C1 Analyzing Some Potential Security Problems Using a Regular Telephone Set

Ching-Sheng Chang, and Shi-Wei Lee, Ministry of Justice Investigation, 74, Chung-Hwa Road, Shin-Tien City, Taipei, Taiwan 231, ROC*

The goal of this presentation is to identify potential security problems in using regular telephone sets and to share the authors' experiences with counter-measures for finding audio surveillance equipment by attaching wire-taps or coupling devices. It also benefits those inexperienced with eavesdropping equipment to help prevent a disclosure while talking about confidential information in a telephone conversation.

Improvements in telecommunications in the last century have enabled people to talk to each other efficiently over the phone without geographic or time barriers. The telephone set has become the most popular form of telecommunication because it is available to every office and family in the world. Consequently, eavesdropping is often used to monitor specific persons under surveillance. Normally, the placement of the eavesdropping device is done secretly. Advanced integrated circuit technology is inte- grated into these devices. Therefore, wiretaps are getting smaller and better than before. The newest device is tiny in size and light weight. This small size and weight is reflected in the increased number of wiretapping cases. Fortunately, most cases are resolved in time by the investigating authority. This paper will discuss personal experiences involving real counter mea- surement jobs rather than discussing the high technique of applications and implementations. By way of sharing experiences on some special cases, it will remind readers of possible job related consequences. However, it shall be kept in mind, eavesdrops do not necessarily use physical elements or high technology. Many of them modify the circuitry layout in the tele- phone set to achieve the purpose of listening. By picking up special prop- erties from regularly installed elements, nobody is able to visually rec- ognize the difference between normal and illegal telephone components. After all, signal transmission can be done by any possible method. This paper is going to describe some real cases of eavesdropping on a telephone set and show the results from a lab proving the feasibility of execution in the field. This presentation will be very helpful to people working in coun- termeasures who are analyzing a telephone bug. It will also be useful as a reference of procedures to do surveillance for finding equipment for eaves- dropping on telephone communication.

Surveillance, Telephone, Countermeasure

 ** Presenting Author*