



Audio Engineering Society Convention Paper

Presented at the 122nd Convention
2007 May 5–8 Vienna, Austria

The papers at this Convention have been selected on the basis of a submitted abstract and extended precis that have been peer reviewed by at least two qualified anonymous reviewers. This convention paper has been reproduced from the author's advance manuscript, without editing, corrections, or consideration by the Review Board. The AES takes no responsibility for the contents. Additional papers may be obtained by sending request and remittance to Audio Engineering Society, 60 East 42nd Street, New York, New York 10165-2520, USA; also see www.aes.org. All rights reserved. Reproduction of this paper, or any portion thereof, is not permitted without direct permission from the Journal of the Audio Engineering Society.

Towards Multimodal Interfaces for Intrusion Detection

Miguel Á. García-Ruiz¹, Miguel Argas Martin², and Bill Kapralos²

¹*School of Telematics, University of Colima. Colima, Mexico.*

²*University of Ontario Institute of Technology. Oshawa, Canada.*

Correspondence should be addressed to Miguel Á. García-Ruiz (mgarcia@uocol.mx)

ABSTRACT

Network intrusion detection has generally been dealt with using sophisticated software and statistical analysis tools. However, occasionally network intrusion detection must be performed manually by administrators, either by detecting the intruders in real-time or by revising network logs, making this a tedious and time-consuming labor. 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. We propose a multimodal human-computer interface to analyze malicious attacks during forensic examination of network logs. We describe a sonification prototype which generates different sounds according to a number of well-known network attacks.

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 can take a considerable amount of time to decide on a course of action when disconnecting or shutting down services are not viable solutions [43].

Several proactive and reactive defense approaches have been proposed. Some of these are signature and anomaly-based, while some of them use self-learning techniques, ranging from probabilistic analysis [48] to neural networks [22]. The reaction techniques can vary from raising an alarm or delaying traffic to complex auto-configurable mechanisms [41] or automatic generation of patches [33]. Typical IDSs rely on the presence of common attacks characteristics such as performing “many” similar actions in a “short” period of time [46], spoofing IP addresses [39], attempting connections to or from non-existing hosts or services [44], etc. Intrusion attacks are becoming clever in the ability to hide or attenuate any identifiable characteristic by protecting themselves against reverse engineering, implementing polymorphic techniques [11], or by propagating to a pre-defined set of hosts taken from a pre-computed hit-list [14].

A number of IDSs have been proposed (e.g., [24, 26, 49]), and some of them have become commercially available products [41]). 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 an IDS is yet to exist. Therefore analyzing IDS logs is a challenging task due to the large amount of entries representing false positives or false negatives [46].

In this paper we present new paradigms for intrusion detection assisted by multimodal interfaces (i.e., visual, auditive, gustatory, olfactory, and tactile). In addition, a prototype sonification-based network IDS system is proposed.

The following paper is organized as follows. Section 2 presents a number of proposed interfaces for intrusion detection. An overview of the proposed intrusion detection system in addition to preliminary results are presented in Section 3. Finally, concluding remarks and plans for future research are presented in Section 4.

2. RELATED WORK

Valdes and Fong [45] 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. The authors indicate that appropriate entropy analysis may enable this technique for early detection of malicious traffic (see also [36]).

With the huge amount of network information that flows in a typical organization or institution currently, it is difficult to cope with traffic analysis using visualization alone, almost certainly leading to “information overload” given that one sense (e.g., vision) is used to analyze that information.

In terms of human-computer interaction (HCI), network intrusion detection (NID) analysis has been carried out using visual, auditory or haptic information channels, where most of the studies have been done with two modalities at the same time. Although visual, auditory, and haptic channels have been studied and also used separately for intrusion detection, little is known about how to best combine the sensory channels. Furthermore, few, if any at all research efforts have examined the use of the sense of taste and smell for NID. A multimodal interface consists of the integration of multiple human sensory modalities in a computer interface that allows the human and the computer to exchange information, that is, to interact [5, 38]. Multimodal interfaces involve human input modalities (gaze, head movements, gestures, speech, etc.) and computer output modalities (primarily visual, auditory, and tactile display of information) that need to be adequately integrated to have a useful application. In multimodal interfaces, each modality can reinforce, supplement or complement each other, with the goal of alleviating cognitive load and allowing extra information channels [35].

