Server Sounds and Network Noises

Tobias Hildebrandt
SBA Research, Vienna, Austria
tobias.hildebrandt@univie.ac.at

Stefanie Rinderle-Ma
Faculty of Computer Science, University of Vienna, Austria
stefanie.rinderle-ma@univie.ac.at

***Abstract*—For server and network administrators, it is a challenge to keep an overview of their systems to detect potential intrusions and security risks in real-time as well as in retrospect. Most security tools leverage our inherent ability for pattern detection by visualizing different types of security data. Several studies suggest that complementing visualization with sonification (the presentation of data using sound) can alleviate some of the challenges of visual monitoring (such as the need for constant visual focus). This paper therefore provides an overview of the current state of research regarding auditory-based and multi-modal tools in computer security. Most existing research in this area is geared towards supporting users in real-time network and server monitoring, while there are only few approaches that are designed for retrospective data analysis. There exist several sonification-based tools in a mature state, but their effectiveness has hardly been tested in formal user and usability studies. Such studies are however needed to provide a solid basis for deciding which type of sonification is most suitable for which kind of scenarios and how to best combine the two modalities, visualization and sonification, to support users in their daily routines.**

I. Introduction

The amount of network traffic is constantly increasing, which poses a challenge for network and server administrators in terms of keeping an overview of their systems and identifying potential intrusions. There exists a substantial amount of research that deals with systems that apply visualization techniques for real-time monitoring of security-relevant aspects, as well as for retrospective analysis of security-related data, dedicated to support users in their tasks. This research makes use of the fact that humans excel at recognizing novel patterns in complex data, a capability that computer security support tools ideally combine with the ability of software to process vast amounts of data [1].

There exist different approaches for different levels of data granularity, such as systems that visualize packet traces (raw, low-level events), network flows (aggregated data) or alerts [1]. Systems that rely solely on visual means to convey data, as useful and beneficial as they are in many situations, have also certain drawbacks: operators have to dedicate their full attention to them, as they might miss potential intrusions in case they turn away from their screens or shift their concentration to something else. This makes it impossible for them to stay informed about network activities at all times and at the same time work on other tasks, which can be a challenge for many organizations. Furthermore, the number of visual dimensions and properties data can be mapped onto is limited.

Therefore, we suggest to combine existing visualization techniques to convey data with methods from the area of sonification in order to tackle some of the mentioned drawbacks of current monitoring and analysis of security data. Sonification is "'the use of non-speech audio to convey information" [2], and it has a few characteristics that make it especially suitable for monitoring and analysis of time-based data [3]:

- Sonifications do not need a visual focus and can be processed passively, allowing users to work on another task while at the same time getting informed about security-relevant data and events.
- We are very sensitive to even small changes in rhythms and sequences because sound is inherently a temporal medium, while visualization is primarily a spatial medium. Therefore sonification is very suitable to convey information that changes over time, such as network events or a changing system status. Thus, sonification does not only suggest itself to real-time monitoring, but also to the retrospective analysis of time-based data.
- Sound is very good at attracting attention, therefore alarms and alerts often base on sound instead of visuals.

Due to these characteristics, several researchers (e.g. [4]) argue that audio is more suitable than video in cases of peripheral monitoring activities - activities in which the monitoring is performed as a background task, while the primary focus is on another task.

This paper therefore analyzes the existing research that applies sonification and multi-modal techniques (combining visualization and sonification) to support users in computer security-related tasks. Approaches that base on purely visual means are however not in the focus of this paper, as there exist already a number of current and comprehensive surveys of this research area (which will be mentioned in the next chapter).

II. Security Visualization

There has been a long history of research in applying visualization techniques to support users in security monitoring and analysis. But not only researchers, also practitioners in companies and organizations have been using visualization-based tools for quite some time, e.g. for monitoring network attacks [5].

There have been several recent overviews of visualization-based security tools and their functionalities (e.g. [6] or [5]). Regular conferences - such as VizSec (Visualization for Cyber Security) - advance the research in this field. Shiravi et al. [6] classify security visualizations according to the data types that they base on. The authors distinguish between network traces, security events, network activity context, user/asset context,

network events and application logs. The authors also provide a comprehensive overview of the current research in visualization for security, listing approaches e.g. by application domains such as host/server monitoring, internal/external monitoring, port activity, attack patterns or routing behavior.

