Poster: Sonification in Security Operations Centres: What do Security Practitioners Think?

Louise Axon, Bushra Alahmadi, Jason R. C. Nurse, Michael Goldsmith and Sadie Creese
Department of Computer Science, University of Oxford
{louise.axon, bushra.alahmadi, jason.nurse, michael.goldsmith, sadie.creese}@cs.ox.ac.uk

This poster is related to a paper appearing at the Workshop on Usable Security (USEC) 2018.

Title: *Sonification in Security Operations Centres: What do Security Practitioners Think?*

Authors: Louise Axon, Bushra Alahmadi, Jason R. C. Nurse, Michael Goldsmith, and Sadie Creese

Abstract: In Security Operations Centres (SOCs) security practitioners work using a range of tools to detect and mitigate malicious computer-network activity. Sonification, in which data is represented as sound, is said to have potential as an approach to addressing some of the unique challenges faced by SOCs. For example, sonification has been shown to enable peripheral monitoring of processes, which could aid practitioners multitasking in busy SOCs. The perspectives of security practitioners on incorporating sonification into their actual working environments have not yet been examined, however. The aim of this paper therefore is to address this gap by exploring attitudes to using sonification in SOCs. We report on the results of a study consisting of an online survey *(N=20)* and interviews *(N=21)* with security practitioners working in a range of different SOCs. Our contribution is a refined appreciation of the contexts in which sonification could aid in SOC working practice, and an understanding of the areas in which sonification may not be beneficial or may even be problematic. We also analyse the critical requirements for the design of sonification systems and their integration into the SOC setting. Our findings clarify insights into the potential benefits and challenges of introducing sonification to support work in this vital security-monitoring environment.

Sonification in Security Operations Centres: What do Security Practitioners Think?

Louise Axon, Bushra Alahmadi, Jason R. C. Nurse, Michael Goldsmith and Sadie Creese
Department of Computer Science, University of Oxford, {firstname.lastname}@cs.ox.ac.uk

Motivation and Research Aims

Sonification, in which data is represented as sound, can be used to turn network attacks and network-security information into audio signals [1, 2]. Anecdotal evidence suggests that this technology could aid security practitioners working in Security Operations Centres (SOCs), using a range of security tools to detect and mitigate malicious computer-network activity.

While sonification appears a feasible solution, the perspectives of security practitioners on incorporating sonification into their working environments have not yet been examined. We addressed this gap in our study by interviewing security practitioners.

Figure 1: A Security Operations Centre [5]

Specifically, we explored the views of security practitioners working in SOCs, through an online survey (N=20) and interviews (N=21), Our goal was to better explore the following areas:

- Understanding and refining **contexts of use** in which sonification may improve SOC working practice
- Investigating the perceived **challenges** in the integration of sonification into SOC environments
- Determining requirements for the **design** of sonification systems useful for monitoring tasks in SOCs

Participants

We recruited 20 online survey participants, and 21 interview participants, between January and June 2017.

Participants were security practitioners working in SOCs with whom we had previously established relationships.

	Internal SOC total	Multitenanted SOC total
Manager	3	1
Senior Analyst	0	3
Analyst	7	3
Engineer	2	0
Analyst & Engineer	0	2

Table 2: Interviewee Demographics

Developing Tentative Use-Cases Using Literature and Online Survey

Literature survey: explore possible uses

3 OQs affirmed by online survey responses

Tentative use-cases (UCs) derived:

UC1. Detecting anomalies in the network traffic
UC2. Monitoring as a non-primary task
UC3. Monitoring data presented across multiple screens
UC4. Alleviating fatigue from monitoring screens
UC5. Enabling monitoring whilst outside of the SOC

Online survey: address outstanding questions (OQs).
OQ1. Do security practitioners feel capable of detecting anomalies directly from the network traffic?
OQ2. Are security practitioners required to multitask while monitoring in SOCs?
OQ3. Are security practitioners required to visually monitor information presented on multiple screens?

Methodology

Our methodology followed the general requirements analysis process [3].

Stages of our study:

Literature and online survey → Tentative use-cases → Semi-structured interviews → Refined contexts of use, integration and design

Stages of requirements analysis process [3]:

Information gathering → Identify user needs → Envisioning and evaluation → Requirements specification

We developed a network-packet sonification prototype, which mapped properties of packets to properties of musical notes, as described in Table 1 and Figure 2, to familiarise participants with the concept of sonification in the semi-structured interviews.

