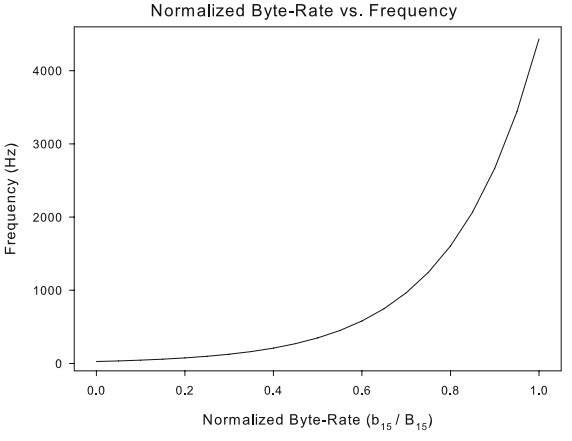

Fig. 2. Normalized frequency described by (1)

Mapping 2. The second sound mapping of this work used the byte-rates and packet-rates present in each of the 16 queues as input data for the sonification process. In this mapping, the 88 piano keys are divided into 16 groups, $G_0 \sim G_{15}$, where G_0 includes the first five frequencies (keys) of the piano keyboard, G_1 includes the next five frequencies (keys) and so on, and finally, G_{15} contains the last five frequencies (keys) of the piano keyboard. The byte-rates $b_0 \sim b_{15}$ from the 16 queues are mapped to one of the frequencies in the corresponding set of keys $G_0 \sim G_{15}$ respectively as follows: (b_i/B_i) maps to frequency f_i in G_i, for $0 \leq i \leq 15$, where B_i is the maximum byte-rate of queue i.

As with the first mapping (Mapping 1) described above, the packet-rates from the 16 queues could be mapped to 16 amplitudes: $a_0, a_1, \ldots a_{15}$ using (2). This results in 16 sounds (tones) represented by their frequencies and amplitudes $(f_0, a_0), (f_1, a_1), \ldots (f_{15}, a_{15})$. The corresponding output sound is then determined by the following formula using (3):

$$x(n)_{\text{sum}} = \sum_{i=0}^{15} x(n)_i. \tag{4}$$

4.2 Experiments and Preliminary Results

Fig. 3 illustrates the layout of our experimental equipment. We configured a single machine (3.20 GHz Pentium 4 with 1 GByte RDRAM, two 100 Mbit Ethernet network cards) as a router running Linux Kernel 2.6 and a BFWC

module. We also used a collection of four machines (3.20 GHz Pentium 4, 512 MBytes RAM, and running Linux Kernel 2.6) as attacking machines for running DoS and nmap. Finally, the victim is an FTP (File Transfer Protocol) server (3.20 GHz Pentium 4 with 1 GByte RDRAM) running Windows 2003 and IIS (Internet Information Services).

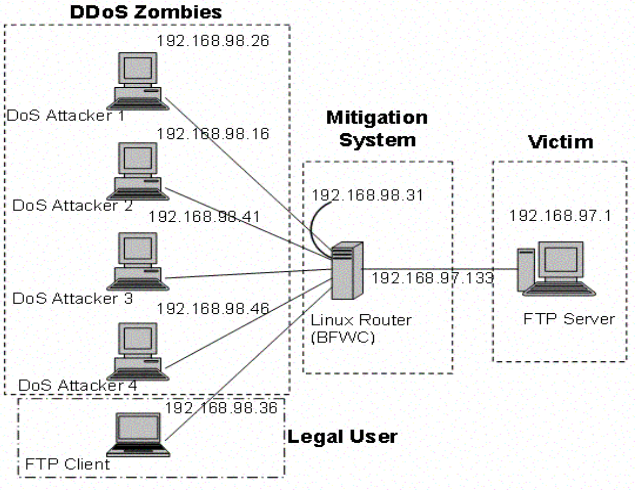

Fig. 3. Experimental environment setup

Disruptive vs Non-disruptive Traffic: The traffic in our test network consist of disruptive and non-disruptive traffic. We define *disruptive traffic* as the packets generated by the DoS or the port scaning tools (see subsections below) from the attacking machines. The traffic generated by the FTP Server and FTP Client are defined as *non-disruptive traffic*.

Denial-of-Service: The four attacking machines use TFN2K (Trible Flood Network 2000), a powerful DoS tool that can employ typical DoS attacks such as ICMP Flood, SMURF Flood, SYN Flood, UDP Flood, Targa3, and any combination of these attacks. During the experiments, TFN2K was used only to perform SYN Flood attacks. The four attacking machines were configured to bombard the victim machine. The configuration of the equipment is as follows: we setup the FTP Server running IIS to receive FTP and HTTP requests through the Linux Router machine which is implementing the sonification system. The four attacking machines on the other side target the FTP server. Finally, another Linux machine (FTP Client) is used as a non-malicious workstation to access the FTP Server through the intermediate Linux Router. The traffic in this test network consist of disruptive and non-disruptive traffic.

