Testimony by Geoffrey S. Goodfellow

Before the Subcommittee on Transportation, Aviation and Materials
on the subject of Telecommunications Security and Privacy.

22 September 1983

1. Introduction

My name is Geoffrey S. Goodfellow. I am primarily employed by the Computer Science Laboratory at SRI International, Menlo Park, California. For the past 10 years at SRI, I have been involved in research efforts related with packet switched computer network communication systems, protocols and security technologies. I have also been involved in various operating and sub-system development projects. Currently, my responsibilities include a position as Principle Investigator of SRI's involvement in a Department of Defense program aimed at developing and proving secure computer systems, that operate at different security levels and communicate via networks. A detailed biography of my career from 7th grade school where I discovered computers (which eventually lead to my permanent abandonment of the formal educational system during high school) to how I got to where I am today with no degrees or any type of equivalency to my name is included at the end of my testimony.

I am a coauthor of *the Hacker's Dictionary -- A Guide to the World of Computer Wizards*, a new book being published this fall.

THE STATEMENTS INCLUDED HEREIN ARE MY OWN AND DO NOT NECESSARILY REPRESENT THOSE OF SRI INTERNATIONAL OR ANY CLIENTS OF SRI.

2. The Nature of Computer Hackers and Hacking.

The primary nature of a computer hacker can be defined as follows:

- A person who enjoys learning or knowing the details of computer systems and how to stretch their capabilities, as opposed to most users of computers, who prefer to learn or know only the minimum amount necessary in order to get their job done.

- One who programs computers enthusiastically, for the sheer fun of it, and gets a non professional amount of enjoyment out of using them.

- A person capable of appreciating the irony and beauty (i.e. 'hack value') of a program.

- A person who is good at programming quickly or is an expert on a particular program. *(This definition and the proceeding ones are correlated, and people who fit them congregate).*

Unfortunately, though, hacking has an unsavory faction to it:

- A malicious or inquisitive meddler (i.e. 'poacher') who tries to discover information by poking around. For example, a "password hacker" is one who tries, possibly by deceptive or illegal means, to discover other people's computer passwords. A "network hacker" is one who tries to learn about the computer network (possibly because he wants to interfere--one can tell the difference only by context, tone of voice and manner of approach).

Hackers of all factions, whether benign or of the unsavory flavor, consider themselves somewhat of an elite, though one to which new members are gladly welcome. Hacking is meritocracy based on ability. There is a certain self-satisfaction in identifying yourself as a hacker *(but if you claim to be one and are not, you'll quickly be labelled 'bogus').*

The hacker is intensely interested in technology and is a very inquisitive person. Many are social outcasts who don't enjoy the same things as most other kids their age. Hackers of the unsavory flavor are a very curious breed of individual -- many can best be described as loners looking for someone to appreciate their talents. They know full well that what they're doing errs on the 'dark side *(of the force)*' -- to coin a phrase. Unsavory hackers want to get caught so they can be given the appreciation they desire -- and the process of getting caught adds an essence of thrill to their endeavor.

I would like to state for the record, that benign hackers, such as I, deplore the unsanctioned entry and subsequent rummaging of mainframe computer systems and networks. These types of activities are tarnishing the profession of hacking and giving it a bad name.

In the *Real World*, computer system organizations are generally run like totalitarian police states. This unfortunate reality fosters resentment in hackers and a desire to challenge the reverence of authority develops. As a result, the way hackers bring themselves to a system managers attention is via the medium they know and relate to best: a terminal and modem and your computer system. In most cases, the hacker wouldn't personally think of or know how to go about calling up the director of a computer system and offering his services to you as a bright young guy for the fear of reprisals or not being taken seriously. Instead, they choose to 'introduce' you to them by meddling with your computer system, cavalierly circumventing security and protection mechanisms, in order to satiate their hunger for knowledge and develop an understanding of how things work.

The organization will respond in kind by trying to 'plug the leak' of an intrusion into their system by erecting barriers. This type of reaction is precisely the wrong approach to take, because the hacker will notice the beefed-up defenses and see them as a further challenge of his prowess and ingenuity and legitimate users are subjected to greater inconvenience.

Instead, what an organization should do is try to befriend hackers which have penetrated their inner sanctums. The perspective that should be taken is one of *"Is it helpful or useful for you to do this?"* rather than *"Are you authorized to do this?"*. You must in effect come down to the hackers level and circulate among them. Show them that you appreciate their talents. If you ask them nonforeboding questions and take a genuine interest in what they're doing, most of the time you'll find they're more than happy to tell you exactly what it is they're looking for or interested in. The hacker wants to learn and you can be their guide/teacher. This is how I was dealt with by the firm that caught me during my unsavory hacking days in 1973 when I breached security on a large commercial timesharing network and many of its host computer systems. I was very much inspired by this method of catching and steering unsavory hackers towards more constructive use of their talents.