2.1. Visualization and Intrusion Detection

Visual analysis of recorded data in network logs to identify intrusion detection has been extensively researched and applied using visual cues such as color coding, position, shape, size, motion, information clustering, in addition to 3D graphical representations, 2D graphs, and histograms (see [10, 20]). Although visualization can be very useful for discriminating data patterns, identifying regions of interest, and focusing the user’s attention, the majority of research pertaining to information and scientific visualization for NID is concerned with the drawbacks of visual cluttering and occlusion. Axelssons [2] work

focuses on using visualization to constantly monitor the network traffic by representing data from network logs using visualizations of trellis plot of parallel coordinates. His method has been successfully tested as a tool for network analysts to detect patterns of common worm types just with small logs in the range of hundreds of recorded accesses. Abdullah *et al.* [1] used stacked histograms to represent an overview of ports activity (packet counts in each port) in a given period of time for real-time analysis, along with time, port number, and graph scaling techniques to “drill down” the data visualization. The authors argue that this can be useful to shorten the time to carry out computer forensics after a malicious attack has been made, particularly to find patterns or trends of the attacks, like the “fingerprint” of the well known Sasser worm.

2.2. Tactile Interfaces and Intrusion Detection

Haptic interfaces are relatively less explored than visual interfaces. However, they can convey useful feedback to the user by representing information into variations of kinesthetic force or amounts of tactile parameters, such as vibration, temperature, pressure, texture, and viscosity. Haptic interfaces can be effective for sensory substitution and to complement the visual channel, and in the perception of sudden and very small changes in various tactile parameters including vibration [8]. One of the problems associated with haptic-based rendering in computer hardware is the relatively lack of good realism in actual interfaces, and under continuous tactile stimuli the tactile human sense adapts and tends to ignore or decrease its attention to the stimuli [40]. Nyarko *et al.* [34] investigated the use of haptics for analyzing NIDs. They mapped modeling of physics-based forces (e.g., electric fields, viscosity, and gravitational forces) onto intrusion detection characteristics such as attack type (previously arranged as numbers), attack severity, frequency, time and system IP. With this system, it is possible for the user to select the mappings. An experimental user study was conducted to test the developed system. A haptic device that can render 6DOF (six-degrees-of-freedom) kinesthetic forces and vibrations was used. Results demonstrated that, although there was a slight improvement with respect to the speed in the recognition of intrusion detection, significant improvements were observed with in detection accuracy.

2.3. Auditory Interfaces and Intrusion Detection

As with haptic interfaces, very little research has investigated the application of sound interfaces for NID.

Auditory display is the use of non-speech sound to present information [27]. Auditory display is currently employed in a variety of complex environments including computers, medical workstations, aircraft cockpits, and control centers in nuclear reactors [32]. 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” [32]. 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 [27].

Sound can be very effective in human-computer interaction for mapping complex information and discriminating data patterns, for carrying out situational awareness and to represent alarms as long as sound is correctly designed and adapted to the computer interface [27]. However, 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 sound is played. An alternative is to have the analyst wear headphones, especially those who are closed-cup to cover the ears and thus avoid disturbing others nearby. Barra *et al.* [3] and Gilfix and Couch [19] 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 NID analysis. Varner and Knight [47] proposed an audio/visual and agent-based system for monitoring the network in real time to identify malicious attacks. Gopinath [21] carried out a study where data from network logs was sonified to signal malicious attacks by identifying false positives and denial of service.

2.4. Olfactory and Gustatory Interfaces for Intrusion Detection

Research regarding HCI for intrusion detection has primarily focused on visual, auditory and haptic information while olfactory and gustatory interfaces have been primarily ignored. In this section a brief

overview of the use olfactory and gustatory modalities is provided. Recent developments (e.g., Dinh *et al.* [13]; Nakaizumi *et al.* [31]) demonstrate that currently it is technologically feasible and effective to produce and incorporate various smells into computer interfaces, and particularly into multimodal interfaces such as virtual reality environments. Bodnar, Corbett and Nekrasovski [6] conducted an experiment that compared the efficiency and disruptiveness of visual, auditory, and olfactory information that was delivered by a multimodal messaging notification system. They observed that the olfactory modality was not as efficient as the visual or auditory modalities for delivering notifications. They also observed that delivering information via the olfactory modality was the least disruptive. The fact that olfactory information is the least disruptive can be taken advantage of. For example, consider the situation where a network analyst is concentrating on a particular task and does not wish to be distracted by unimportant intrusion attacks. In such a situation, specific odors can be generated “in the background” and could serve as warning alerts. In other words, “olfactory icons” (scents that can be used to convey information at the computer interface [25]), can be used to notify an administrator about intrusion attacks.