Port scanning: In this part of the experiment only one of the four attacking machines is used (the remaining machines did not participate at all). The attacking machine used nmap to perform a port scan on the victim machine. nmap

was set up to scan a subnet of IP addresses ranging from $x.y.0.0$ to $x.y.255.255$, and for every single IP scan ports 0 to 1024.

We used three different scenarios for both attacking schemes (DoS and port scaning).

Scenario 1. In this scenario the attack tool (TFN2K or nmap) is shut down in the attacking machine(s) and the mitigation system mechanism in the Linux Router is enabled. The FTP Client then accesses the FTP Sever to upload a large file into the FTP Server.

Scenario 2. Here the attack tool (TFN2K or nmap) was allowed to attack the FTP Server from the attacking machine(s). The mitigation system mechanism was disabled for this scenario. Again the FTP Client machine was allowed to upload a large file into the FTP Server. The purpose of this scenario is to show the severity of the attack. It was observed that the performance of the victim machine was degraded dramatically, close to the point of being non-operational.

Scenario 3. In this scenario the attacking machine(s) was allowed to attack the FTP Server, except that this time the mitigation system was enabled in the Linux Router. Under this scenario, while attack packets (DoS or port scans) were dropped (i.e., put into queue 15), the system was able to emit alarm sounds.

Analysis of generated sounds. For each of the two mappings (described in Section 4.1), we ran the experiments under Scenarios 1 and 3: (a) Scenario 1 did not generate any sounds using Mapping 1 (as expected for this mapping). This situation is ideal, since we would not want the system to generate any sounds under "normal" traffic conditions, where no attacks are underway. Opposed to Mapping 1, Mapping 2 does generate sounds under Scenario 1; these sounds are due to the FTP file transfer, and may not be desirable under "normal" conditions. (b) For both mappings, Scenario 3 produces sounds that may allow humans to distinguish between different attacks. The sounds generated by this scenario are "notably" different in such a way that distinguishing between DoS and port scanning is relatively easy (while the system mitigates the attack automatically). This indicates that multimodal interfaces coupled with effective mitigation systems may result in better IDSs that allow system administrators to realize, through audio signals, what mitigation actions are underway, and in response to what type of attack. The sounds generated in our experiments can be downloaded from [23]. To confirm the user benefits of our sound-assisted IDS, we would need to conduct a formal usability study; however, this task is out of the scope of the present work (see future work below).

5 Concluding Remarks and Future Work

In this paper we have reviewed the literature related to the use of multimodal interfaces in intrusion detection. Furthermore, we presented an attack mitigation system enhanced with sound alarms, which was tested under a number of simple attack scenarios including denial-of-service and port scanning.

The results indicate that sound may complement intrusion detection and mitigation systems while taking advantage of all the benefits of audible interfaces. Our work represents an ongoing effort toward the design of alternative interfaces for complex intrusion detection systems such as Snort. We have yet to test our system under other attacks and using more and diverse legitimate traffic. We also plan to employ sonification into other intrusion detection systems to see how sound can improve their effectiveness in conveying useful information for human analysis.

Furthermore, we acknowledge that sonificating robust intrusion detection systems is challenging since they may carry large numbers of complex alarms and report on convoluted system status. Also, we acknowledge that a complete usability study will corroborate or refute our conjectures regarding the effectiveness of sound-assisted intrusion detection in general. Nevertheless, our goal at this stage is to be able to construct effective sonification systems that enable simplified intrusion detection and mitigation systems to convey meaningful alarms through diverse sensory channels.

Acknowledgements. We thank anonymous reviewers for their valuable comments on earlier versions of this paper. The first and second authors thank the support of the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

1. Barra, M., Cillo, T., De Santis, A., Petrillo, U.F., Negro, A., Scarano, V.: Personal webmelody: Customized sonification of web servers. In: ICAD. Proceedings of the International Conference on Auditory Display, Espoo, Finland (July 29 – August 1, 2001)
2. Blattner, M.M., Glinert, E.P.: Multimodal integration. IEEE Multimedia 3(4) (1996)
3. Burdea, G.C., Coiffet, P.: Virtual Reality Technology, 2nd edn. Wiley-IEEE Press (2003)
4. Crosby, S., Wallach, D.: Denial of service via algorithmic complexity attacks. In: Proceedings of the 12th USENIX Security Symposium, Washington, DC (2003)
5. Fyodor: The art of port scanning. Phrack Magazine, 7(51) (1997), [Accessed: March 6, 2003], `http://www.phrack.org`
6. García-Ruiz, M., Vargas Martin, M., Green, M.: Towards a multimodal human-computer interface to analyze intrusion detection in computer networks. In: First Human-Computer Interaction Workshop (MexIHC), Puebla, Mexico (2006)
7. García-Ruiz, M., Vargas Martin, M., Kapralos, B.: Towards multimodal interfaces for intrusion detection. In: Proceedings of the 122nd Convention of the Audio Engineering Society, Vienna, Austria (May 5–8, 2007)
8. Gilfix, M., Couch, A.: Peep (the network auralizer): Monitoring your network with sound. In: LISA XIV. Proceedings of 14th System Administration Conference, New Orleans, USA (December 3–8, 2000)
9. Goodrich, M.T., Sirivianos, M., Solis, J., Tsudik, G., Uzun, E.: Loud and clear: Human verifiable authentication based on audio. In: IEEE ICDCS (2006)

