Telephone Security Group

National Telecommunications Security Working Group Information Series

Executive Overview

January 1996

Table of Contents

Introduction

The Telephone Security Group (TSG) is a standing committee under the Facility Protection Committee, Security Policy Board, of the U.S. Government. The TSG's membership is made up of representatives from throughout the Executive and Judicial branches of the government and the Department of Defense. The TSG's charter is to provide security policy, procedures, and countermeasures direction for telephone and telecommunications systems employed within all sensitive information processing areas. The primary instrument for doing this is the series of documents published by the TSG, known as the TSG Standards.

The TSG Standards are written for technical security personnel and the telecommunications manufacturers who supply telephone equipment for use in sensitive information processing areas. The TSG has written this Executive Overview to provide the salient points and present them in a non-technical forum. It is important that managers at all levels become aware of the efforts required to provide adequate safeguards to real security concerns generated by today's telecommunications technology.

History of the Problem

Entities hostile to the U.S. government have spent countless hours and dollars searching for ways to collect intelligence information. They've developed elaborate schemes to cultivate human sources and produced sophisticated technical devices to be used to satisfy their collection requirements. However, none have been as simple, yet as fruitful, as the common telephone. The telephone is the device of choice because it contains all of the parts of a surveillance system; such as, a microphone, a wire line (connected to the microphone) leading out of the controlled area, and located in discussion areas. Furthermore, the information provided by a telephone is always in a ready to use form...the spoken word. More than 50% of all hostile attacks on U.S. offices, both foreign and domestic, have been through exploiting the common telephone. [1]

The Problem Today

Today's telephones are still under attack, only by a wider base of information collectors. It's true the iron curtain has fallen, but instead of the traditional foe who sought a military advantage, we're now faced with more than one hundred new threats from those who seek to gain an economic advantage over the US. Those entities are not just targeting the military, but our entire economic base including research and development, manufacturing, and marketing[2]. They are using more sophistication and outright malicious attacks to gain information. Our newspapers and trade journals are full of stories related to technology break-ins. Even our educational institutions are being infiltrated[3].

Typically, the perpetrators of today's technological security breaches are merely exploiting the power designed into our modern telecommunication systems. The methods used are intended (by the manufacturers) for beneficial purposes, such as custom calling features or for network maintenance purposes. Aside from the loss of information are huge dollar losses caused by toll fraud. Toll fraud is the intentional penetration of a telecommunications system for the purpose of using the service for personal monetary gain (without having the owners' permission). Toll fraud and system abuse is a $5 billion per year industry, of which, the companies who are victims carry the cost. The U.S. government has been the victim in more than a dozen reported cases, some topping the list of more than $12 million dollars per break-in. As reported by one industry specialist, "*it's not a matter of **if** you are a victim, but **when** you are a victim.*"[4]

What does this mean to you? It means that more people are attacking telephone and telecommunication systems than ever before. The methods being used are more effective and more damaging than ever seen in the past. The methods of exploiting these systems are the same, whether they're after secrets or toll fraud "*it's a matter of intent!"*[5] The impact to government and businesses alike is the loss of information and money!

How open is the System?

To better understand the scope of the telecommunications dilemma, let's refer to an example using today's jargon. The mainstream of all telecommunications world-wide is the *information super highway*, which is comprised of; international telephone, facsimile, televideo, telemarketing, banking, computer wide area networks, power grids, air traffic control, and government communications. All forms are commingled on the super highway by means of packetizing the information. These packets are placed onto, or taken from, the super highways by means of tributary roads. Individual users are connected via smaller lines equivalent to a driveway leading to a home. The roads and driveways, like the super highway, can be used by anyone. Any particular person or agency can be reached by merely knowing their address. In fact, the super highway even provides an on-line atlas whereby addresses can be instantly looked-up.

The information transported along the super highway is not afforded privacy by the system itself. Some users encrypt their information to prevent corruption or losses, but not everyone does. The telephone company does not ensure data privacy either. They only protect their ability to charge and collect for service (their revenue base). Therefore, the packets can be copied, re-routed, delayed, and read by almost anyone who understands how the system operates. Hence, the popular term, "*surfing the super highway*."

