The Rainbow Books

CSC-STD-002-85

DEPARTMENT OF DEFENSE

PASSWORD MANAGEMENT

GUIDELINE

Approved for public release;
distribution limited.

12 April 1985

DEPARTMENT OF DEFENSE
COMPUTER SECURITY CENTER
Fort George G. Meade, Maryland 20755

CSC-STD-002-85
Library No. S-226,994

FOREWORD

DataDome Ex. 1012, p. 1
DataDome v. Arkose Labs
IPR2025-00694

This publication, "Department of Defense Password management Guideline," is being issued by the DoD Computer Security Center (DoDCSC) under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The guidelines described in this document provide a set of good practices elated to the use of password-based user authentication mechanisms in automatic data processing systems employed for processing classified and other sensitive information. Point of contact concerning this publication is the Office of Standards and Products, Attention: Chief, Computer Security Standards.

Robert L. Brotman 12 April 1985
Director
DoD Computer Security Center

ACKNOWLEDGMENTS

Special recognition is extended to Sheila L. Brand, DoD Computer Security Center (DoDCSC), and Jeffrey D. Makey, formerly DoDCSC, as principal authors of this publication.

Acknowledgment is also given for the contributions of: Daniel J. Edwards, Mary E. Flaherty, Steven J. Padilla, DoDCSC, John J. Stasak III, Gregory L. Wessel and Bernard Peters, Department of Defense, Col. Roger R. Schell, formerly DoDCSC, and James P. Anderson, James P. Anderson & Co, who gave generously of their time and expertise in the formulation and review of this document.

DataDome Ex. 1012, p. 2
DataDome v. Arkose Labs
IPR2025-00694

CONTENTS

FOREWORD..... i
ACKNOWLEDGMENTS..... ii
CONTENTS.....iii
INTRODUCTION..... 1

1.0
SCOPE.....1
2.0 CONTROL OBJECTIVES..... 2
3.0 DEFINTIONS..... 3
4.0 GUIDELINES..... 4
4.1 SSO Responsibilities..... 4
4.1.1 Initial System Passwords..... 4
4.1.2 Initial Password Assignment..... 4
4.1.3 Password Change Authorization..... 6
4.1.4 Group IDs..... 6
4.1.5 User ID Revalidation..... 6
4.2 User Responsibilities..... 6
4.2.1 Security Awareness..... 6
4.2.2 Changing Passwords..... 6
4.2.3 Log into a Connected System..... 8
4.2.4 Remembering Passwords..... 8
4.3 Authentication Mechanism Functionality..... 9
4.3.1 Internal Storage of Passwords 9
4.3.2 Entry..... 9
4.3.3 Transmission..... 10
4.3.4 Login Attempt Rate..... 10
4.3.5 Auditing..... 10
4.4 Password Protection..... 11
4.4.1 Single Guess Probability..... 11
4.4.2 Password Distribution 11
APPENDIX A: Password Generation Algorithm..... 13
APPENDIX B: Password Encryption Algorithm..... 13
APPENDIX C: Determining Password Length..... 17

APPENDIX D: Protection Basis for Passwords..... 23
APPENDIX E: Features for Use in Very Sensitive Applications 25
APPENDIX F: On the Probability of Guessing a Password..... 27
REFERENCES..... 31

DataDome Ex. 1012, p. 3
DataDome v. Arkose Labs
IPR2025-00694

password entered at login and comparing the encrypted form with the encrypted password stored in the password database.

4.3.2 Entry

Encryption of stored passwords should be used whenever the access control mechanisms provided by the ADP system are not adequate to prevent exposure of the stored passwords. It is recommended that password encryption be used even when other access controls are considered adequate, as this helps protect against possible exposure when access controls are bypassed (e.g., system dumps). When encryption is used to protect stored passwords, it is recommended that the algorithm meet the specifications in Appendix B. It is recommended that encryption be done immediately after entry, that the memory containing the plaintext password be erased immediately after encryption, and that only the encrypted password be used in comparisons. There is no need to be able to decrypt passwords. Comparisons can be made by encrypting the password entered at login and comparing the encrypted form with the encrypted password stored in the password database. Passwords should be entered after providing a user ID to the system. If the entry is correct, the system should then display the date and time of the user's last login.