The development of gustatory interfaces is very much in its infancy. Haptic and multimodal devices have been developed to simulate biting (Iwata, *et al.* [23]), but there are no reported developments on flavor delivery for representing meaningful information. Furthermore, to our knowledge, there are no reported developments in the literature to date regarding network intrusion detection using olfactory or gustatory interfaces. Distinctive smells or odors may be used to represent information from logs or monitoring network ports in real time to perform intrusion detection, ideally working in conjunction with other sensory channels to supplement, reinforce, or complement them to alleviate sensory overload and to minimize attention disruption. Perhaps a “stinky” odor or a disgusting flavor could represent an alarm mapped to an attack to the network, complementing visualization of particular characteristics of that attack on a computer screen.

Table 1 summarizes what we consider some putative strengths and weaknesses of each modality used

in a computer interface, in the context of network intrusion detection.

3. PROPOSED SONIFICATION METHOD

To date, most of the research on human-computer interfaces to support NID has been focused on bimodal applications to convey NID information, say visual and sound, or haptic and visual, but there is a lack of studies about the integration of those modalities in the domain of NID. In addition, very little research has been carried out about three or more sensory channels at the computer interface for the analysis of intrusion detection. It is necessary to find out which sensory combination works best in NID systems. 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 see what has been already computed and filtered out about network traffic and network logs. Multimodal interfaces can augment the capacity of the human analyst to cope with large amounts of information contained in network logs in search of malicious attacks.

Our approach is to study the benefits of a proposed multimodal human-computer interface (using three or more sensory channels) to analyze malicious attacks during forensic examination of network logs (this system was first proposed in [16]), since this task is time consuming and tedious when administrators do it.

One way of applying multimodality for intrusion detection is to integrate sensory channels in a virtual reality (VR) environment, since it is multimodal by definition. Virtual reality can be defined as “a high end computer interface that involves real time simulation and interaction through multiple sensorial channels” [9].

3.1. Sonification Prototypes

We are currently analyzing the technical aspects of the types of sounds and sound delivery techniques that are most effective for sonification of network logs. We are exploring the use of stereophony, pitch, and timbre to determine whether these parameters are effective for communicating the magnitude of network attacks and to identify their patterns. To further test our ideas regarding the sonification of network logs, we generated two sonification prototypes using auditory icons (sound effects of animals)

Sensory modality	Putative benefits	Putative limitations
Visual	<ul style="list-style-type: none"> -Color and graphic cues help discriminate information and identify attacks. -Visual information is persistent. -Useful for finding information patterns of worms and attacked IP addresses. -Visual interfaces are relatively easy to develop. -Multiple views of information (i.e. scaling, 3D) can be useful for analyzing large network logs. 	<ul style="list-style-type: none"> -Partially blind and colorblind network analysts may experience problems. -Visual cluttering and occlusion can happen. -Rapid and flashing displays may trigger epileptic seizures to susceptible analysts. -Difficult to monitor since eyes must be constantly directed to the visualization.
Auditory	<ul style="list-style-type: none"> -Useful for driving attention on particular tasks of NIDs (audible alarms). -Useful for finding information patterns of worms and attacked IP addresses. -A particular sound may be identified among many (“cocktail party effect”) i.e. from a group of alarms. -Complementary visual/auditory information allows efficient sensory correlation. 	<ul style="list-style-type: none"> -Auditory information is temporal, heard for a limited time. -Sounds can be annoying if badly designed and played. -Not all people have “perfect pitch” (the cognitive ability to discern a particular tone among many).
Gustatory and Olfactory	<ul style="list-style-type: none"> -Can enhance the mood and reduce the stress of the analyst. -Can improve recall and attention. -Can improve retention of learned items or tasks. -Analysts do not need to change their attention to perceive gustatory or olfactory stimuli. 	<ul style="list-style-type: none"> -Mechanical production and dissemination of odors and flavors and be difficult to perform. -Some analysts may exhibit allergies or adverse reaction to some odors and flavors. -Odors and flavors can be persistent and difficult to eliminate rapidly. -Quantity of smell may be difficult to perceive.
Haptic	<ul style="list-style-type: none"> -Can be effective for sensory substitution and complement the visual channel. -It is possible to perceive sudden and very small changes in some tactile parameters (vibration). 	<ul style="list-style-type: none"> -Under continuous tactile stimuli, the tactile human sense adapts and tends to ignore or decrease its attention to that stimuli. -Relatively lack of good realism produced with current computer hardware.

