Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

1. Overview:

- A. Since 31 JUL 06, access to all Army networks was mandated to be via the Common Access Card (CAC) only. Passwords remain an important aspect of computer security to achieve authenticated access control at the workstation or host level for authenticating access to Army resources until CAC is fully implemented. As such, all users, employees, including contractors and vendors, with accounts on, or access to Army Information Systems (ISs), are responsible for taking the appropriate steps to generate and secure their credentials.
- B. Passwords are used for a variety of purposes. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), users must use strong passwords in their official and personal accounts.
- C. Only randomly generated passwords, generated by a special purpose generator that draws from the largest ASCII character sets available, can keep a step ahead of password cracking programs and should be routinely used when passwords are required.

References:

- A. JTF-GNO CTO 07-015, Public Key Infrastructure (PKI) Implementation, Phase 2 (U/FOUO) DTD 11 DEC 07
- B. AR 25-2; Information Assurance (URL LINK)
- C. How to Enable NTLM 2 Authentication Microsoft
- D. How to Disable LM Authentication on Windows NT Microsoft
- E. How to Prevent Windows from Storing a LAN Manager Hash of Your Password in Active Directory and Local SAM Databases. Microsoft
- F. Top 20 Critical Internet Vulnerabilities SANS
- G. System Administrator Standard Operating Procedures (SOP) BlackBerry Devices with Internal Bluetooth Capability

Related BBPs: None

2. Point(s) of Contact (POC):

NETCOM ESTA / OIA&C

Greg Weaver (CTR SPT) greg.weaver@us.army.mil 703-602-7421; DSN 332 Timothy Hiligh (CTR SPT) timothy.hiligh@us.army.mil 703-602-7509; DSN 332

Mr. Gary Robison gary.robison@us.army.mil 703-602-7395; DSN 332

3. Description of Required Resources: The System Administrator or Network Administrator (SA/NA) must be certified on the existing IA approved product list and the utilization of an approved scanning application to verify compliance.

4. Administrative Requirements:

A. Authenticate user access to all systems with a minimum of a USERID and an authenticator. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

- B. Changing passwords more frequently is authorized and encouraged, for example every 30 days, if password generation software or devices are utilized that meet configuration standards or use one-time or time-based credentials.
- C. SA/NA will provide advance user warning and notification that expiration of their password is approaching to assist in choosing good passwords. Preference is a 10-14 day notification window.
- D. The use of one-time passwords is authorized.
- E. The use of time-based tokens is authorized.
- F. User accounts that have system-level privileges through group membership accounts or programs such as "sudo" must have a unique password from all other accounts held by that user.
- G. Remove, change, or disable all default, system, factory installed, guest, function-key embedded, or maintenance accounts and passwords. When SNMP is used, the community strings will be changed from the standard defaults such as "public," "private", and "system", and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- H. The use of password generating software or devices is authorized as a memory aid (mnemonic) when it randomly generates and enforces password length, configuration, and expiration requirements; protects from unauthorized disclosure through authentication or access controls; and presents a minimal or acceptable risk level in its use. The use of password management applications or devices should allow users the ability to scroll through offered selections to choose an acceptable mnemonic to remember.
- I. **TACTICAL EXCEPTION NOTE**: Consistent with the processes outlined in AR 25-2, the expiration change interval may be extended beyond the requirement for root/secman passwords on tactical systems fielded or being fielded to areas of conflict. The Designated Approving Authority (DAA) will ensure that a risk analysis is performed to address the need to extend the password change interval for these types of accounts. The DAA will then ensure suitable countermeasures are developed and that the risk analysis, along with the required countermeasures, is documented in accreditation documentation and in the approval memorandum signed by the DAA. This only will be done in situations where security, operational effectiveness, and/or troop safety is enhanced by not providing unit level administrators access to these privileged accounts in order to maintain the integrity of the deployed or deploying tactical systems functional software baseline. Only tactical system DAAs recognized in writing by the Army CIO/G-6 may approve these case-by-case deviations. Consistent with the provisions for tactical systems in both AR 25-2 and DoDI 8500.2, allowances are made for the tactical environment in order to reduce the risk to combat crews from denial of service/lock out situations or other impractical implementations that affect troop safety with a limited amount of risk.

5. Description:

A. Army Password Requirements

(1) All system or system-level passwords and privileged-level accounts (e.g., root, enable, admin, administration accounts, etc.) will be a minimum of 15-character case-sensitive password changed every 60 days (IAW JTF-GNO CTO).