3. What Can and Should Be Done to Help Abate The Unsavory Hacking Problem?

From my own observations and inspections of systems and from what I have been reading in the press, I have come to the conclusion that computer site administrators are not taking reasonable and prudent measures to protect their computer systems from even the most casual methods of circumvention. A rather egregious example of this would be the installation of which the 414s allegedly logged into with username "test" and password "test". Usernames and passwords of this sort are not uncommon and sites which set up logins like this are just asking for a break in -- just as someone who would leave a key in the lock on the front door of their house, complete with the WELCOME! mat out for all to see, invites the casual burglar.

The way I view 'reasonable and prudent' measures of protection from the *casual* penetration is by drawing a paradigm with the way DoD classified information is handled.

With respect to the handling and use of classified information, it is the responsibility of the organization to which you belong, in conformance with DoD guidelines, to provide you with rules and regulations in the handling of classified information. It is also the responsibility of your organization to provide you with a safe place (i.e. a vault) to store said information and to provide adequate safeguards (such as alarm systems, security personnel and patrols) to prevent unauthorized access.

The same methodology should be taken to heart by administrators of computer systems. It's their responsibility to provide reasonable and prudent measures to prevent unauthorized access attempts from gaining access to the system. This means a few very basic things like:

- Forcing users to choose reasonable passwords - not their spouse's name or their dog's name.
- Setting up proper modem controls on dial-up/remote access ports so that disconnection causes any jobs (or trojan horses left on the port) to be flushed and results in resetting the port to not-logged in status.
- Reporting incorrect password attempts to the system console or log file.
- Causing line disconnection after a few successively repeated incorrect password attempts.
- Using encrypted passwords, so it is not possible to compromise an entire systems password list when circumvention of a systems protection mechanisms is attained. This is analogous to the DoD's *compartmentalization* of information -- so a breach in one area does not sacrifice security in all areas.

The second facet of the paradigm is the users' responsibility. I don't go out to lunch and leave my secrets sitting on my desk. I put them in a vault. And I don't go throwing them over the embassy walls. So it is the same for the computer system user. It is the users responsibility to choose reasonable passwords and not leave them written down anywhere, such as on their desk blotter or white board or to pass them out to others.

The third matter is a paradigm of a different nature. This has to do with socially acceptable values. Namely, when I was brought up, I was taught about trespassing. If I went to someone's house and found the front door is wide open, I don't really know of anyone who would walk right in and look around.

They would instead stand at the door, ring the doorbell or knock or call out. This type of responsibility or sense of morals has to be applied to the computer technology field.

Research into methods of improving the safeguarding of information flow through technology should be pursued. One such project is the one of which I am the Principle Investigator of at SRI, which has to do with this type of technology. Our involvement has to do with developing and proving technologies that will absolutely assure that I will only have access to information in a computer system database of which my clearance and my 'need to know' entitles me too, while prohibiting me from information I am not cleared or permitted to access. However, one must carefully weigh the value of increased security with the cost in user convenience and flexibility.

Explicit federal and state criminal statutes should be enacted to allow a vehicle for vigorous prosecution, should it be warranted or desired, by injured parties. These explicit laws would also hopefully act as a method of deterrence.

4. Let Us Not Lull Ourselves into a False Sense of Security.

In general unsanctioned computer system penetrations can be performed by individuals who possess three basic aspects of computer knowledge: access, skill and information.

Access can be defined as a terminal and modem. Skill can be defined as ingenuity or familiarity with computer systems, especially with the given system type that the penetration is directed towards. Information can be defined as dial-up phone numbers, network address or means of accessing a given computer system -- perhaps even physical. Information can also include various methods, most likely in the form of 'bugs' (i.e. shortcomings) or 'features' (i.e. an aspect inherent to the hardware or software design of the system) which will permit the holder to circumvent the operating system security and protection mechanisms, and in effect gain *carte blanche* access to the computer. *Carte blanche* can be defined as allowing the holder to override file security and protection considerations, in that you can read or alter any data and even change the nature of the computer operating system software itself.

In the *good ol' days* such skill and information was not widely known. However, with the ever increasing number of computer systems, both personal and mainframe alike, information and skill is spreading to an ever increasing number of individuals and institutions. Unfortunately, not all of the individuals are as scrupulous as they should be. Such instruments as 'Pirate Bulletin Board' systems are being used to disseminate this information on a nationwide, on-call, as needed basis.

What does this mean?

Up until now most unsanctioned computer system penetrations have not been the high technological acts of chicanery the media has made them out to be. They were primarily performed by individuals who were as familiar with computer technology as, say, an auto enthusiast is with what goes on under the hood of your car. The 'auto whiz' has the breadth of knowledge necessary to 'hot wire' a motor vehicle, just as your computer literate individual has the breadth to necessary to perform a technological 'hot wire' inside a computer system.

However, the current low to medium technological approaches to system penetrations are likely to change.

I define the technological levels as follows: *high tech* is defined as a new method of circumvention. High tech methods are primarily invented by individuals or a group of individuals who have an in depth understanding of the desired technology the caper is directed against. *Medium tech* can be defined as an

individual who has the same basic level of understanding as the high tech guy, but uses the knowledge and perhaps fine tunes or refines it a bit (i.e. the medium tech individual is a knowledgeable user). The *low tech* individual is just a user of the knowledge with little or no understanding of what is involved in making the technology perform its desired function.

