CSC-EPL-88/007

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

COMPUTER ACCESSORIES INC.

PRIVATE ACCESS

26 April 1988

SUBSYSTEM EVALUATION REPORT

COMPUTER ACCESSORIES INC

PRIVATE ACCESS

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

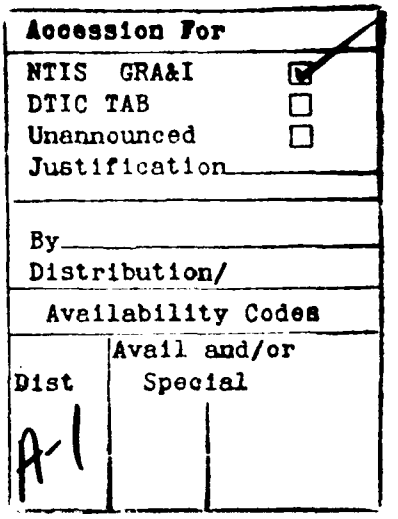
FOREWORD

This publication, the Subsystem Evaluation Report of Private Access, made by Computer Accessories Inc, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of an evaluation of Computer Accessories Private Access product. The requirements stated in this report are taken from *Department of Defense Trusted Computer System Evaluation Criteria* dated December 1985.

Approved:

April 26, 1988

Eliot Sohmer
Chief, Evaluations, Publications, and Support
National Computer Security Center



ACKNOWLEDGEMENTS

Evaluation Team Members

Stephen D. Schneider

Cleo M. Andrus

Richard A. Humphreys

National Computer Security Center
9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The product Private Access has been evaluated by the National Computer Security Center (NCSC). Private Access is considered to be a subsystem, rather than a complete trusted computer system, and therefore it was evaluated against a relevant subset of the security requirements in the *Department of Defense Trusted Computer System Evaluation Criteria*, dated December 1985, here after referred to as the "Criteria". The subsets for this product include Identification and Authentication (I&A) and Audit.

The NCSC evaluation team has determined that Private Access applies these security features to any system that uses standard, dialup telephone lines for access to its systems. Private Access can protect one Personal Computer from unauthorized access over a single telephone line. No security is provided for local operation. Private Access uses a variable password and fixed callback procedures to guarantee the authenticity of users and their location. Additionally, Private Access has time of use restrictions and an audit of I&A actions. Private Access will "turn on" its host system giving an authorized user complete control over the host computer. The remote access feature, used in conjunction with software not provided by the company, will allow the remote user to run the host computer without returning system control to the host. (This return to the default terminal occurs with some program calls). Private Access will power down the system if an illegal access attempt is made. A limit of 100 user ID's/Passwords may be assigned. Privileged users can modify the trusted secure data base remotely.

Private Access is a stand-alone device (roughly the size of a modem) whose security mechanisms are secure from electronic tampering as long as system passwords remain secure.

Because this is a subsystem, it is not capable of protecting information with such assurance that classified information may be maintained on a system protected only by this system. Neither may Private Access be used to upgrade the protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. Private Access may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. Managers should note that subsystems are not capable of protecting information with such assurance that classified information may be maintained on a system protected only by subsystems. Neither may subsystems be used to upgrade the protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

Subsystems considered in the program are special-purpose products that can be added to existing computer systems to increase security and implement a security feature from the TCSEC. They

also have the potential of meeting the limited security needs of both civilian and government departments and agencies. The scope of a computer security subsystem evaluation is limited to consideration of the subsystem and the attached system, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an assessment is made of a subsystem's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

Private Access is a stand-alone device (roughly the size of a modem) which is connected by RS-232C configured cables between the Personal Computer and the modem. Each Private Access can protect one Personal Computer from unauthorized access over a single telephone line. It does, in effect stand as a security wall between the telephone system and the computer. No security is provided for local operation. When in "remote mode" it will sense that the modem is receiving a call and prevent access to the personal computer until the caller has been verified by Private Access. Verification is accomplished through the use of an ID and Password and, optionally, a call-back. "Super Users" (those with 'system' passwords and system administrator capabilities) can modify the access privileges from remote locations. Additionally, Private Access has time of use restrictions and an extensive audit of identification and authentication activities. Private Access has the ability to "power up" its host computer when an authenticated user calls. That user then may be given complete control over the host computer. Control is passed from the host's console and keyboard, through the communications ports to the remote caller's computer. Additional software is required to fully utilize the range of control features; this is not brought out in the literature. Up to 100 different user ID's/passwords can be assigned; in large companies this number may not be adequate.

