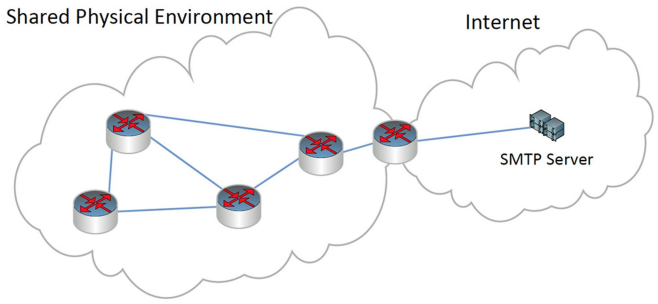
Researchers at the Fraunhofer FKIE develop a malware prototype able communicate using inaudible audio signals-- allowing it to exchange data even between infected machines lacking a network connection.



Based on technology originally designed for underwater communications, the use of ultrasonic frequencies (or "covert acoustical communication") allows the penetration of "air gaps" sealing computers from the outside world.

The malware uses built-in microphones and standard speakers to transmit small amounts of data from distances of nearly 20m at up to 20 bits per second-- a distance it can enlarge by creating an "acoustic mesh network" out of infected devices repeating the audio signals.

Applications the researchers suggest for such technology include an acoustical multi-hop keylogger and connecting to and tunneling over the internet. As for countermeasures, switching off audio input and output devices would do the trick, as well as the implementation of audio filtering solutions able to block the high-frequencies ranges covert data transmissions use.

Such a development in exotic malware reminds us of an unusual case faced by security consultant Dragos Ruiu. As reported by Ars Technica, Ruiu has spent the last 3 years dealing with what he calls "badBIOS," a mystery malware supposedlly able to use high-frequency signals to jump between airgaps.

"We had an air-gapped computer that just had its [firmware] BIOS reflashed, a fresh disk drive installed, and zero data on it, installed from a Windows system CD," Ruiu tells Ars Technica. "At one point, we were editing some of the components and our registry editor got disabled. It was like: wait a minute, how can that happen? How can the machine react and attack the software that we're using to attack it? This is an air-gapped machine and all of a sudden the search function in the registry editor stopped working when we were using it to search for their keys."

The badBIOS story sounds like something out of science fiction, even if Ruiu remains a respected figure in the security community. However the Fraunhofer FKIE researchers show ultrasonic-based malware is a distinct possibility, so who knows?

Go On Covert Acoustical Mesh Networks in Air

Go Meet "badBIOS" (Ars Technica)