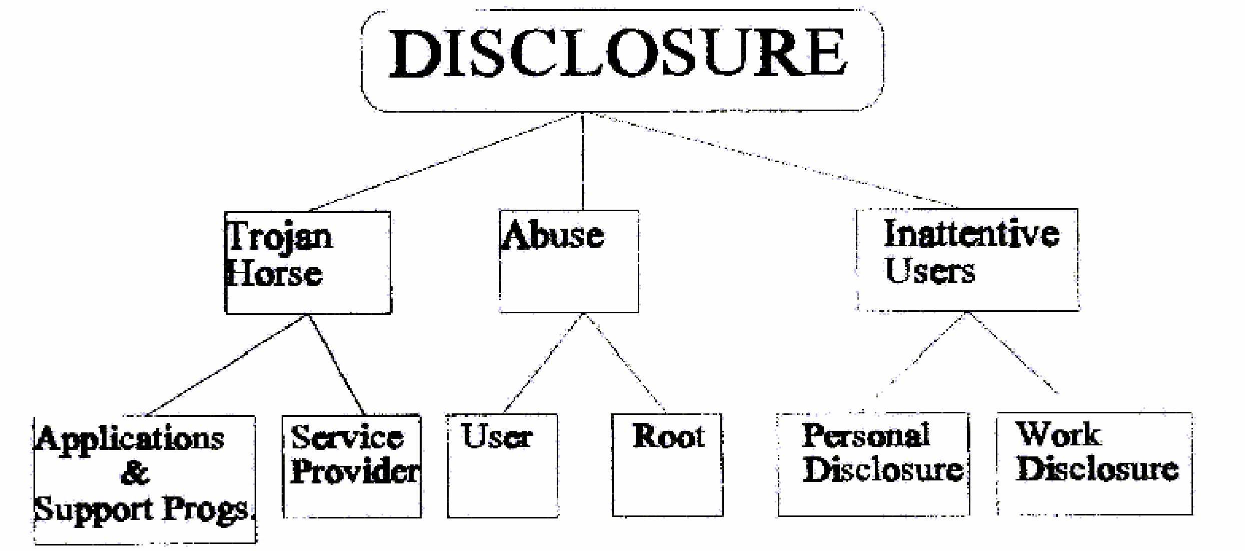
Emerging Security Issues Involving the Presence of Microphones and Video Cameras in the Computing Environment

Sam Nitzberg
241 Cummings Avenue
Elberon, NJ 07740

Microphones and video cameras are becoming more common accessories in the modern computing environment. As their popularity has been increasing, little has been said regarding any new security problems which may be created by their presence. My intention is to examine security problems that their presence may contribute to, and assess their severity, as well as possible remedies.

The diagram below offers one view of how disclosure threats may be considered in computing environments with microphones and / or video cameras. These devices can be used to covertly monitor the audio and video of happenings in their vicinity.



The issues represented in the above diagram may be considered critical for a host of reasons. Immediately under disclosure are represented what are often relatively easy to perform attacks, and arguably, the most significant vulnerability present - inattentive users. Further, the attacks mentioned at this level in the diagram (the use of Trojan horses and flagrant abuse) represent the mechanisms through which microphones and cameras may be most easily and most effectively exploited to the detriment of innocent parties. Trojan horses may be viewed as relatively common vehicles for attack in modern computing systems; while strong checksums, authorized delivery channels for software systems, and operating systems with varying levels of program or user access or authority may reduce this threat, there is still the potential for serious problems. Trojan Horses may appear as adulterated applications or support programs, or may even be present in the form of service-provider software or even as actual services. Regarding abuse, it is very easy in many environments for a single, trusted administrator to undermine the in-place security policy of a computing system or environment. While it may be more difficult for an individual user to do so, it is often very possible; regardless, even without privileged systems access, it is possible in certain environments for individual users to have or be able to obtain significant access to systems resources. Lastly, inattentive users may often discuss sensitive work-related or personal matters in front of computing stations capable of performing eavesdropping. Such innocent indiscretions could be taken advantage of. This diagram is intended to represent one view of the problem at hand, not necessarily an all-encompassing or definitive one.

The presence of microphones and video cameras in computing environments has the potential to create some significant security concerns. Part of this belief is based on the existence of what has been described in the media world as the "Hot Microphone" problem. Such a problem exists when a speaker is to appear for a presentation, and not knowing the equipment around him is live (microphones, video-cameras, etc...), proceeds to say things not intended to be preserved for posterity nor distributed by the media. Perhaps the most famous example of this would be the occassion when President Ronald Reagan said privately and jokingly at a press conference, "My fellow Americans, I am pleased to tell you today that I have signed legislation that will outlaw Russia forever. We begin bombing in five minutes."[Reagan] Following this remark, officials at the highest levels of Soviet government voiced their severe displeasure. While less visible, many individuals from all walks of life have said things equally embarrassing in front of their computer systems, and the presence of microphones in today's computing environments has introduced the hot-microphone problem into labs, offices, homes, and the corporate workplace.

The potential exists for computer-based eavesdropping both in the local and networked computing models. On a local system, a computer could eavesdrop, and digitize and record conversations to disk for later retrieval. Standalone situations hinting at future possibilities have already arisen. Recently in New Jersey, a man filed for divorce from his wife, citing a computer exchange she was having as evidence of infidelity. He discovered this through accessing her electronic mail, without being granted authority. From this, it would not be a far jump for individuals to be capable of covertly accessing recorded voice and / or video exchanges between parties. In networked environments, a few scenarios exist. With networked systems, the voice data may be stored for later retrieval, as in the previous model, or the system may be used to implement a real-time voice audio or video monitoring system. Taken to its full extreme, the possibility exists for multiple nodes in a network to be used to constantly eavesdrop, fully reporting , storing, and replaying audio on a single workstation. An example of this could involve a single employee using each of the workstations on the floor of a building to conduct surveillance through his or her workstation. Such an employee would most likely hold a systems administrative position, and such a software or operating systems setup would allow him to effectively wiretap the offices of a building without the risk associated with conventional, highly-intrusive covert surveillance equipment. Such abuse by a privileged account holder could be relatively simple to perform without the proper measures to preclude such activities. Such measures would include enforcing separation of duty for critical tasks, maintaining proper and auditable logs for administrative chores, and even conducting routine criminal background checks on employees (where allowed by law).

Of interest are factors related to the bandwidth required for these voice and/or video communications. Voice can be captured and transmitted very nicely in 4 to 8 kbps without compression.[IEEE1, IEEE2] At ethernet lan rates (10mbps), this equates to 4kbps/10mbps * 100 = .04% of network capacity, without compression, easily allowing for real-time eavesdropping without degrading the local area networks. Based on this, the storage required to accommodate audio for a full 24-hour day would be 44 megabytes of storage. While these figures are crude, provide only upward bounds, and do not reflect overhead due to any possible protocols involved, they would tend to discount full-time bugging and storing of audio for most long-term situations. Regarding video, live video and audio teleconferencing may be achieved with 28.8 kbps of bandwidth (for dial-up connections, presumably with compression provided by modems), or 115kbps of capacity (for network connections). Still shots (images) typically require less than 100k per image [CONNECTIX]. From this, it would appear reasonable that the technical means and methods for peeping would seem to be similar to those applicable for eavesdropping. A present-day example of threats may be seen to be possible by companies which are presently creating the capability for strangers to communicate through dial-up lines and internet connections through their systems [IEEE2]. It would be a simple matter for these companies to digitally store any such conversations. Further, precedents exist where even official telephony representatives have eavesdropped on paid customer-calls on the public network [The Phone Book].

Microphones are becoming more common in today's computing environments. A number of factors are contributing to this trend. A great many systems, such as the Sun SparcStation 20 tend to include microphones in their standard delivery / configuration. Many of these microphones are plugged in, clipped to the front of the computer's monitor, and are essentially forgotten. Notebook computers have been selling in large numbers, with most of the recent sales consisting of systems including internal microphones dubbed "multi-media" notebooks by vendors. While it is a trivial matter to include a microphone in the design of such systems, it is not generally considered commercially desirable to compel the user to have to carry around an external microphone - yet one more corded attachment or device to keep track of.

Traditionally, the microphone was an often ignored piece of equipment in the computing environment. Musicians with fairly elaborate musical systems incorporating computers were one group which actually used their microphones. Voice annotation for records is becoming more common by users of database systems, and more systems, such as medical entry systems are using voice recognition. Recently, software for both PC based Windows systems and Unix workstations to allow "telephone calls" to be placed between machines either on the same network, or connected via the internet to be placed have been gaining in popularity. The potential would appear for such software to act as, or to allow "wiretapping," which should be of concern to all users of such software. The price for video cameras for computers has been dropping, with models available for as little as $100 [WIRED]. As more applications make use of these cameras, as their prices continue to drop, and standard video formats are accepted, their numbers, too shall increase.

A problem still should be addressed - how can someone be protected from the "Hot Microphone" problem? One approach which might be discounted as expensive or impractical for most purposes would be to use microphones with encryption circuitry ("encrypting microphones") or encrypting, secure video cameras. Besides possible cost questions, the obvious problem of possible peeping and eavesdropping may be converted into the potentially much more difficult problem of key management. One possible hardware - based approach would involve a DMA (Direct Memory Access) microphone. The audio input from this microphone would be sent directly into a memory location specifically allotted for this purpose.

Any attempt for the computer to read microphone input would have to go through DMA circuitry to access this address. When read operations would be performed to this address, an indicator would go on. In this fashion, at least, anyone near the given system could definitively know if the computer was being used to record them. Presently, this would be a kludge in most systems, and not likely to be implemented. While some microphones (such as a certain model sometimes supplied by Sun Microsystems) have an on/off switch, many do not. All systems should have an obvious on/off switch for the microphone. Further, systems in corporate settings should be equipped with a plainly visible sticker indicating the presence of any microphone or video cameras, again as all of these are not obvious, and they are easily forgotten. In terms of education, systems management, and security measures being taken, it would seem that the simplest and cheapest measures are often likely to be the most effective.

The requirement of many operating systems, such as Unix, to run administrative procedures in a privileged mode can limit the damage a Trojan Horse may inflict on a system. If properly managed and maintained, such systems should not become severely compromised. Even if a system is compromised, the proper use of firewalls to restrict information flow should prevent the threat from propagating through additional networks. Still, due care must be taken in how privileged accounts are used, maintained, and how systems software is installed and upgraded.

At various levels, audit trails and audit analysis methods may be used to identify and characterize typical and legitimate users of microphone devices, as well as audio from microphones being acquired for extended periods without just cause. Naturally, most environments will not be capable of performing audit analysis at real-time rates. However, the possibility to notice attacks (such as microphone-based eavesdropping) when they are initiated or shortly thereafter could be used to help identify such situations.

On some systems, the mere presence of a microphone introduces a vulnerability. Multiple versions of SunOS and Solaris were released with permissions set weakly for /dev/audio [CERT]. CERT's advice was to either unplug or turn off the microphone if a given site was seriously concerned with audio vulnerabilities [CERT]. While Windows 95 systems do provide authentication in networked environments, Windows 95 has weaknesses in its security in its Standalone mode. With respect to microphone input, Windows systems usually have their microphone connected through a sound board. The microphones typically do not have on/off switches, and are controlled through the soundboard, which in turn is controlled by software. Therefore, Windows 95 would seem to be an operating system and environment ripe for abuse.

Dial-up service providers for PC-type computers could create special problems for those whose systems contain microphones. A number of service providers provide their own software for use with Microsoft Windows to allow access. Such software could be made to include eavesdropping software, a Trojan Horse, without the knowledge of the end-user. Ken Thompson relates the moral: "You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code." [THOMPSON] Such Trojan Horses would allow the service provider to perform eavesdropping while the connection exists, or to configure the affected system to constantly eavesdrop, and forward the audio when connections are established to the service provider, for specially selected users. While such scenarios may seem, or even be, a bit fanciful, they are tame in comparison with some of the extreme measures which have been taken at times to conduct surveillance through the use of high technology. One text describes how a "front" business was used, along with international shipping and buyers, to entice a diplomat's staff member to buy an elegant desk retrofitted full of hi-tech radio bugging and transmitting gear [OSTROVSKY]. Software bugs (pun intended) are not invasive, could be made to self-destruct relatively cleanly, and could even be upgraded remotely.

Many security applications, network configuration tools, and proper administrative mechanisms exist to properly secure computers which have microphones and video cameras as accessories. While the hot-microphone problem does exist in computing environments, it represents a typical case of what may be considered the general computing security problem - how to ensure that all users and privileged users may perform their allowable operations, while not permitting them (or anyone else) to perform operations to which they are not entitled. Those most vulnerable to the mentioned threats are likely to be those in small environments, maintained by only a single administrator. In these environments, the best advice for users would tend to be caveat lector (reader beware).

REFERENCES:

CERT	CERT ADVISORY CA-93:15
CONNECTIX	Telephone interview with Technical Support, 19 April 1996
IEEE1	Design Trade-offs in Cellular/PCS Systems Dr. On-Ching Yue, AT&T Bell Laboratories Lecture 21 Feb 96, Colt's Neck Inn for NJ Coast Section IEEE
IEEE2	Internet Telephony Talk by Lior Haramaty, VocalTec, Inc. 12 Feb 96, Colt's Neck Inn for NJ Coast Section IEEE
OSTROVSKY	By Way of Deception: The Making and Unmaking of a Mossad Officer Victor Ostrovsky & Claire Hoy, St. Martin's Press, NY (C) 1990
REAGAN	Audio available from http://www.dnaco.net/~bkottman/sounds/
THE PHONE BOOK	J. Edward Hyde, Henry Regnery Company (C) 1976
THOMPSON	Reflections on Trusting Trust Ken Thompson Turing Award Lecture Communications of the ACM, August 1984, Vol. 27, Number 8
WIRED	Connectix Advertisement, April 1996