End user equipment (at the end of the driveway) can be *surfed* by almost anyone along the super highway, too! As a matter of fact, the network routinely queries (surfs) the health and availability of all subscribers. For example, before your home telephone rings with an incoming call, the distant telephone switch sends a call set-up message all the way to your location to ensure your telephone is on-hook, idle, available for a call, and compatible with the calling party's equipment. The same holds true for other forms of communications.

The information super highway is an open system architecture, where everybody is permitted to know how the system works.

The Open System's Contributions to the Problem

System openness, coupled with new telecommunications features, is being taken advantage of by the technically competent. It's analogous to riding a bicycle, *once you've learned you'll never forget*. Once a user learns how to navigate the super highway, or use a facet of the technology, the lessons learned are easily translated to other facets of the system. For example, a voice mail user learned how to use a company proprietary voice mail system and then used that knowledge to gain access to other voice mail systems. The information obtained from the exploited voice mail systems contained marketing leads from one of his company's competitors. This surfer turned market leads into company profits until he was caught and prosecuted.

Likewise, computerized telephone system users are learning the feature access codes of the system and using them to gain access and manipulate other computerized telephone systems[6]. The features being exploited are methods to activate speed dial list, call accounting records, hands-free telephone activations, and much more.

The open architecture and system features were never intended as a means to exploit these systems. They were engineered for convenience and maintenance, but the unscrupulous are turning them into criminal tools...tools that are being used in the international arena.

The TSG Standards and What They do for you

The TSG Standards prescribe the design, installation, and maintenance procedures for telecommunications equipment to be used in sensitive information processing areas. They provide a means to apply rational countermeasures to real-world problems. The standards are not necessarily applicable to all users, rather only those portions that provide guidance for the telecommunication systems (or components) employed within their areas. The methods prescribed within the Standards are effective against the loss of intelligence (information), as well as countering toll-fraud abuses. Toll fraud protection is not a formal part of the TSG charter; rather it is a *value added* benefit of a comprehensive telecommunications security program.

The provisions of the TSG Standards will be helpful to you when assessing the need for telecommunications security. They can be used to establish a baseline of the minimum telecommunications security requirements. The TSG Information Series *Computerized Telephone Systems (CTSs) - A Review of Deficiencies, Threats, and Risk* provides very detailed information specific to features, services, and countermeasures.

Summary

The issues surrounding telecommunications security are growing as fast as technology itself. The old concerns of telephone exploitation have grown exponentially with the advent of today's modern, feature-rich telecommunication systems. This is due in part to the computerization of telecommunications networks, and due to a consumer population hungry to learn and use today's technology. Technological advances have given birth to the information super highway, which is comprised of a mega-lane freeway, with thousands of side roads, and millions of driveways. Each tributary is connected to a plethora of telephone, facsimile, and computer devices, operated by an exhausting number of users. Some users are misusing the power and versatility of the open system architecture to create tools for criminal ill will. Opposing the efforts of those who are exploiting these systems stands yourself and your security staff. With the understanding gained through this paper, you can benefit from the security expertise and efforts of the entire TSG. The TSG Standards can provide you with the means to establish your telecommunications security baseline as required by some program protection plans. Ultimately you are responsible for implementing protective measures for your program areas, but you don't stand-alone. The TSG, in partnership with your telecommunications security staff, is striving to protect your assets, your money, your program, and our country.

---

1. *Records of Discoveries of Eavesdropping Installations and Technical Penetrations* (S) dated March 1991
2. *The National Security Threat List* (S) published periodically by the Federal Bureau of Investigations
3. *The Cuckoo's Nest* Cliff Stoll who thwarted the Hanover Hackers.
4. *MCI's Invisible Criminals*, a quote from Mr. Bruce Wells, MCI Corporate Security.
5. *Invasion of Privacy and 90's Technology*, by Paul F. Barry and Charles Wilkinson
6. AT&T's GBCS Products *Security Handbook* dated April 1994.