It is recommended that the system not echo passwords that users type in. When the system cannot prevent a password from being

echoed (e.g., in a half-duplex connection), it is recommended that a random overprint mask be printed before or after the password is entered, as appropriate, to conceal the typed password. The complete password as entered by the user should be an exact match, character for character, with the user's current password.

4.3.3 Transmission

During transmission of a password from a user's terminal to the computer in which the authentication is done, passwords should be protected in a manner that is consistent with the damage that could be caused by their compromise. Since passwords are no more sensitive than the data they provide access to, there is generally no reasonto protect them, during transmission, to any greater degree (e.g.,encryption) than regular data is protected. See Appendix D for guidanceon the protection of passwords.

4.3.4 Login Attempt Rate

By controlling the rate at which login attempts can be made (where each attempt constitutes a guess of a password), the number of guesses a penetrator can make during a password's lifetime is limited to a known upper bound. To control attacks where a penetrator attempts many logins through a single access port, the password guess rate should be controlled on a per-access port basis. That is, each access port should be individually controlled to limit the rate at which login attempts can be made at each port. When a penetrator can easily switch among multiple access ports, it is recommended that the password guess rate also be controlled on a per-user ID basis. It is recommended that maximum login attempt rates fall within the range of one per second to one per minute. This range provides reasonable user-friendliness without permitting so many login attempts that an extremely large password space or an extremely short password lifetime is necessary. See Appendix C for a discussion of the relationship between the guess rate, password lifetime, and password space. Note that it is not intended that login be an inherently slow procedure, for there is no reason to delay a successful login. However, in the event of an unsuccessful login attempt, it is quite reasonable

DataDome Ex. 1012, p. 4
DataDome v. Arkose Labs
IPR2025-00694

to use an internal timer to enforce the desired delay before permitting the next login attempt. The user should not be able to bypass this procedure.

4.3.5 Auditing

4.3.5.1 Audit Trails

The system should be able to create an audit trail of password usage and changes. Such an audit trail should not contain actual passwords or character strings that were incorrectly given as passwords, since this could expose the password of a legitimate user who mistyped his user ID or password. Auditableevents should include: successful login, unsuccessful login

attempts, use of the password changing procedure, and the locking of a user ID due to its password reaching the end of its lifetime. For each recorded event, the audit record should include: date and time of the event, type of event, offered user ID for unsuccessful logins or actual user ID for other events, and origin of the event (e.g., terminal or access port 11'). Audit records of password changes should also indicate whether or not the change was successful.

4.3.5.2 Real-time Notification to System Personnel

It is recommended that each accumulation of 5 consecutiveunsuccessful login attempts from a single access port or against a single user ID results in immediate notification of the event to the ADP system operator or the SSO. While there is no requirement for the SSO or operator to take any action upon receiving the notification, frequent notifications may indicate that a penetration attempt is in progress and may warrant investigation and possible corrective action.

4.3.5.3 Notification to the User

Upon successful login, the user should be notified of:

* The date and time of user's last login;

* The location of the user (as can best be determined) at last login; and

* Each unsuccessful login attempt to this user ID since the last successful login.

This provides a means for the user to determine if someone else is using or attempting to guess this user ID and password.

4.4 Password Protection

4.4.1 Single Guess Probability

The probability that any single attempt at guessing a password will be successful is one of the most critical factors in a password system. This probability depends on the size of the password space and the statistical distribution within that space of passwords that are actually used. Since many user-created passwords are particularly easy to guess all passwords should be machine generated using an algorithm that meets the specifications in Appendix A.

4.4.2 Password Distribution

During distribution to the user. passwords should be protected to the

DataDome Ex. 1012, p. 5
DataDome v. Arkose Labs
IPR2025-00694