Packet property	Musical property
IP/port common-ness	Note consonance
Source/destination IP/port	Octave of note
Packet size	Amplitude
Direction of traffic	Pan of sound

Table 1: Sonification Prototype Mappings

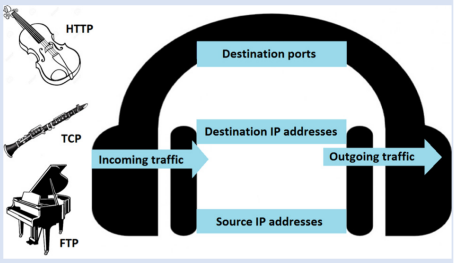

Figure 2: Sonification Prototype Design

In the interviews, we discussed each of the **tentative use-cases** (developed as highlighted later), focusing on its utility, and requirements for integration in SOCs and sonification design.

Interview: What Security Practitioners Thought

The Likert Scale ratings given by practitioners for the potential utility of each **tentative use-case** are presented in Table 3. Below the table, we present a selection of comments made by practitioners about the use-cases.

Use-Case	Mode	Median	Comparison of Non-Neutral Scores (disagree:agree)
UC1. Anomaly detection	3.5	4	2:12
UC2. Multitasking	5	4	5:12
UC3. Multiple screens	4	4	5:14
UC4. Visual fatigue	2	3	9:8
UC5. Outside-SOC activities	5	5	1:19

Table 3: Use-Case Potential Utility Ratings

UC1. Detecting anomalies in the network traffic: *"There's still a lot of human analysis, and a machine can only determine the really obvious ones"... "When say a DoS attack or some other form of attack would take place, I'm sure it would stand out because you would get used to hearing a certain type of tune or hum from day-to-day activity."*

UC2. Monitoring as a non-primary task: *"One issue we have is that when we see something of interest, and we are researching that or raising a ticket for escalation, you're no longer monitoring. So, at points in time when you're not monitoring, if there was an audible cue that 'oh actually, there is something happening right now, maybe my attention should be back there'."*

UC3. Monitoring data presented across multiple screens: *"I will still use 7 screens, even if I have all the sound in the world"..."If I don't have enough screens, I've got to constantly minimise, maximise, and copy this and go here and it can be very difficult."*

UC4. Alleviating visual fatigue: *"I can see it as an alternative to visualization for when you get to a point when your eyes are tired... the thing is if you only switch it on when you get to that point, then I think you won't really understand what normal would be, so you would still need it on in the background to some extent."*

UC5. Monitoring whilst outside of the SOC: *"Today it's only me here, and I did have to leave to the shop earlier"... "They wouldn't need to rush back, keep checking, they could just go about their business and know, 'right, when I hear that sound, I need to take whatever action'".*

Implications of Findings

Refined Contexts of Use

- **Detecting anomalies in network traffic.** Presenting high-resolution sonifications of the network traffic to enable humans to hear network anomalies. This concept is similar to the use of security visualizations for use in real-time network security-monitoring and in retrospective network "threat hunts".
- **Multitasking whilst monitoring as a non-primary task.** Sonifying network-security data, including both network packets and alerts, to be monitored as a secondary task, while carrying out a separate primary task.
- **Monitoring whilst outside of the SOC.** Enabling security practitioners to continue their security-monitoring work whilst outside of the SOC (e.g., grabbing a drink), by listening to sonified displays.

Design Requirements

- **Sonification of alerts.** Sonified alerting, both separately to and in combination with the network traffic sonification, was suggested for communicating critical events – in particular, type and severity.
- **Mitigating fatigue.** Practitioners felt that sonification could be fatiguing. Sonification design approaches (e.g. aesthetic sonification) should aim to mitigate fatigue.

Integration Challenges

- **Headphones/speakers/earpieces.** Using speakers could distract other SOC practitioners not using the sonification, while headphones may isolate practitioners and hamper collaboration. A potential solution suggested was the use of a single earpiece.
- **Existing SOC workflow and soundscape.** The sonification should work with the existing soundscape. Existing soundscapes varied: no deliberate noise; radio for the whole room; practitioners listening to music through headphones.

References

1. Ballora, M., Giacobe, N.A. and Hall, D.L., 2011. Songs of cyberspace: an update on sonifications of network traffic to support situational awareness. In *Proc. SPIE* (Vol. 8064, pp. 80640P-80640P).
2. Mancuso, V.F., Greenlee, E.T., Funke, G., Dukes, A., Menke, L., Brown, R. and Miller, B., 2015. Augmenting cyber defender performance and workload through sonified displays. *Procedia Manufacturing*, *3*, pp.5214-5221.
3. Maguire, M. and Bevan, N., 2002. User requirements analysis. In *Usability* (pp. 133-148). Springer US.
4. U. S. Air Force photo, American Forces Press Service, 2013.

EPSRC Engineering and Physical Sciences Research Council
UNIVERSITY OF OXFORD
CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY