HOW LINK22 SHIELD INTERFERE WITH SOUND

link22 Shield is constructed to prevent a phone, or similar, from listening in on what is said in the room. This is mainly achieved by the soundproof box consisting of a soundproof lid, inner box and rubber seals that efficiently dampen the sound from within the meeting room. Electronics within link22 Shield ensure that the remaining sound from the surrounding is efficiently disrupted by a masking sound that is played by the speakers.

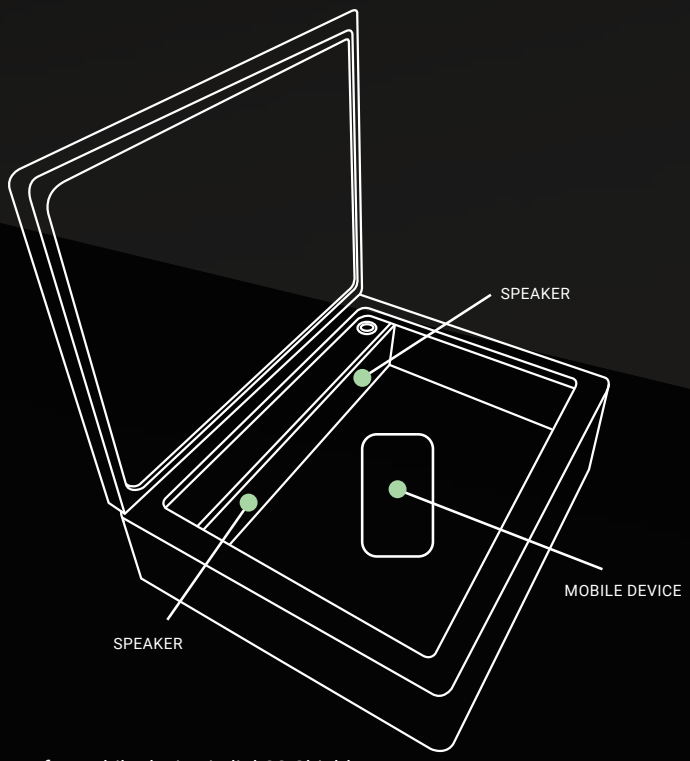

Illustration of a mobile device in link22 Shield.

PROBLEM DESCRIPTION

What is desired to be achieved is a masking sound that is sufficiently loud to disrupt the meeting participants' speech, but at the same time, not as loud as to be an interfering element in the meeting. The soundproofing in link22 Shield ensures that the masking sound can be played at a loud volume and have the sounds of the meeting efficiently dampened.

An important requirement on the masking sound is that it shall be practically impossible to filter out from a recording made on mobile device placed in link22 Shield. Poor sound generation could in theory lead to an opponent being able to filter out the masking sound. link22 Shield defends itself from this through multiple technical measures.

Keep reading if how the masking sound in link22 Shield is generated seems interesting.

DESIGN OF MASKING NOISE

To solely use white noise (static) as masking sound is less efficient than to combine the naoise with random voices. This is partly due to the random speech being the same frequency as the sound that we want dampened, meaning the meeting participants' speech. In addition, it is also more difficult for humans to filter out speech than noise, which heightens security.

The sound generation in link22 Shield is a combination of random synthetic voices and a specifically adapted noise. Before we go into detail about these parts, we will explain how link22 Shield randomize the noise.

RANDOMIZATION

Not many are aware that it is quite difficult to randomize. Technical solutions often use built-in randomization in a computer. However, the computer itself cannot randomize. It does the best it can, but with enough resources, the randomization can be analyzed and finally become entirely predictable. Since link22 Shield randomize to create both the static noise and the synthetic voices, it is important that real randomization is used.

When link22 designed link22 Shield, we utilized our extensive experience with cryptographic appliances, which is clearly visible from how we create and use randomization. The special hardware in link22 Shield generate randomization by utilizing known physical phenomenon that are random by nature. This generates real randomization that is not possible to predict. The randomization hardware is monitored and if it stops randomize, link22 Shield goes into an error mode.

SYNTHETIC VOICES

link22 Shield uses two computer-generated voices that are talking over the top of each other. They are reading from a word-list of over 350 000 words randomly. Their pitch and pronunciation changes continuously in a random way. This is done to further lessen the possibility of finding patterns.

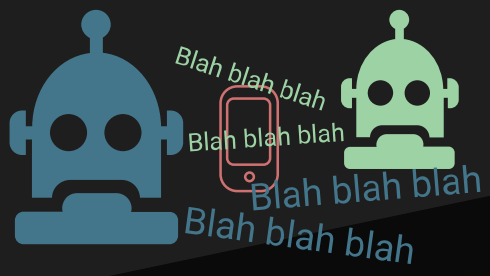

Illustration of the computer-generated voices.

STATIC NOISE

Not all static noise is the same, and link22 Shield creates a special static noise, pink noise, that is extraordinary suitable for disrupting speech, while at the same time not being as disrupting to its surroundings as other static noises. Pink noise often occurs in nature, for example the noise of rain. The noise is created by software and uses the special randomization hardware in link22 Shield.

Illustration of pink noise in link22 Shield.

CONCLUTION

The combination of randomized computer-generated voices, and the pink noise, being played at a loud volume within the soundproof structure makes link22 Shield into efficient telephone tapping protection.

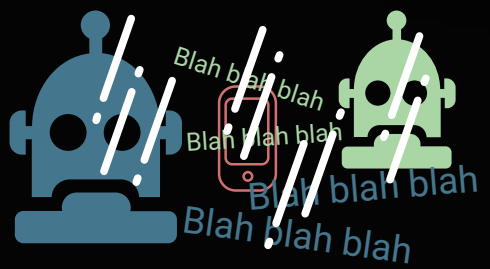

Illustration of the sound environment for a mobile device inside link22 Shield.