According to Goodall [1], the main security-related tasks with which visualization can help users, are:

- detecting anomalous activity
- discovering trends and patterns
- correlating intrusion detection events
- computer network defense training
- offensive information operations
- seeing worm propagation or botnet activity
- forensic analysis
- understanding the makeup of malware or viruses
- feature selection and rule generation
- communicating the operation of security algorithms

We argue, that in most or all of those areas, supplementing visualizations with sonification techniques can further support human operators. Due to the aforementioned characteristics, sonification has successfully been researched in different areas in which it is crucial to monitor developments in real-time, such as business process monitoring (e.g. [7]), industrial production monitoring (e.g. [8]), but also web server and network monitoring. For a recent overview of sonification in process monitoring, please refer to [3].

III. Auditory Displays and Security

This section tries to give a more or less comprehensive overview of the research in auditory and multi-modal solutions in a computer security context. There is a wide array of different techniques and methods to convey data aurally, which are designed to represent different types of data. There exist basic techniques such as auditory icons or earcons, which are typically used for auditory cues or alerts. On the other end of the spectrum there are more complex types, e.g. based on continuous sonification, where different qualitative and quantitative data dimensions are mapped to various acoustic properties, such as volume or pitch, using techniques such as parameter mapping. An overview of the different types and techniques can be found in [9]. The mentioned existing overview of the usage of sonification in process monitoring [3] covers also the areas network and server monitoring, however not comprehensively.

A. Method

The following literature survey bases on a Google Scholar search performed on 4 March 2015. The keywords ”sonification” and ”security” were used in all searches, which were combined alternately with one of the keywords ”monitoring” and ”analysis”. Papers that did not fit the topic were excluded. Examples are e.g. papers in which the term ”sonification” is only mentioned in the related works section and that do not feature an approach or system that actually incorporates sonification techniques, or papers that only mention ”security” as one of several application domains in which a generic framework or sonification technique can be applied, without specifying a computer security-related use case. In cases where several papers by the same authors describe the same approach (e.g. in more detail), only the most recent paper has been included.

B. Literature

There exists a variety of research that employs sound (often in parallel to visuals) in a security context. This existing research can be categorized along different axes: in terms of the applied modalities, there are approaches that base solely on sonification, and such that are multi-modal, thus using both, visualization and sonification. Further, the existing research aims to support users in different security-relevant tasks, such as real-time intrusion detection in networks, or the retrospective analysis of security-related data (e.g. web server log files). A third type of research deals with using sound as a means to improve security education. As a basis for the developed sonifications, different types of data are being used, ranging from unfiltered event data (such as individual web server requests), over filtered event data and aggregated state-based data (such as e.g. the traffic load of a server) to alert notifications. Of course, the existing research is in different stages of maturity, ranging from vague system proposals, over prototypes that can be used to conduct user studies, to systems that are already publicly available for download and in use.

C. Findings

Table I summarizes the different existing approaches. The two columns on the left state the reference of the paper as well as its year of publication. The field ”Scope” refers to the aforementioned distinguishing into approaches for real-time monitoring, retrospective analysis and training, while the field ”application” states their intended area of use, such as network monitoring. ”Granularity” describes which kind of data is sonified (e.g. alerts) and ”Modality” categorizes the publications into approaches that are ”standalone” sonifications and such that are combined with visualization into multi-modal systems. ”Status” describes the maturity of the respective research approach, e.g. concept. Finally, the field ”Study” states if a user study has been conducted or not.

In total, 26 papers have been found that matched the predefined criteria explained before, including publications that were found by investigating the references of already identified literature (backward snowballing). After removing publications by the same authors that describe the same system or concept, the 20 papers that are included in the aforementioned table remained. It is striking that out of those 20 publications, only three explicitly consider the retrospective analysis of historic data (see Fig. 1a).