10. Gopinath, M.C.: Auralization of intrusion detection systems using Jlisten. Master's thesis, Birla Institute of Technology and Science, India (2004)
11. Heyes, D.A.: The sonic pathfinder: A new electronic travel aid. Journal of Visual Impairment and Blindness 77, 200–202 (1984)
12. Hofmann, A., Horeis, T., Sick, B.: Feature selection for intrusion detection: An evolutionary approach. In: IJCNN. Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks, Budapest, Hungary, vol. 2 (2004)
13. Jung, J., Paxson, V., Berger, A.W., Balakrishnan, H.: Fast portscan detection using sequential hypothesis testing. In: Proceedings of the 2004 IEEE Symposium on Security & Privacy, Oakland, USA (May 2004)
14. Kim, H.-A., Karp, B.: Autograph: Toward automated, distributed worm signature detection. In: Proceedings of 13th USENIX Security Symposium, San Diego, USA(August 9–13, 2004)
15. Kramer, G. (ed.): Auditory display: Sonification, audification, and auditory interfaces. Santa Fe Institute Studies in the Sciences of Complexity, Proc. Vol. XVIII. Addison-Wesley, Reading, MA (1994)
16. Neuhoff, J.G., Kramer, G., Wayand, J.: Pitch and loudness interact in auditory displays: Can the data get lost in the map? Journal of Experimental Psychology: Applied 8(1), 17–25 (2002)
17. Newsome, J., Karp, B., Song, D.: Polygraph: Automatically generating signatures for polymorphic worms. In: Proceedings of the 2005 IEEE Symposium on Security and Privacy, Oakland, USA (2005)
18. Obrenovic, Z., Starcevic, D., Jovanov, E.: Multimodal presentation of biomedical data. Wiley Encyclopedia of Biomedical Engineering (2006)
19. Onut, I.V., Zhu, B., Ghorbani, A.: A novel visualization technique for network anomaly detection. In: Proceedings of the 2nd Annual Conference on Privacy, Security and Trust, Fredericton, Canada (2004)
20. Oviatt, S., Cohen, P.: Multimodal interfaces that process what comes naturally. Communications of the ACM 43(3), 45–53 (2000)
21. Papadopoulos, C., Kyriakakis, C., Sawchuk, A., He, X.: Cyberseer: 3D audio-visual immersion for network security and management. In: Proceedings of the, ACM Workshop on Visualization and Data Mining For Computer Security, pp. 90–98, Washington DC, USA (October 29, 2004)
22. Park, K., Lee, H.: On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In: SIGCOMM 2001. Proceedings of the Special Interest Group on Data Communication, San Diego, USA (2001)
23. Qi, L., Vargas Martin, M.: IDS sonification (2007), `http://www.hrl.uoit.ca/~mvargas/IDS_sonification/SoundRecording.zip`
24. Qi, L., Zandi, M., Vargas Martin, M.: A network mitigation system against denial of service: A Linux-based prototype. In: EuroIMSA. Proceedings of IASTED Internet and Multimedia Systems and Applications, Chamonix, France (March 14–16, 2007)
25. Singh, S., Estan, C., Varghese, G., Savage, S.: The EarlyBird system for real-time detection of unknown worms. Technical Report CS2003-0761, University of California, San Diego, San Diego, USA (2003)
26. Staniford, S., Paxon, V., Weaver, N.: How to 0wn the Internet in your spare time. In: Proceedings of the 11th USENIX Security Symposium, San Francisco, USA (August 5–9, 2002)
27. Twycross, J., Williamson, M.M.: Implementing and testing a virus throttle. In: Proceedings of the 12th USENIX Security Symposium, Washington, USA (August 4–8, 2003)

28. Valdes, V., Fong, M.: Scalable visualization of propagating Internet phenomena. In: Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security, Washington DC (2004)
29. 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 5(3), 186–199 (2006)
30. Varner, P.E., Knight, J.C.: Security monitoring, visualization, and system survivability. In: IEEE/SEI. Information Survivability Workshop (ISW) (2001)
31. Venkataraman, S., Song, D., Gibbons, P., Blum, A.: New streaming algorithms for fast detection of superspreaders. In: Proceedings of the Network and Distributed System Security Symposium, San Diego, USA (2005)
32. Wang, K., Stolfo, S.J.: Anomalous payload-based network intrusion detection. In: Proceedings of the Seventh International Symposium on Recent Advances in Intrusion Detection, Sophia Antipolis, France (September 15–17, 2004)