Parts 1-3

```
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
*=*=*        Government Computer Security Techniques       *=*=
*=*=*=*=*=*=*      Written By: The Line Breaker     *=*=*=*=*=*=
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
```

As most of you know (those who have been around for over 1 year), I am a computer security consultant by trade. I do work for most large companies and sometimes the government. Well I am here now going to explain in great detail the fundamentals of government computer security. There are going to be roughly 25 sections to this g-phile, so open your buffers and let them rip.

Each file is broken into several parts starting with the control title and ending with the principles of note. I help design most of the systems that you are about to read about, and most of the problems that you run across in your every day hacking should be solved here. The secret to the philes is to read them carefully and then reverse the process in some cases, otherwise they will help you understand in greater detail the workings of computer security.

```
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
*=*=*            C.S.T. Volume One -- G-phile One          *=*=
*=*=*=*=*=*=*        Written By: The Line Breaker     *=*=*=*=*=*=
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
```

Control Title: Low Building Profile

Description -> buildings housing computer systems and the computer facilities should be unobtrusive and give minimum indication of their purpose. There should be no obvious signs identifying computing activities outside or inside buildings. Buildings should look unimpressive and ordinary relative to nearby buildings. Building lobby directories and company telephone books should not identify locations of computer activities except for offices and reception areas that serve outsiders and are located separately from operational areas. Physical access barriers, including access control signs, should be reasonably visible, however.

Strengths -> a low profile reduces the likelihood of attention by destruction-minded outsiders. Such attention tends to be directed away to other more visible targets.

Weaknesses -> a low profile may reduce business promotion values and inconvenience visitors, vendors, delivery people, and others

who have a legitimate need to find computing facilities.

Purpose -> deterrence

Control Area -> computer center

Mode -> manual procedure

Area of Responsibility -> management, security

Cost - low

Principles of Note -> avoidance of need for design secrecy, completeness and consistency, least privileged
*=

*=
==*   C.S.T. Volume One -- Phile Two   *=*=
==*=*=*=*=*   Written By: The Line Breaker   *=*=*=*=*=*=
*=

Control Title -> telephone access

Objective -> avoid computer access exposure

Description -> limiting access to a computer and data files can be an important means of security. Several means of accomplishing this are possible. It may be possible and important to eliminate dial-up access to a computer. A computer interfaced to the dial-up public telephone network is exposed to access from any telephone in the world. There may be a trade-off in computer security by giving up or limiting the benefits of dial-up access. This can be accomplished by using only point-to-point wire or leased-line telephone access to the computer. An alternative is to provide dial-up access to a small computer for development or other timesharing purposes while reserving another computer for more sensitive production activity that is not interfaced to dial-up telephones. A control computer providing access to two or more other computers can also be used as a means of protecting them from dial-up access. An alternative method of restricting access is to provide for dial-up access at limited periods of time of day. During periods of dial-up access, particularly sensitive files or applications would not be resident in the computer system or secondary storage. A partial degree of protection for dial-up access systems is to maintain strict need-to-know availability of the telephone numbers and log-in protocol for accessing the

computer system. Most dial-up timesharing computer services have similar access protocols; therefore, a unique, very different initial access exchange of identifying information may be useful to limit access. The telephone numbers should be unlisted, different in pattern of digits, and have different prefixes from voice telephone numbers for the organizations that are publicly listed. Call back to verifying the source of telephone access is also popular.

Strengths -> avoidance of exposure is a particularly strong means of simplifying and reducing the problems of securing computer systems. Limiting or eliminating dial-up access significantly reduces exposure.

Weakness -> an important objective for computers is to make them easily and widely accessible. Eliminating or limiting dial-up significantly reduces this capability.

How to Audit -> access capabilities, review access logs

Purpose -> prevention

Control Area -> computer system

Mode -> hardware

Area of Responsibility -> operation

Cost -> high

Principles of Note -> least privilege, limit dependence on other mechanisms

```
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
*=*=*            C.S.T. Volume One -- Phile Three           *=*=
*=*=*=*=*=*=*      Written By: The Line Breaker     *=*=*=*=*=*=
*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=
```

Control Title -> limit transaction privileges from terminal

Objective -> prevent loss or destruction of assets, prevent unauthorized browsing of systems files, prevent "hacking", prevent system crashes caused by unauthorized use of certain system commands

Description -> in addition to controlling resources (files, off-line data storage volumes, etc.), the transactions that a particular user is permitted to initiate are limited. What the system commands that a user can use or is informed of is controlled by the user's job duties. Thus, the system's level and application command, such as reporting who is currently logged into the system, are restricted on a need-to-know basis. Logs may be kept for all attempts to use an authorized system command; this can be used to determine who needs training or perhaps disciplinary action.

Strengths -> prevents users from performing unauthorized acts, including examination of files names of other users and other system-related commands. Without these systems transactions, compromise of the operating system and other such abuses are made significantly harder to accomplish. Because the system commands are monitored and controlled by the computer, they can be sustained and enforced.

Weaknesses -> may unduly restrict users' ability to perform their jobs, especially if the users are programmers. Undue restriction may result in reduced productivity and increased levels of frustration. Determination of what commands should be restricted may be involved and time consuming.

How to Audit -> examine system commands permitted for certain groups of users for reasonableness. Review request for changes in systems command privileges for authorization and need. If available, examine logs for unauthorized attempts to use systems commands that certain users are not permitted to use.

Purpose -> prevention

Control Area -> computer system

Mode -> computer operating system, computer application system

Area of Responsibility -> operations management

Cost -> medium

Principles of Note -> simplicity, least privilege, independence of control and subject, substantiality