The Sound of Security: Sonification for Cyber Monitoring Centers

When walking into a security operations center (SOC), the first thing that one would notice would be screens everywhere. This is not an uncommon occurrence in monitoring centers around the world. From the smallest IT services provider to the giant monitoring centers at Google, there will always be screens with real-time data constantly streaming. Although this information is extremely helpful, there are often so many visual cues that any incident that needs to be recognized is lost in the flood of numbers and colors. If this is simply a flag for a mistyped password, this is not a problem. However, if these are the early signs of a data breach or network failing, large amounts of people can be negatively affected. In an effort to combat this, there has been new research into transforming some of these visual monitoring tools into auditory monitors.

There have been several proposals for how networks and cybersecurity incidents could effectively be represented musically. It is important to mention the few that appear to have the most merit. They also provide the foundation that more complex systems could be built around. Many auditory monitors are considered "network auralizers" which work "by comparing sounds with the sound of the 'normally functioning' network" (Axon et al. 28). This could mean at the protocol level, normal events like DNS (Domain Name System) queries and ARP (Address Resolution Protocol) requests would be considered 'normal' and could establish an auditory baseline. From a musical perspective, this could mean standard protocols could be a part of an established key or, slightly more complex to implement, an established melody. If suspicious network activity happens, then the event would be similar to a trill or an off-pitch sound to alert the listener that something is potentially wrong. For example, multiple failed TCP (Transmission Control Protocol) handshakes or lots of ICMP (Internet Control Message Protocol) packets pinging the network would trigger these alerts. This design could be used, based on size of the company and specific monitoring center goals, to represent an entire network or “the whole state of the part of the system the system manager is interested in” (Axon et al. 29).

Although more complicated sonification monitors have been tested with varying degrees of success, they run into the same issues as visual monitors: too much information to be easily isolated and investigated. These monitors should instead focus on one aspect of a monitor at a time to be truly efficient. For instance, some monitors could have a steady melody that is stopped if, for example, a network outage occurred. On the other hand, it might be helpful to look at this from the opposite angle for security monitors. Normal security events (ex: successful login) would be traditional harmonies that are perhaps much slower in tempo. If multiple failed logins are then logged, the piece could become dissonant to help isolate the suspicious activity. Volume also plays a key role in this type of monitor. As anyone regardless of technical expertise can attest, the louder an alert, the easier it is to recognize. Most proposals assert that volume should increase as more events occur, whether they are continuous network blips or a ransomware attack beginning to encrypt a system. The specificity to which alerts are assigned volume changes and to which degree would be based on the specific needs of a company or user.

There is a fine line between noticeability and hindrance that needs to be approached carefully with auditory monitors. For example, “the more distinctive and invasive the sound, the more likely that a listener will notice. However, overuse of the noise will cause fatigue” (Falk and Dykstra). This will change based on the preferences of the user, the needs of a monitoring system, and the size of the company. Nevertheless, the new technologies surrounding sonification in a network monitoring center can help ease the identification of events that need to be investigated.

Works Cited

Axon, Louise et al. “A Formalised Approach to Designing Sonification Systems for Network-Security Monitoring.” *International Journal on Advances in Security,* vol. 10, no. 1-2, 2017, pp 26-47. www.cs.ox.ac.uk/files/9190/2017-secadv-angc.pdf. Accessed 15 July 2024.

Falk, Courtney and Josiah Dykstra. “Sonification with Music for Cybersecurity Situational Awareness.” *The 25th International Conference on Auditory Display,* June 2019. *Georgia Tech Library,* repository.gatech.edu/entities/publication/bd17d29b-6c46-4c93-b1ba-288ced101387. Accessed 15 July 2024.