In the not to distant future with higher stakes, increased levels of knowledge and other aspects better understood, I believe we will see a trend towards a more 'higher tech' level of system penetrations and circumventions. These capers will be harder to detect and deter.

The further development of *formal specification* and *verification techniques* and associated technologies will permit the system developers, reviewers or specifier himself to verify that a given system specification is consistent with a given model of desired operation.

5. Recommendations

In conclusion, I would like to say that I believe the scale of the hacking problem is going to escalate dramatically as more of the technology makes its way into the mass market. There is no one easy solution to these problems. The directions that need to be taken are technological, ethical/moral and social. Hopefully an increased awareness of the vulnerability of our systems to penetration and circumvention will allow us to see the light, in the form of solutions, at the end of the tunnel. And hopefully that light, is not a train.

6. Biography *(The Making of a Hacker)*

My first experience with computers (and the world of 'hacking') manifested itself during my 7th grade school when I discovered a room full of teletypes connected to a computer system at Stanford University which offered Computer Assisted Instruction/drill programs.

Having discovered 'The Computer Room', I started arriving at school early each day to be able to play with them. I would also spend the lunch hour, recess and as long as I could after school in the computer room, as well.

Luckily, that summer I was permitted to hang-out at the Stanford facility which had the computer system that served our school and others. This allowed me the opportunity to interact with the system designers and learn how everything worked. At the facility, I quickly began to develop a keen interest in system-level software, such as the operating system and privileged type programs which only 'the wizards' could run or know the inner workings of. However, I did not let this fact keep me from learning about the system.

During the 8th grade, my parents wishing to contribute to their son's apparent avid absorption of computer technology, procured a used teletype machine and modem from a large time-sharing computer firm. I don't know how, but in the process, they managed to talk the firm out of 'free' account for after hours and weekend use. The firm then promptly forgot about me. After running the usual course of computer games, which quickly became quite boring, my attention turned towards the operating system and its protection mechanism, which I took delight in finding ways around. This of course, was noticed by the time-sharing company and one summer evening, after they were sure it was me inside their system, their vice president and district manager came knocking at our door, and in effect said, "gotcha!". The result of being caught was that I was hired for the summer to help them make their system more secure and plug the holes that I had uncovered in my wanderings.

While employed for the summer, 1973, I chanced to meet up with another summer hire who had done some work at NASA-AMES and had knowledge of a Department of Defense computer network, called the ARPANET, which linked together computers all over the country at various research establishments, universities and military bases. My new-found friend passed me a dial-up number, and on a scrap of paper, wrote a few commands that would allow me to connect up to various systems on the network.

In these early days of the ARPANET (which pioneered packet switching technology, a method for allowing computers of different flavors and types to 'talk' to one-another), the majority of the computers had 'guest' accounts on them with purposefully obvious and published passwords. This was done in order to promote the free use of resources at other host systems and to let users of the network have a chance to explore, learn and use said systems.

Needless to say, this was a gold mine that no hacker, such as myself, could pass up. So I spent the better part of the summer learning and using as many different computer systems as possible, all over the country.

One of my favorite systems to use was the guest login account on a host called SRI-AI, a PDP-10 running the Tenex operating system, which belonged to the Stanford Research Institute's Artificial Intelligence Center. I thought it nice to have a system right in my very own home town. I made it a point to get to know the operations of this system as well as I could in hopes that perhaps someday I might have a login account of my own to use and it would be nice to be familiar with it in such an event.

Well, that day came when, as usual, I logged into the public guest account, and out popped a message of the form "Welcome to the SRI-AI computer public guest account. If you think you have a need for your own account, send a note (with the on-line electronic mail program, of course) to the system administrator, explaining your need."

Such an invitation was just to good to pass up and having my very own login account is something I had dreamed about. So, I took it upon myself to send a message saying I was a hacker who had been spending time on the public guest account learning about their system and wanted to have an increased level of access and login area of my own to store files. In return, I would freely help improve the systems capabilities thru my hacking.

After some initial trepidation on the part of the systems administrator was overcome, my account was granted. This allowed me to make SRI-AI my home base of network operations. I immediately proceeded to hack away to my heart's content, now that, in effect, I had become a legitimate network user.

After demonstrating my competence and some semblance of responsibility, I was granted system privileges (i.e. *carte blanche* access to all system resources). This permitted me to learn and develop a further understanding of the system.

So, I hung around SRI for about 9 months. I was given a building pass, so as to have physical as well as electronic (remote) access to the computer systems. This allowed me to come and go at odd hours, which are the hours hackers are best known to keep.

Then, there was an opening for a part-time weekend computer operator's job, and since I had demonstrated my competence, I was immediately hired for the position. I was now in my senior year of high school, and as a result of my increased access to computers, my grade average followed the typical hacker curve, i.e. down. until, two weeks into the final quarter of my senior year in high school, I dropped out, and became full-time at SRI. I have never returned to a classroom since the day I left school in 1974.