Evaluation of Functionality

This section describes the performance of Private Access. The unit furnished by the company, successfully demonstrated all of the capabilities outlined in the Operators' Manual. The Private Access unit is installed between the host modem and computer during the initial equipment configuration. The configuration section includes instructions on all cable connections, modem Dual-In-Line Package (DIP) switch settings, and communications software initialization. After equipment installation the System administrator must activate the Private Access Configuration Mode to correctly prepare the unit memory. After all the preceeding steps have been completed, Private Access will provide identification, authentication, and auditing of those I & A mechanisms. Subject to Private Access' security features, a remote terminal can then gain access to the host computer terminal over the telephone lines. Private Access does not control or audit local powerup and access. The initial equipment installation is straightforward and all connectors are conveniently located on the back of the Private Access unit.

Operational Modes

Private Access has three basic operational modes: The Local Mode, the Remote Mode, and the Configuration Mode. The "Remote" switch, located on the front panel, transfers operation between the three modes. Momentarily depressing the Remote switch toggles operation between the Local

and Remote Modes. The Local Mode is indicated by the "Remote" LED being off. The Remote Mode is indicated by the "Remote" LED being on. The most powerful feature of this product is the remote access power on/power off capability. This feature allows a remote user to initiate a local program which executes a set of commands and then powers down the system when the job is finished. To perform useful work via remote access, additional software purchases are required.

Local Mode

This mode permits normal on-site use of the computer and its communication capabilities, but provides no system security. Power is applied to the host computer from the rear panel power recepticals of Private Access by toggling the "Remote" switch. After this sequence Private Access becomes transparent to any modem communication. Once in the local mode, Private Access does not interfere with normal modem operation. This is the same as turning security off. From the local mode a Super User can access the Configuration Mode (see description below.) When ending a "Local Mode" session, toggling the Remote Mode switch causes Private Access to remove power to the host after a set delay time (default = one minute). Physical security of the local equipment is required to ensure system security.

Remote Mode

Once in Remote Mode, Private Access monitors the modem for detection of a ring signal. Remote Mode operation allows for access to the host computer from a remote location. After detection of a ring, Private Access initiates a local computer powerup sequence. The unit then requests the user's ID and Password. If the user name, password and access time match the information stored in the Private Access database, then the requestor is granted access to the computer. Private Access becomes "transparent" and the user's terminal communicates directly with the host PC thru the communications port. There is no audit of authorized user actions. The user may execute standard DOS commands from this port and see the results on his remote terminal. Tailored software packages must reside on the host computer for the remote user to run applications under DOS. This is because the application, once given control by DOS sends its output to the default terminal, which is the host terminal. The lack of even a minimal audit on authorized users is a weakness if the authorized user is performing an unauthorized act.

Configuration Mode

This mode is entered in order to program or review Private Access parameters and logs. The configuration mode is entered locally by depressing the Remote switch for approximately 3 seconds. The configuration mode is entered from a remote terminal, after a valid logon, by pressing three consecutive percent signs, %%%. The "on" LED will blink while the configration mode is invoked. The power of this function is most dramatically demonstrated through access by a Super User, the equivilent of a system administrator. The Super User has access to the complete range of

functionality Private Access offers. The Super User is allowed to change audit data and give or deny access of the host computer to any other user, in short, to control the full range of capabilities. However, when the average user goes into the configuration mode, he is given a very limited subset of Private Access functions.

Features

The remote power control feature allows the user to turn the host computer power on and off from a remote location through a modem. It is the opinion of this evaluator that this is the most powerful feature of the product.

The Operator's Manual defines three security features available in this product; user identification, password authentication and callback. User identification and password security, when combined, meet some requirements of the Trusted Computer System Evaluation Criteria for Identification and Authentication. It was clearly demonstrated that the callback feature as outlined in the Operator's Manual worked correctly. However, there is an innate weakness in the callback feature as applied to computer security. Private Access only controls one telephone line, therefore, it must return calls on the same line as called in on. Under these conditions single line fixed callback can be easily defeated by the caller and should therefore not be used as the authentication technique. However, it does add an additional level of assurance when used in conjunction with user ID and a password. All three features increase the security assurance this product provides.

Private Access provides a thorough audit record of all remote accesses to the host computer. Audit data can be displayed in several areas; the Complete Activity Log, the Legal Access Log, and the Illegal Access Log. The Complete Activity Log as the name implies contains information on all login attempts. It also has the number of the transaction, user ID, an invalid password if attempted, date on/off, time on/off, and seven flags (R,C,V,U,P,A, and L). The flags indicates remote access, configuration mode entered, valid access, invalid user ID, invalid password attempt, incorrect access time, and whether or not the user's ID was locked-out at access attempt. The other two logs display similar data for their respective topics. The Legal Access Log maintains an audit trail that consists of a log of the machine's usage. The Illegal Access Log maintains a record of failed access attempts, thus providing the system operator with the capability of detecting unauthorized attempts to access the machine. Private Access can log up to 175 combined accesses and access attempts. If more than 175 accesses or access attempts occur before clearing the log, subsequent accesses are logged as event #175 and the previous entry in this location is overwritten. The overwrite feature diminishes the assurance this product offers.

Evaluation of Documentation

The Private Access documentation consists of a 45 page Operator's Manual, which has four sections and five appendices. This document was designed for use with three different models: L20, P157, and L10. The documentation begins with an introduction to the equipment in section one and a description of the three different product models. Section two of the manual describes start-up procedures. This section of the documentation could have been more specific in it's discussion of the setup procedures. Additional software is needed to run programs resident on the host computer from a remote location and the Operator's Manual does not highlight that issue. The third section of the documentation outlines the remote communications function of Private Access. This function works well with most commercially available communication packages. The fourth section discusses the Main Menu and its use. The final section of the document houses the appendices. Included in the appendices is the FCC statement, trademark information, unit specifications, control keys, and skip menu codes.

Private Access Operator's Manual

Section 1: The "Introduction" section discusses the use of the Operator's Manual, conventions used in the manual, operational modes, user profiles, and equipment features.

Section 2: "Getting Started" describes initial system setup including cables required, DIP switch settings, communication software settings, passwords and initial Super User identification.

Section 3: The "Remote Communication" section highlights the communication software set up, remote access, remote configuration, user main menu, and callback procedures for the remote user.

Section 4: The "Main Menu" section discusses use of the menus. All the menus are explained in this chapter. All the facilities of the system can be modified thru the menus concerning powerups, user access times, passwords, and communication parameters. In addition there are many menus available just for reviewing system activity and settings.

Appendices: The "Appendices" section of the documentation contain; the FCC statement, trademark information, unit specifications, control keys, and skip menu codes. This information resides in five appendices A through E.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data stored on these systems. Initially, protection was provided solely by the individual who maintained physical possession of his own data and operating system on diskettes, resulting in a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access due to other users' data. Other security mechanisms were not deemed necessary since the user was only able to inflict damage to his own data or operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In a working environment where it was common to have many users share the same workstation, they now shared and stored their data on the same hard disk memory unit. In this environment, users no longer had the assurance that their data was protected from unauthorized access, or even that the underlying operation system had not been subverted. Procedural controls could no longer provide the adequate user isolation and controlled sharing necessary for this environment.

Private Access model L20 is designed to help add assurance in the protection of the host terminal. When configured as tested, Private Access provides identification & authentication of remote access, callback, and auditing of I&A mechanisms. Once the host terminal has been reached using the documented software the user is relatively limited with respect to what can be accomplished from the remote terminal. Standard DOS commands such as, delete, type, and various directory commands can be executed from the remote terminal. However, remotely called programs cannot be run without using additional software to keep the called program from turning keyboard control of the host computer back over to the host itself.

PRODUCT TESTING

Test Procedure

Testing represents a significant portion of a subsystem evaluation. The test suite used by the evaluation team tested Private Access for identification & authentication of remote access, fixed callback, and auditing of I&A. The functional test suite focused upon those security features identified in the Private Access Operator's Manual, 1986. The test suite consisted of five parts. The first part tested that all the functions available to the system operator functioned as documented. The User Profile and the Complete User Activity Log were then filled to see how these conditions would be handled. The third part tested Private Access's ability to control I&A; user access, logout and lockout. The callback functions were tested to establish their capabilities. The final part tested the ability of the remote user to run DOS commands on the host computer.

Most tests were performed using a Model L20, Stand Alone Private Access, set up between two desktop computers connected via RS-232C standard connections and a null modem cable. The host computer system disk included a software batch file program to implement the DOS commands necessary to link the two systems. This allowed the distant terminal using a communications package to issue DOS commands directly to the host computer. After all local and remote testing not requiring the callback feature was completed, the system was reconfigured to use actual modems and telephone lines. This made it possible to check out the callback functions which could not be tested using the direct connect method.

Test Results

This section will describe the testing results of Computer Accessories' Private Access, which was configured as described in the Testing Procedure section.

Configuration Mode

Each of the menu's were checked and all of the options tested to see if they worked as stated in the documentation. All worked as documented with the exception of the "Identify Super User Authorizations Menu". This menu when exiting purportedly returned the super user to the "Main Menu" but instead returned to the "Modify User Authorizations Menu". This caused no problem because from here the "Main Menu" could easily be reached. During this portion of the testing the "Save All Parameters" and "Load All System Parameters" options were tested and performed as documented while using CROSSTALK, one of the Operator's Manual suggested communications packages, but did not fare as well when using other communications packages. When using KERMIT to save the system parameters there was no easy way to capture the information. It was necessary to go in and delete all information captured up to the beginning of system parameters.

Local Mode

While in the local mode Private Access does not provide any security to the host computer. However, a super user can enter the Configuration Mode and while there a limited amount of auditing will be done. The auditing consists of entries to the Complete Activity Log only. To maintain system assurance, physical security should be provided around the local equipment.

Remote Mode

The Identification and Authentication mechanism performed as documented; no valid access was allowed to the host terminal without first entering a valid identification and password. The option exists to require only an identification but this option is not recommended.

The callback feature operated correctly when configured as documented. Both the fixed callback and variable callback sequence functioned properly during testing.

The audit mechanism operated correctly. The team found that every time a user attempted to log on an audit record was created under each user's ID. The record lists any incorrect passwords given and both the date and time of the log on and log off. In addition to the basic audit information one option presented a table listing seven possible audit flags. The flags are set to indicate whether or not remote or configuration mode was entered, and the validity of the access attempt. If access is denied, this is displayed as well as the reason for the denial. Reasons for denial include bad password, access attempt beyond time slot, and user locked out. All of the above are located in the "Complete Activity Log" while subsets of this are included in "Legal Access Log" and the "Illegal Attempts Log". All of the logs contained accurate information on the traffic through Private Access including accesses to the configuration mode.

A very good feature of this unit is its identification and authentication method. When an incorrect ID is entered the password is still requested before access is denied. This in conjunction with the auditing of illegal access attempts allows the system operator to identify the presence of a security threat and simultaneously discourages "hackers". Private Access proved to work satisfactorily in all respects.

In summation, Private Access does provide a useful and effective user identification and authentication capability to host systems lacking such a feature. The fixed callback provides another layer to the security already provided. Its audit mechanism is reliable. The product is able to uniquely identify each system user and the system protects its own authentication data from unauthorized access, through the use of authorization logs. The proper operation of all equipment functions was rigorously tested by a thorough test suite.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b RESTRICTIVE MARKINGS None
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; Distribution Unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-88/007	5 MONITORING ORGANIZATION REPORT NUMBER(S) S231,242
6a NAME OF PERFORMING ORGANIZATION **National Computer Security Center** 6b OFFICE SYMBOL (If applicable) C12	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (*City, State and ZIP Code*) **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	7b ADDRESS (*City, State and ZIP Code*)
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State and ZIP Code*)	10 SOURCE OF FUNDING NOS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO
11 TITLE (*Include Security Classification*) (U) Subsystem Eval Report - Computer Accessories Inc Private Access	
12 PERSONAL AUTHOR(S) Schneider, Stephen; Andrus, Cleo; Humphreys, Richard	
13a TYPE OF REPORT Final 13b TIME COVERED FROM TO	14 DATE OF REPORT (*Yr, Mo., Day*) 880426 15 PAGE COUNT 19
16 SUPPLEMENTARY NOTATION	
17 COSATI CODES FIELD / GROUP / SUB GR	18 SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*) Private Access NCSC TCSEC Criteria I&A audit

19 ABSTRACT (*Continue on reverse side if necessary and identify by block number*)

Private Access is a stand-alone device which is connected by RS-232C configured cables between the PC and the modem. Each Private Access can protect one PC from unauthorized access over a single telephone line. This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21 ABSTRACT SECURITY CLASSIFICATION **UNCLASSIFIED**
22a NAME OF RESPONSIBLE INDIVIDUAL DENNIS E. SIRBAUGH	22b TELEPHONE NUMBER (Include Area Code) (301)859-4458 22c OFFICE SYMBOL C12

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE