C1 Conventional Surveillance is Adaptable to the IP Camera and the IP Eavesdropping of Security (Countermeasures)

Ching-Sheng Chang, Taipao Chin, BA, and Min-Chang Shi, BA, Investigation Bureau Ministry of Justice, 74 Road Shin-Tien City, Taipei County, Taiwan 231, Taiwan, Republic of China*

After attending this presentation, attendees will understand that the webcam is becoming a criminal tool for remote monitoring and will recognize that conventional equipment is still useful to overcome the application of new technology for webcam surveillance.

The webcam uses the Internet and the Wireless LAN so popular today, and it is a convenience to connect people. Reversely, it threatens security. No one is an exception to violation of personal privacy, especial to VIPs and governmental officials. This presentation will impact the forensic community and/or humanity by demonstrating how this is becoming a considerable issue to the forensic community.

The Internet has been developed as a worldwide communication network and it is almost extended to anywhere of the world. Furthermore, Bluetooth technology and wireless LAN are built easily and are commonly available. In the past invaders, for some specific reasons, had to combine few electronic components for assembling a covered device as a spy tool in order to monitor activities or to listen to conversations of someone at a hidden place. In principle, the components include the sensors (pin-hole camera or small microphone) and transmitter (the simplest one is a cable only, or various RF modulation modules). Then the signal is transmitted to the receiver. As a mature technique today, to check and find those suspected devices using advanced detection equipment will not be a problem.

Relatively, as the Internet becomes a popular communication tool of transporting multimedia message, it is easier to do the same illegal action than before. An offender is easily able to remotely monitor the activities of others because spy camera and eavesdropping have been migrated to webcam as new tools to violate privacy and human right as well as causing criminal behavior. This paper intends to describe some efficient methods in finding illegal webcams and providing a guideline to search for hidden webcams or bugs via conventional detection equipments.

The context of this paper will focus on the portion of the sensors for detection and surveillance rather than paying too much attention to the portion of signal transmission. By means of this paper, the authors would like to remind readers (especial forensic persons) about emphasizing the inspection to the suspected webcam with microphone device. It is important to regulate any computer system with a capability of internet connection (wire line or wireless) shall not be allowed for a confidential meeting. For example, an advanced model of notebook PC is a particular one used for doing a spy job, but it is neglected from security inspection. The task of counter-measurement shall rely on high- tech measuring equipment but also depends on the skill to recognize what are some potential resources of insecure accessories.

The purpose of this study is to eliminate a puzzle about counter- measurement for the challenge to the illegal application of webcam with wires or wireless transmission.

Web Camera, Countermeasure, PC

** Presenting Author*