Table 1: Putative benefits and limitations of each sensory modality for intrusion detection (adapted from García-Ruiz and Gutierrez-Pulido [17]).

and earcons (sounds of piano notes). Auditory icons are natural sound effects that represent actions or information at the computer interface [18]. Similarly, earcons are short musical sounds made of string, wind or percussion instruments, and also represent actions or information in interfaces [4]. We developed a program (written using the Tcl language [37]) that employs the Sox (Sound Exchange) program [42] (Windows versions) to generate the log sonifications. As an example, the U.S. Defense Advanced Research Projects Agency (DARPA) Intrusion Detection Evaluation Data Set was used [30] (despite known flaws in the DARPA data set [28], we are confident it will suffice for a preliminary analysis). This log was generated by a network intrusion detection system, and contains markers of five types of possible attacks. We used that log as it is, without modifications.

3.1.1. Prototype One

A .wav file with the log sonification and auditory icons was generated using our program. These are the mappings of auditory icons to the five types of attacks registered in the log:

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

3.1.2. Prototype Two

We generated a second sonification 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 to “guess”
- A 197Hz key note is mapped to “port-scan”
- A 263Hz key note is mapped to “rcp”
- A 525Hz key note is mapped to “rsh”
- A 1056Hz key note is mapped to “rlogin”

Each line of the log with no possible attack is mapped to a 0.125 second of silence. The mappings were assigned randomly. The sounds were output in stereo. In prototype one, the output to the left channel is a frog sound. The sound output to the right channel is a bird sound. In prototype two, the sound output to left channel is a 128Hz pure tone (note). The sound output to the right channel is a 1056Hz pure tone.

The duration of the auditory icons and earcons is one second. These particular sounds were chosen in order to allow the use of five distinguishable sounds in terms of their average frequency (pitch) and timbre. The auditory icons were obtained from a set of sound effects produced by the P.D.I., S.A. company from Spain. The piano sounds were obtained from the Media Lab, University of Applied Sciences [29]. Both of the sonification prototypes that are described here are freely available from [15]. Each animal and piano sound was edited following the audio earcon creation guidelines of Brewster, Wright and Edwards [7].

The sounds were tested informally by two of our project participants using a pair of closed-cup Maxell Studio Series HP-2000 headphones. They suggested that the piano notes were easier to identify because of their stereo position (panning), although auditory icons (the animal sounds) were useful to recall better their mappings to the attack types. Future usability studies will determine whether other types of headphones and surround-sound speaker systems are more effective in allowing for greater sound quality and potential spatial positioning.

We are currently developing other programs for generating the required sounds using MIDI files. In particular, the Csound program [12] is being explored to generate the sounds in MIDI format, especially to use the sound position in 3D feature, using its HRTF (Head-Related Transfer Function). The use of MIDI files certainly will increase the sound quality, since the downloaded files we used for the first prototype have some hiss in the background. We hypothesize that the sounds played in 3D will help discriminate the attack values mapped to those sounds, played along with 3D visualization of the attacks.

4. CONCLUSIONS AND FUTURE WORK

This paper has presented an overview of the application of multimodal technology to network intrusion detection (NID). The advantages and disadvantages of presenting NID information to an operator using various modalities including visual, auditory, haptic, and olfactory were presented. Particular emphasis was placed on the sonification of NID information and two prototype systems were presented. Multimodal interfaces can be useful and capitalize on each modality to support humans in the analysis of NID. In particular, they can be used to notify the network analyst of NID acts in real-time, providing them with valuable feedback in order to allow them to carry out computer forensics when a system has already been attacked, and to allow them to devise and analyze system recovery solutions. It remains to be seen whether fully-fledged multimodal interfaces are useful, in terms of technical feasibility and cognitive advantages, to facilitate support of network intrusion detection in very large data sets, and especially to detect attacks in time and to identify them correctly in computer forensics and systems recovery.

Future work includes the application of the proposed sonification-based intrusion detection system to a computer server with bio-molecular information (containing 3D models of organic molecules and genetic sequences), working as a test bed, that is being used for research and for educational applications at the University of Colima, Mexico. Experiments will be performed to test the effectiveness of the proposed system. Furthermore, we will investigate allowing the users of the system to choose the particular sound effects used in the mappings in order to allow for simple identification on a personal level.

ACKNOWLEDGEMENTS

Miguel Argas Martin acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC).