Ballora et al. describe in [16] and [15] systems that sonify entries of web server log files, stating that their systems are designed to work in a real-time mode as well as for historic data analysis. In a later publication [14] the authors suggest a new system that bases not only on raw events but also on aggregated state-based data (e.g. current throughput/traffic rates), again stating that it is suitable for real-time monitoring

TABLE I: Auditory and multi-modal approaches in computer security.

Ref	Year	Scope	Application	Granularity	Modality	Status	Study
[10]	2015	Monitoring	Network	State-based data	Sonification	Concept	No
[11]	2014	Monitoring	Network	State-based data	Sonification	Prototype	No
[12]	2014	Monitoring	Network	Filtered events	Multi-modal	Prototype	No
[13]	2012	Monitoring	Network	State-based data	Sonification	Concept	No
[14]	2011	Monitoring&Data analysis	Network	Raw events, State-based data	Sonification	Prototype	No
[15]	2010	Monitoring&Data analysis	Web server	Raw events	Multi-modal	Prototype	No
[16]	2010	Monitoring&Data analysis	Web server	Raw events	Sonification	Prototype	No
[17]	2009	Monitoring	Network	Alerts	Multi-modal	Concept	No
[18]	2009	Monitoring	Network	State-based data	Sonification	Prototype	No
[19]	2007	Training	Network	Alerts	Sonification	Prototype	(Yes)
[20]	2007	Monitoring	Network	State-based data	Sonification	Prototype	No
[21]	2006	Monitoring	Network	Not specified	Multi-modal	Concept	No
[22]	2004	Monitoring	Network	State-based data	Multi-modal	Concept	No
[23]	2004	Monitoring	Network	Filtered events	Sonification	Prototype	Yes
[24]	2004	Monitoring	Network	State-based data	Multi-modal	Prototype	No
[25]	2003	Monitoring	Network	Filtered events, State-based data	Sonification	Prototype	No
[26]	2002	Monitoring	Network	Not specified	Multi-modal	Concept	No
[27]	2002	Monitoring	Network	Filtered events	Sonification	Prototype	(Yes)
[28]	2002	Monitoring	Web server	Filtered events, State-based data	Sonification	Tool	No
[29]	2000	Monitoring	Network	Raw events, State-based data	Sonification	Tool	No

as well as for retrospective analysis. Of course, many of the other systems technically support historic data analysis as well, as they often use log files as a basis. But, as they are not designed specifically with the use case of retrospective analysis in mind, there is a certain likelihood that they are not very suitable for this use case. This is because real-time monitoring is typically a peripheral monitoring task, meaning that it is done in parallel to other tasks, grabbing the users attention only when necessary. Of course, such a system should be designed very subtle and unobtrusive, in order to avoid fatigue when using it for a complete workday. Historic data analysis is on the other hand typically a direct monitoring task, meaning that it is performed only for a limited period of time and therefore with the users full attention. Such a system can thus be designed more obvious. Another factor is, that in order to be able to analyze a large amount of data in a short period of time (e.g. the server logs of the last 24 hours or even of a complete month), the sonification needs to be designed in a much more compressed and condensed manner than for real-time monitoring. While most systems aim at supporting potential users in their security-related tasks, Garcia-Ruiz et al. [19] propose the usage of sonification in order to teach network intrusion detection.

In terms of the application area, 17 of the 20 presented papers deal with network monitoring in general, typically with the aim of supporting users in detecting intrusions. 3 approaches more specifically aim at the goal of web server monitoring ([16], [15], [28]). The first two of those approaches ([16], [15]) are the only ones that solely present unfiltered event-data.

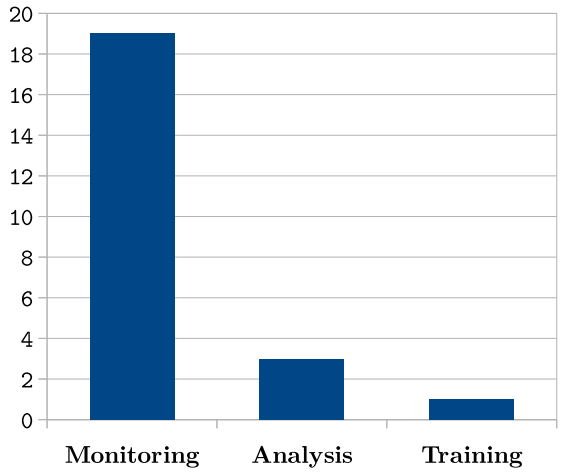
Most other approaches either base on filtered event data, e.g. by presenting only events that fit pre-defined criteria or auditory alerts, or on higher-level quantitative, state-based data. Vickers et al. [11] describe a system that sonifies the SOC (Self-organized Criticality) of a network. Brown and Ruiz [18] sonify the bit-rates and packet-rates of a delay queue, an approach shared with Qi et al. [20]. Ballora et al. sonify, in addition to raw events, the amount of network traffic [14]. The ”Peep”-system sonifies state-based data, such as the average server load or the number of users on a specific machine, as well as event data [29]. Giot et al. [13] propose to sonify various network-state information, such as e.g. packet sizes or port usage statistics. Papadopoulos [24] et al. propose a system that sonifies quantitative network traffic data, without mentioning the specifics of this proposed software. Fig. 1b summarizes these findings.

In terms of modality, 6 of the 20 publications feature multi-modal solutions that combine visual and auditory means. Looking at the integration between acoustic and visual conveyance, the existing literature covers the whole range of possibilities: Muoz-Arteaga [17] suggest to apply audio purely as a means to convey intrusions that have already been discovered by intrusion detection software, while visual means are then used to find out additional information.

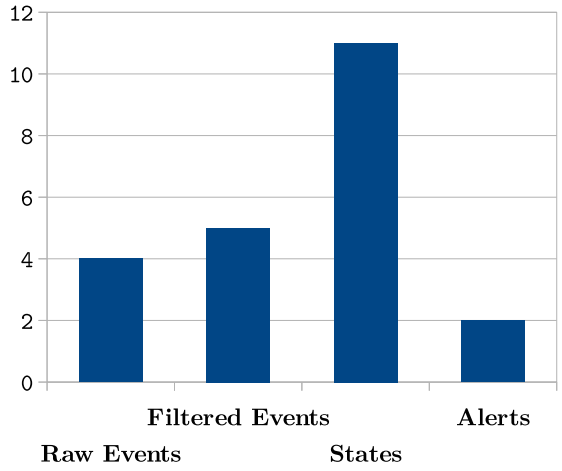
The opposite of this interplay of modalities is proposed by Varner et al. [22]. In this proposal, visualization is used to convey the status of network nodes, while the user could then select a specific node to hear a sonification that conveys additional details. A more integrated approach is described by Ballora et al. [15], where network information is at the same time conveyed aurally using a multi-channel sonification and visualized using a 3D visualization. Papadopoulos et al. [24] propose a system that combines 3D audio and 3D visuals in parallel to convey different network-related data. Garcia-Ruiz et al. [21] propose a system that combines 3D audio in conjunction with visualization to convey network attacks . The details of this proposed system are however not specified. The same holds true for a position paper [26] that proposes to use visual and auditory means without specifying details. Fig. 2a summarizes this aspect.

In terms of maturity, several of the presented research papers constitute research agendas or proposals for systems and prototypes that yet need to be developed. Most of the publications however describe already developed prototypes in several stages of maturity, while only two publications seem to base on ready-to-use tools that are publicly available ([28], [29]), as can be seen in Fig. 2b.

A characteristic that is very striking, is that even the mature systems have not or hardly been evaluated for usability (see

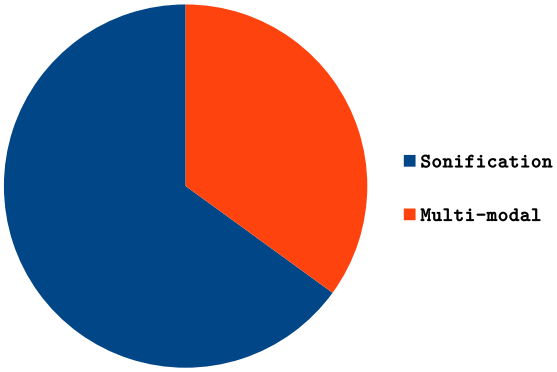


(a) Scope

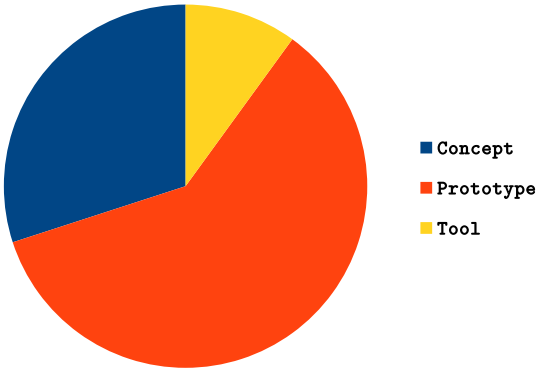


(b) Granularity

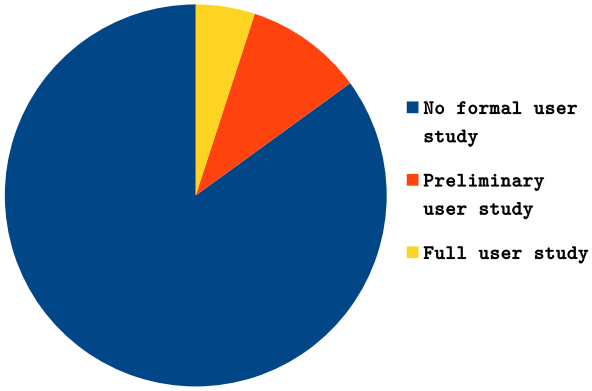
Fig. 1: Scope and Granularity.



(a) Modality



(b) Status



(c) Evaluation

Fig. 2: Modality, Status and Evaluation

Fig. 2c). In several papers, case studies describe functionality tests in a certain context, however mostly without involving potential users. Most papers mention no kind of testing at all, while a few publications include preliminary and informal testing. There seems to be only one publication in which a formal user evaluation is being described([23]). Garcia-Ruiz et al. [19] performed an informal, preliminary experiment with 29 subjects who filled out questionnaires after they were played different sonifications to find out their preferences and suggestions in terms of sound design. Kimoto et al. [27] mention a first tentative user study with 4 users. In this study users were played a sequence of sounds indicating traffic loads at different points in time, which users more or less successfully estimated based on the sonifications. However, the number of subjects is too low to provide generalizable results.

Both mentioned user studies did not include a comparison of the respective sonification with the status-quo in the respective area (typically visualization-based systems). Such a comparison has been performed in a study conducted by Gopinath [23] with 20 subjects. The author conducted different user studies, comparing sonification-based approaches with control groups that had to perform the same tasks without auditory support. The sonification groups performed the tasks (detection and identification of intrusions) significantly faster than the control groups. However, the control group had to perform the tasks by reading log files without having access to visualization-based tools, which may limit the generalizability of the results.

D. Recent Approaches

After conducting the literature search, three new systems have been presented that apply audio for computer security

purposes. In [30], a prototype that sonifies log files of streaming servers is presented. In its current state it is designed to allow for the analysis of historic log data, but will according to the authors be adapted for real-time monitoring in the future. It bases on a continuous sonification of aggregated server data, such as server load, as well as metadata on the content that is being handled by the server. The authors conducted a small case study with 5 participants, who were able to perform most of the provided tasks effectively. The NetSon system sonifies and visualizies network traffic in real time, with a specific focous on larger-scale organizations [31]. The system presents server load and aggregated metadata from random samples that are taken at a pre-defined sampling rate. No formal user studies have been conducted with the system as yet, however it is being used productively at Fraunhofer IIS, who provide a live web stream of their installation.[1] Furthermore, even though it has not been presented in a scientific publication yet, Microsofts' multi-modal system *Specimen Box* is worth mentioning. It allows for the detection and anlysis of botnet activity in real-time and in retrospect.[2]

E. Summary

In summary, there exists already a substantial body of research for the application of sonification in computer security in various forms of maturity, ranging from vague proposals to ready-to-use tools. It is clear from the survey, that the vast majority of research deals with systems for real-time monitoring, while historic data analysis seems not to be in the focus of attention. Furthermore, there seems to be a lack of formal user and usability testing. In terms of the granularity of the data that is sonified, there seems to be a trade-off between utilizing our potential for pattern recognition and risking a cognitive overload of the user. A system that sonifies all occurring events in real time would be very detailed and rich in information. On the one hand, if not properly designed, it can easily lead to an information overload and thus to annoyance and fatigue. On the other hand, such a fined grained data conveyance could enable users to detect patterns and possible intrusions very early, possibly even ones that an automated, rule-based system would not detect. In this case, intelligence would be transferred from the intrusion-detection software to the users' cognition and his/her inherent capability for pattern recognition. The other extreme would be a system that mainly bases on automated software and uses sound merely to inform the user that an intrusion has been detected or that a critical state has been reached. Such a system would apply sonification only as a means to convey alarms and alerts and therefore not utilize its full potential.

IV. Conclusion and Future Directions

As the amount of network traffic, administrators and operators have to monitor increases, obtaining an overview of the networks' and systems' status and detecting potential intrusions becomes a challenge. Therefore, many tools support users by leveraging our natural pattern recognition abilities with visualization techniques. However, as purely visual solutions have certain drawbacks (such as their need for direct attention), we suggest to research multi-modal solutions, combining visualization and sonification. This paper presented and analyzed different existing auditory and multi-modal approaches for security.

There is a broad foundation of research that covers different approaches for the monitoring of network intrusions and server status. However, these different approaches with their different data granularities, sonification techniques and integrations with visualization have hardly been tested with users. Therefore, it is yet unclear, which approach is best suitable for which kind of scenario and how effective the different systems are in reaching their goal to support users in their tasks. The state of research would be advanced if various kinds of user evaluations were performed, from quantitative experiments (e.g. using typical short tasks that operators have to perform) in a peripheral monitoring scenario, as e.g. suggested in [32], to qualitative case studies where the respective system is tested in realistic scenarios for long-term usability, such as in end-user companies and organizations. This evaluation is necessary to prove the potential of sonification in this area both to the scientific community and to practitioners.

Furthermore, there seems to be a lack of research that deals with retrospective data analysis. This is remarkable, given the fact that for other domains there is a huge pool of approaches that use sonification for retrospective data analysis. In the security context however, although there exist several approaches that base on log files and therefore technically would support a retrospective analysis, they are (with a few exceptions) not designed for the specificities of this task (such as the need to sonify large amounts of data in a short time frame). Furthermore, as retrospective analysis is typically a direct monitoring task (as opposed to real-time monitoring), different sonification techniques and interaction mechanisms are required than for direct monitoring. To maximize effectiveness, such systems would have to integrate visual and auditory means tightly, contain comprehensive data selection and filtering mechanisms as well as the possibility to control data compression and sonification playback speed.

Of the mentioned potential data sources for security visualizations ([6]), not all suggest themselves for sonification to the same extent. Due to its inherent time-based nature and our auditory cognition, sonification is especially suitable for data that changes over time. However, visualization is in general more adequate in conveying spatial information (e.g. network topology maps), as well as data that is not time-based (such as e.g. detailed information on different servers at a specific point in time). Thus, while network traces, security events, network events and application logs seem to suggest themselves for sonification, network activity context and user/asset context seem, in general, more suitable for visualization. Most of the data sources that are suitable for sonification have already been used for this purpose. An exception is the usage of sonification of application logs in a security context. Potential types of applications that could be of interest as data sources include database systems, workflow systems, or systems for enterprise resource planing (ERP) [6]. To our best knowledge, none of the three mentioned types of systems have so far been used as data sources for sonification in a security context. As most of the existing approaches described in this paper aim primarily at detecting intrusions from outside an organization, and thus

[1] http://www.iis.fraunhofer.de/en/muv/2015/netson.html
[2] http://o-c-r.org/2014/11/15/specimen_box/

concentrate on network and server monitoring, we suggest to research also into the sonification of application logs (e.g. of workflow systems) in order to detect security threats from inside an organization as well.

V. Acknowledgement

This research was partly funded by COMET K1, FFG - Austrian Research Promotion Agency.

References

[1] J. R. Goodall, "Introduction to Visualization for Computer Security," in *VizSEC 2007*, ser. Mathematics and Visualization, J. R. Goodall, G. Conti, and K.-L. Ma, Eds. Springer Berlin Heidelberg, 2008, pp. 1–17.

[2] G. Kramer, B. Walker, T. Bonebright, P. Cook, J. Flowers, and N. Miner, *Sonification Report: Status of the Field and Research Agenda - Report prepared for the National Science Foundation by members of the International Community for Auditory Display*. International Conference on Auditory Display, 1999.

[3] P. Vickers, "Sonification for Process Monitoring," in *The Sonification Handbook*, T. Hermann, A. Hunt, and J. G. Neuhoff, Eds. Logos Berlin, 2011, pp. 455–492.

[4] C. Schmandt and G. Vallejo, "Listenin to domestic enviroments from remote locations," in *Proceedings of the 9th International Conference on Auditory Display (ICAD2003)*, E. Brazil and B. Shinn-Cunningham, Eds., Boston, 2003, pp. 220–223.

[5] G. Conti, *Security Data Visualization: Graphical Techniques for Network Analysis*, 1st ed. San Francisco: No Starch Press, Oct. 2007.

[6] H. Shiravi, A. Shiravi, and A. Ghorbani, "A Survey of Visualization Systems for Network Security," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012.

[7] T. Hildebrandt, "Towards Enhancing Business Process Monitoring with Sonification," in *Intl. Workshop on Theory and Applications of Process Visualization (TAProViz 2013)*, ser. Lecture Notes in Business Information Processing. Berlin, Germany: Springer, 2013.

[8] W. W. Gaver, R. B. Smith, and T. O'Shea, "Effective sounds in complex systems: the ARKOLA simulation," in *Proc. of the SIGCHI conference on Human factors in computing systems: Reaching through technology (CHI'91)*. ACM, 1991, pp. 85–90.

[9] A. Csapó and G. Wersényi, "Overview of Auditory Representations in Human-machine Interfaces," *ACM Comput. Surv.*, vol. 46, no. 2, pp. 19:1–19:23, Dec. 2013.

[10] T. Fairfax, C. Laing, and P. Vickers, "Network Situational Awareness: Sonification and Visualization in the Cyber Battlespace," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance:*, M. M. Cruz-Cunha, Ed. IGI Global, 2015.

[11] P. Vickers, C. Laing, and T. Fairfax, "Sonification of a Network's Self-Organized Criticality," Jul. 2014. [Online]. Available: http://arxiv.org/abs/1407.4705

[12] B. deButts, "Network Access Log Visualization & Sonification," Student Project, Tufts University, Medford, USA, 2014. [Online]. Available: https://tuftsdev.github.io/DefenseOfTheDarkArts/students_works/final_project/fall2014/bdebutts.pdf

[13] R. Giot and Y. Courbe, "Intention - interactive network sonification," in *Proceedings of the 18th International Conference on Auditory Display*. Atlanta, GA, USA: The International Community for Auditory Display, 2012, pp. 235–236.

[14] M. Ballora, N. A. Giacobe, and D. L. Hall, "Songs of cyberspace: an update on sonifications of network traffic to support situational awareness," vol. 8064, 2011, pp. 80 640P–80 640P–6. [Online]. Available: http://dx.doi.org/10.1117/12.883443

[15] M. Ballora and D. L. Hall, "Do you see what I hear: experiments in multi-channel sound and 3d visualization for network monitoring?" vol. 7709, 2010, pp. 77 090J–77 090J–7. [Online]. Available: http://dx.doi.org/10.1117/12.850319

[16] M. Ballora, B. Panulla, M. Gourley, and D. L. Hall, "Preliminary Steps in Sonifying Web Log Data." Washington: International Community for Auditory Display, 2010.

[17] J. Muoz-Arteaga, R. M. Gonzlez, M. V. Martin, J. Vanderdonckt, F. lvarez-Rodriguez, and J. G. Calleros, "A Method to Design Information Security Feedback Using Patterns and HCI-Security Criteria," in *Computer-Aided Design of User Interfaces VI*, V. Lopez Jaquero, F. Montero Simarro, J. P. Molina Masso, and J. Vanderdonckt, Eds. London: Springer London, 2009, pp. 283–294.

[18] A. Brown, M. Vargas, B. Kapralos, M. Garcia-Ruiz, and M. Green, "Poster: Towards Music-Assisted Intrusion Detection," Oakland, USA, 2009. [Online]. Available: http://faculty.uoit.ca/kapralos/publications/ieee_ssp2009.pdf

[19] M. A. Garcia-Ruiz, A. Edwards, M. V. Martin, and S. E. Seoud, "Auditory Display as a Tool for Teaching Network Intrusion Detection," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 3, no. 2, pp. pp. 59–62, Dec. 2007.

[20] L. Qi, M. V. Martin, B. Kapralos, M. Green, and M. Garca-Ruiz, "Toward Sound-Assisted Intrusion Detection Systems," in *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*, ser. Lecture Notes in Computer Science, R. Meersman and Z. Tari, Eds. Springer Berlin Heidelberg, 2007, no. 4804, pp. 1634–1645.

[21] M. V. Miguel A Garcia-Ruiz, "Towards a multimodal human-computer interface to analyze intrusion detection in computer networks," in *Proceedings of the First Human- Computer Interaction Workshop (MexIHC)*. Puebla, Mexico: University of the Americas, 2006.

[22] P. E. Varner and J. C. Knight, "Monitoring and Visualization of Emergent Behavior in Large Scale Intrusion Tolerant Distributed Systems," Pennsylvania State University, Tech. Rep., 2004. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.403&rep=rep1&type=pdf

[23] M. Gopinath, "Auralization of Intrusion Detection System using JListen," Master's Thesis, Birla Institute of Technology and Science, Pilani (Rajasthan), India, 2004. [Online]. Available: https://www.cs.purdue.edu/homes/apm/listen/JListen-1.0-BITS/Gopinath/MS-thesis/thesis-final.doc

[24] C. Papadopoulos, C. Kyriakakis, A. Sawchuk, and X. He, "CyberSeer: 3d Audio-visual Immersion for Network Security and Management," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 90–98.

[25] D. Malandrino, D. Mea, A. Negro, G. Palmieri, and V. Scarano, "Nemos: Network monitoring with sound," in *Proceedings of the 9th International Conference on Auditory Display (ICAD 2003)*. Boston, USA: International Community for Auditory Display, 2003.

[26] J. C. K. Philip E. Varner, "Security Monitoring, Visualization, and System Survivability," Vancouver, 2002. [Online]. Available: http://www.cs.virginia.edu/~jck/publications/security.visualization.isw-2001.pdf

[27] M. Kimoto and H. Ohno, "Design and Implementation of StethoNetwork Sonification System," in *Proceedings of the 2002 International Computer Music Conference*, 2002, pp. 273–279.

[28] M. Barra, T. Cillo, A. De Santis, U. Petrillo, A. Negro, and V. Scarano, "Multimodal monitoring of Web servers," *Multimedia, IEEE*, vol. 9, no. 3, pp. 32 –41, 2002.

[29] M. Gilfix and A. L. Couch, "Peep (The Network Auralizer): Monitoring Your Network with Sound," in *Proceedings of the 14th USENIX Conference on System Administration*, ser. LISA '00. Berkeley, CA, USA: USENIX Association, 2000, pp. 109–118.

[30] W. Hauer and K. Vogt, "Sonification of a Streaming-Server Logfile," in *International Conference on Auditory Display (ICAD) 2015*, ser. Proceedings of the 21st International Conference on Auditory Display, Graz, Austria, 2015, pp. 315–316.

[31] D. Worrall, "Realtime Sonification and Visualization of Network Metadata (The NetSon Project)," in *International Conference on Auditory Display (ICAD) 2015*, ser. Proceedings of the 21st International Conference on Auditory Display, Graz, Austria, 2015, pp. 337–339.

[32] T. Hildebrandt, T. Hermann, and S. Rinderle-Ma, "A sonification system for process monitoring as secondary task," in *2014 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom)*, Nov. 2014, pp. 191–196.