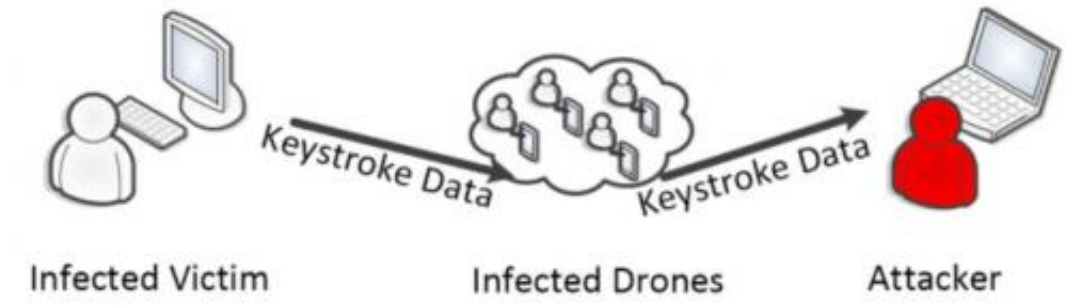
Authors explore security threat of covert acoustical mesh networks in air

December 3 2013, by Nancy Owano



Scenario for a multi-hop acoustical keylogger. Credit: Michael Hanspach and Michael Goetz

(Phys.org) —"If we want to exploit a rigorously hardened and tested type of computing system or networks of this type of computing system, we have to break new ground. Covert channels are communication channels utilizing means for communications that have not been designed for communication at all." So begins a bracing paper published last month in the *Journal of Communications*. Titled "On Covert Acoustical Mesh Networks in Air," the paper discusses devices that can support stealthy communication preventing immediate detection of the covert channels. The authors, Michael Hanspach and Michael Goetz, are research associates at the Fraunhofer Institute for Communication, Information Processing and Ergonomy (FKIE), in Wachtberg, Germany.

The authors warned that "Acoustical networking as a covert

communication technology is a considerable threat to computer security and might even break the security goals of high assurance computing systems based on formally verified micro kernels that did not consider acoustical networking in their security concept."

Researchers in the past have described acoustic wave propagation used in underwater setups but the authors in their research did something different.

"The underlying network stack is based on a communication system that was originally designed for robust underwater communication. We adapt the communication system to implement covert and stealthy communications by utilizing the near ultrasonic frequency range. We further demonstrate how the scenario of covert acoustical communication over the air medium can be extended to multi-hop communications and even to wireless mesh networks."

The authors showed that establishing covert acoustical mesh networks in air is feasible in setups with commonly available business laptops. (The authors noted that a covert acoustical mesh network can be conceived as a botnet or malnet that is accessible via nearfield audio communications.) For their experimental setup, they used five laptops as the mesh network participants. They installed Debian 7.1 on each laptop.

Commenting on their work, Dan Goodin of Ars Technica said the new research shows that "high-frequency networking is easily within the grasp of today's malware." In an email, Hanspach said that commonly available laptops can communicate over their internal speakers and microphones, and form a covert acoustical mesh network. Over that network, "information can travel over multiple hops of infected nodes, connecting completely isolated computing systems and networks (e.g., the internet) to each other."

The authors, in their paper, also discussed countermeasures against covert acoustical mesh networks. These include the use of lowpass filtering in computing systems and a host-based intrusion detection system for analyzing audio input and output to detect irregularities.

More information: Research paper: On Covert Acoustical Mesh Networks in Air, www.jocm.us/index.php?a=show&catid=124&id=600