5. REFERENCES

- [1] K. Abdullah, C. Lee, G. Conti, and J.A. Copeland. Visualizing network data for intrusion detection. In *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY, 2005.
- [2] S. Axelsson. Visualisation for intrusion detection - hooking the worm. In *Eighth European Symposium on Research in Computer Security (ESORICS)*, Lecture Notes in Computer Science (LNCS). Springer, 2003.
- [3] M. Barra, T. Cillo, A. De Santis, U.F. Petrillo, A. Negro, and V. Scarano. Personal webmelody: Customized sonification of web servers. In *Proceedings of the International Conference on Auditory Display (ICAD)*, Espoo, Finland, July 29 – August 1 2001.
- [4] D. Blattner, A. Sumikawa, and R.M. Greenberg. Earcons and icons: Their structure and common design principles. *Human Computer Interaction*, 4: 11–44, 1989.
- [5] M.M. Blattner and E.P. Glinert. Multimodal integration. *IEEE Multimedia*, 3(4), 1996.
- [6] A. Bodnar, R. Corbett, and D. Nekrasovski. AROMA: Ambient awareness through olfaction in a messaging application. In *Proceedings of ICM104, ACM*, 2004.
- [7] S.A. Brewster, P.C. Wright, and A.D.N. Edwards. Experimentally derived guidelines for the creation of earcons. In *Adjunct Proceedings of HCI'95*, Huddersfield, UK, 1995.
- [8] G.C. Burdea. *Force and touch feedback for virtual reality*. John Wiley & Sons, New York, 1996.
- [9] G.C. Burdea and P. Coiffet. *Virtual Reality Technology (2nd Ed.)*. Wiley-IEEE Press, 2003.
- [10] G. Conti, M. Ahamad, and J. Stasko. Attacking information visualization system usability overloading and deceiving the human. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS'05)*, volume 93, pages 89–100, Pittsburgh, USA, July 6–8 2005. ACM Press.
- [11] S. Crosby and D. Wallach. Denial of service via algorithmic complexity attacks. In *Proceedings of the 12th USENIX Security Symposium*, Washington, DC, 2003.
- [12] cSounds. cSounds Official Web Page, 2006. URL: <http://www.csounds.com>.
- [13] H.Q. Dinh, N. Walker, C. Song, A. Kobayashi, and L.F. Hodges. Evaluating the importance of multi-sensory input on memory and the sense of presence in virtual environments. In *Proceedings of the IEEE Virtual Reality*, pages 22–228, 1999.
- [14] Fyodor. The art of port scanning. *Phrack Magazine*, 7(51), 1997. URL: <http://www.phrack.org>.

- [15] M. Garcia-Ruiz. Sonification of security logs, 2006. URL: <http://docente.uco1.mx/~mgarcia/Sonificatedlog.htm>.
- [16] M. Garcia-Ruiz, M. Vargas Martin, and M. Green. Towards a multimodal human-computer interface to analyze intrusion detection in computer networks. In *First Human-Computer Interaction Workshop (MexIHC)*, Puebla, Mexico, 2006.
- [17] M.A. Garcia-Ruiz and J.R. Gutierrez-Pulido. An overview of auditory display to assist comprehension of molecular information. *Interacting with Computers*, 18(4): 853–868, 2006.
- [18] W.W. Gaver. Auditory icons, using sound in computer interfaces. *Human Computer Interaction*, 2: 167–177, 1986.
- [19] M. Gilfix and A. Couch. Peep (the network auralizer): Monitoring your network with sound. In *Proceedings of 14th System Administration Conference (LISA XIV)*, New Orleans, USA, December 3–8 2000.
- [20] J.R. Goodall, A.A. Ozok, W.G. Lutters, P. Rheingans, and A. Komlodi. A user-centered approach to visualizing network traffic for intrusion detection. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1403–1406, 2005.
- [21] M.C. Gopinath. Auralization of intrusion detection systems using Jlisten. Master's thesis, Birla Institute of Technology and Science, India, 2004.
- [22] A. Hofmann, T. Horeis, and B. Sick. Feature selection for intrusion detection: An evolutionary approach. In *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN)*, volume 2, pages 1563–1568, Budapest, Hungary, 2004.
- [23] H. Iwata, H. Yano, T. Uemura, and T. Moriya. Food simulator: A haptic interface for biting. In *IEEE Virtual Reality Conference (VR'04)*, page 51, 2004.
- [24] J. Jung, V. Paxson, A.W. Berger, and H. Balakrishnan. Fast portscan detection using sequential hypothesis testing. In *Proceedings of the 2004 IEEE Symposium on Security & Privacy*, Oakland, USA, May 2004.
- [25] J. Kaye. Making scents: Aromatic output for HCI. *Interactions*, January-February 2004.
- [26] H.-A Kim and B. Karp. Autograph: Toward automated, distributed worm signature detection. In *Proceedings of 13th USENIX Security Symposium*, San Diego, USA, August 9–13 2004.
- [27] G. Kramer, editor. *Auditory display: Sonification, audification, and auditory interfaces*. Santa Fe Institute Studies in the Sciences of Complexity, Proc. Vol. XVIII. Reading, MA: Addison-Wesley, 1994.
- [28] J. McHugh. Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. *ACM Transactions on Information System Security (TISSEC)*, 3(4):262–294, 2000.
- [29] Media Lab. Index of multimedia files, 2006. URL: <http://medialab.it.fht-esslingen.de/ftp/multimedia-files/sound/Instrumente/Verschiedene/>.
- [30] MIT Lincoln Laboratory. DARPA intrusion detection evaluation: Data sets, 1999. URL: http://www.ll.mit.edu/IST/ideval/data/data_index.html.
- [31] F. Nakaizumi, Y. Yanagida, H. Noma, and K. Hosaka. Spotscents: A novel method of natural scent delivery using multiple scent projectors. In *Proceedings of IEEE Virtual Reality*, Alexandria, USA, 2006.
- [32] J. G. Neuhoff, G. Kramer, and J. Wayand. 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.
- [33] J. Newsome, B. Karp, and D. Song. Polygraph: Automatically generating signatures for polymorphic worms. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, Oakland, USA, 2005.
- [34] K. Nyarko, T. Capers, C. Scott, and K. Ladeji-Osias. Network intrusion visualization with NIVA, an intrusion detection visual analyzer with haptic integration. In *Proceedings of the 10th IEEE Symposium on Haptic Interfaces For Virtual Environments & Teleoperator Systems (HAPTICS.02)*, 2002.
- [35] Z. Obrenovic, D. Starcevic, and E. Jovanov. *Multimodal presentation of biomedical data*. Wiley Encyclopedia of Biomedical Engineering, 2006.
- [36] I.V. Onut, B. Zhu, and A. Ghorbani. A novel visualization technique for network anomaly detection. In *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*, Fredericton, Canada, 2004.
- [37] J. Ousterhout. *Tcl and the Tk Toolkit*. Addison-Wesley, 1994.
- [38] S. Oviatt and P. Cohen. Multimodal interfaces that process what comes naturally. *Communications of the ACM*, 43(3):45–53, 2000.

- [39] K. Park and H. Lee. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In *Proceedings of the Special Interest Group on Data Communication (SIGCOMM01)*, San Diego, USA, 2001.
- [40] H.R. Schiffman. The skin, body and chemical senses. *Sensation and Perception*, 1995.
- [41] S. Singh, C. Estan, G. Varghese, and S. Savage. The EarlyBird system for real-time detection of unknown worms. Technical Report CS2003-0761, University of California, San Diego, San Diego, USA, 2003.
- [42] SourceForge. Sox: Sound Exchange, 2006. URL: <http://sox.sourceforge.net/>.
- [43] S. Staniford, V. Paxson, and N. Weaver. How to Own the Internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, San Francisco, USA, August 5–9 2002.
- [44] J. Twycross and M.M. Williamson. Implementing and testing a virus throttle. In *Proceedings of the 12th USENIX Security Symposium*, Washington, USA, August 4–8 2003.
- [45] A. Valdes and M. Fong. Scalable visualization of propagating Internet phenomena. In *Proceedings of the ACM Workshop on Visualization and Data Mining for Computer Security*, Washington DC, 2004.
- [46] P.C. van Oorschot, J.-M. Robert, and M. Vargas Martin. A monitoring system for detecting repeated packets with applications to computer worms. *International Journal of Information Security*, 5(3):186–199, July 2006.
- [47] P.E. Varner and J.C. Knight. Security monitoring, visualization, and system survivability. In *IEEE/SEI. Information Survivability Workshop (ISW)*, 2001.
- [48] S. Venkataraman, D. Song, P. Gibbons, and A. Blum. New streaming algorithms for fast detection of superspreaders. In *Proceedings of the Network and Distributed System Security Symposium (NDSS05)*, San Diego, USA, 2005.
- [49] K. Wang and S.J. Stolfo. Anomalous payload-based network intrusion detection. In *Proceedings of the Seventh International Symposium on Recent Advances in Intrusion Detection (RAID 2004)*, Sophia Antipolis, France, September 15–17 2004.