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

- (2) All user-level, user-generated passwords (e.g., email, web, desktop computer, etc.) will change to a 14-character (or greater) case-sensitive password changed every 60 days.
- (3) Password history will be set to a minimum of 10.
- (4) Set the Observation Window for Account lockout settings to no more than 60 minutes. Set the LockoutDuration setting (also known in Group Policy as the Account lockout duration setting) to 0 and the LockoutThreshold setting (also known in Group Policy as the Account lockout threshold setting) to 3. This allows no more than two unsuccessful logon attempts within a 60 minute period and requires a system administrator to unlock the account.
- (5) When supported, enable that system capability to notify the user of last successful and unsuccessful logon time and date. Users will notify administrative and security personnel when discrepancies are identified.
- (6) The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters with a minimum of characters as follows:
 - a. Contains at least 2 uppercase characters: A, B, C etc.
 - b. Contains at least 2 lowercase characters: a, b, c, etc.
 - c. Contains at least 2 numbers: 1,2,3,4,5,6,7,8,9,0
 - d. Contains at least 2 special characters, i.e. ! @ # $\% ^ \& ()_+ | \sim = \ \{ \} [] : " ; ' <> ? , . /$
- (7) Passwords will not have the following characteristics:
 - a. Is a word found in any dictionary, thesaurus, or list (English or foreign)
 - b. Is any common usage word or reference such as:
 - (I) Names of family, pets, friends, co-workers, fantasy characters, etc.
 - (II) Computer terms and names, commands, sites, companies, hardware, software.
 - (III) Common words such as; "sanjose", "sanfran" or other derivative.
 - (IV) Birthdays, addresses, phone numbers, or other personal information.
 - (V) Word or number patterns like; aaabbb, gwerty, mypassword, abcde12345.
 - (VI) Any of the above spelled backwards.
 - (VII) Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
 - (VIII) Social security numbers (SSNs).
 - (IX) USERID
 - (X) Military slang, acronyms, or descriptors or call signs.
 - (XI) System identification.
- (8) The use of eight character passwords are authorized when:
 - (I) The password generated is a purely random-generated authenticator from the complete alpha/numeric and special character sets and no user-configured passwords can replace, be generated, or accepted in lieu of the generated password. (For example: Credentialing system issues randomly generated authenticator AND enforce use of that authenticator to network resources.)

Or:

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

(II) Access to private applications is conducted over an approved 128-bit encrypted session between systems, and the application does not enforce local user access credentialing to a local network resources. (For example: User accesses local LAN connected system through traditional access procedures then accesses a web portal application over an SSL connection; the web portal password may be 8 characters.)

TACTICAL SYSTEMS NOTE: Deployed/tactical systems with limited data input capabilities will also implement these measures except in those cases where implementation of this guidance is operationally impractical or adversely impose risk of safety-of-use because of the function and design of the system. Deviations from password standards in these cases will be addressed in the accreditation documentation as well as in the approval to operate memorandum signed by the DAA. Only DAAs recognized in writing by the Army CIO/G-6 may approve these case-by-case deviations.

WINDOWS SERVICE ACCOUNTS: Verify the use of AT LEAST a 15 character password for all Windows Service Accounts.

- a. Windows Service Account passwords manually generated and entered by an administrator should be changed yearly or upon loss of system administrator that had knowledge of password, whichever is earlier.
- b. Windows Service Account passwords randomly generated and automatically entered into systems do not have to be changed as frequently.
- c. Many Windows Services do not require accounts to operate effectively. System implementations should minimize usage of Windows Service Accounts unless required. As legacy applications are upgraded to current COTS versions that do not require Windows Service Accounts, this should be accounted for during system implementations.

B. Password/Account Protection Standards

- (1) Enforce password policy through implementation or enhancement of native security mechanisms.
- (2) Use separate authenticators for Army accounts; non-Army accounts (e.g., personal ISP accounts, MyPay, banking, benefits websites, etc.); different OS types such as Windows and UNIX; development systems versus operational systems; different access level accounts; or different classification levels such as NIPRNET, SIPRNET or JWICS.
- (3) Privileged-level account passwords will differ from their normal-user account passwords.
- (4) Share authenticators only when required for trusted operations or authorized; such as group helpdesk accounts, network operations, or watch-standing environments, when alternative logging measures are implemented.
- (5) Prohibit automated scripts or linkage capabilities, including, but not limited to, Web site links that embed both account and authentication within an unencrypted link.
- (6) Stored password mnemonics files on ANY computer system (including Palm Pilots or similar devices) utilize NIST certified AES encryption with at least a 128 bit key.

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

- (7) When required, passwords for privileged-level access to critical applications, devices, or IS shall be secured in an envelope that is signed across the seal so that any attempt at tampering is evident, and that the envelope should be kept in a locked container certified for storage of documents commensurate with the classification of the data which the password protects.
- (8) Here is a list of "don'ts":
 - Don't reveal an authenticator over the phone to ANYONE.
 - Don't reveal an authenticator in an unencrypted email message.
 - Don't authenticate remotely over insecure protocols such as ftp, telnet, http, POP3, or SNMP.
 - Don't talk about authentication processes in front of unauthorized persons.
 - Don't hint at the format of an authenticator (e.g., "my family name").
 - Don't reveal authenticators on questionnaires or security forms.
 - Don't share official access authenticators with family members.
 - Don't allow visitors to "shoulder-surf" while accessing IS.
 - Don't reveal an authenticator to co-workers while on vacation.
 - Don't reveal authenticators in response to unsolicited emails (phishing)
- (9) Do not use the "Remember Password" feature of applications. Use of these features for personal sites (e.g. Hotmail, Yahoo) is a risk accepted by the user, but should be discouraged.
- (10) Disable password save-functions incorporated within software or applications.
- (11) All web-access applications requiring access credentialling will be 128-bit SSL encrypted or stronger.
- (12) The initial password for a new remote user should be sent through a courier service or registered mail, or issued in-person at a trusted intermediary's office with the provision for proof of identity through valid government identifications. If sent by regular mail, passwords will be sent separately from user IDs, have no markings indicating the nature of the enclosure and will be concealed inside an opaque envelope that will readily reveal tampering.
- (13) All temporary passwords issued must be expired immediately when input, forcing the user to choose another acceptable password known only to the user before the logon process is completed.
- (14) Passwords inserted into email messages or other forms of electronic communication shall be CAC encrypted and sent separately from user IDs, with no markings indicating the nature of the attachment.
- (15) If any account or password is suspected of having been compromised, report the incident to the SA/NA immediately. SA/NA will report account compromises to the IA personnel chain, the chain of command, the Installation DOIM, and the appropriate RCERT supporting your organization. Change all account passwords when directed; from a known secure system. Do not use your computer system until an investigation has been completed and the system has been rebuilt from the compromise.
- (16) If a privilege-level account has been compromised by an intruder, all passwords on that system will be immediately changed, and the privileged account disabled on the entire network until completion of the forensic investigation. Consideration must be given to the credibility of any and all accounts created within the suspected time frame, and all user accounts should be considered compromised. Re-issuance of new passwords or accounts may be required.

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

- (17) A user may be required to be authenticated through personal presence, or other DAA approved solution, that verifies the individual's identity and authorization prior to obtaining a new authenticator or password, or to unlock accounts for any unclassified, sensitive, or classified IS or network.
- (18) Users and supervisors are responsible for notifying SAs or IAMs when an individual's access is no longer required. User access will be terminated within 1 day following notification that a user no longer requires access to any IS. Any group account authenticators for which a departing individual had access will be changed immediately.
- (19) SAs should suspend LAN-based accounts that have not been used in a 45-day period for LAN connections and 90 days for web-based portal accounts based on the portal users profile and acceptable risk evaluation.
- (20) SAs will disable user accounts immediately upon identification of unauthorized activity by the user or the user notifies SA personnel that the account is being used illegally.
- (21) The network and system vulnerabilities identified with the use of LanMan (LM) and NTLM will be eliminated and the use of NTLMv2, Kerberos, or equivalent 128-bit encryption implemented between connected systems.
- **C. Standalone IS or Standalone Enclave Standards** SA/NA and IA personnel will establish authentication procedures for those standalone ISs or networks (physically isolated with private IP addresses) that are incapable of being accessed remotely over any connection such as a modem or wireless; or accessible over an operationally connected networked such as the NIPRNET or SIPRNET. Examples of standalone IS include; laboratory or diagnostic equipment, control systems, and human-machine interactive devices.
 - (1) These devices will enforce need to know or need to access requirements as defined by local personnel access procedures or requirements and the type of information accessible and type of system installed.
 - (2) These devices will enforce specific authenticator requirements as necessary to activate the device or system and protect the devices from unauthorized access or use.
 - (3) Authenticator configuration and expiration standards will be included as part of the risk mitigation plan, but these configurations may not meet the BBP standards.
 - (4) Authenticator processes will be approved by the DAA.
 - (5) Authenticators will never be shared outside authorized personnel for such equipment.
 - (6) IS and devices will be protected with physical access controls to the work environment.
 - (7) Procedures will be developed, approved, and enforced for systematic changes as required for instance such as departing personnel or temporary access requirements.
 - (8) Any standalone IS that is moved to an operational network shall enforce authentication standards of that operational network.

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

- **D. Application Development Standards:** Application developers must ensure their programs contain the following security precautions. Applications:
 - (1) Will support authentication of individual users, not groups.
 - (2) Will provide non-repudiation either through the application or the host operating system.
 - (3) Will not store passwords in clear text or in any reversible form.
 - (4) Should provide or implement role management.
 - (5) Should support standards based authentications such as: TACACS+, RADIUS, PKI, and/or X.509 with LDAP security retrieval, whenever possible.
 - (6) Must be developed, acquired, and fielded that prevent or preclude unauthorized use of legitimate identification and authentication through attacks such as session replay, impersonation, masquerading, object reuse, or spoofing of the supplied credentials.
- **E. Standards for Passwords and PINs for Email / PED data retrieval devices:** Data retrieval devices (for example, BlackBerries) are capable of two-way unclassified wireless transmission and reception, but are not considered as extensions of a LAN environment as would be established through a wireless access point or connection. The device functionality is restricted to text messaging capabilities only. Device passwords should comply with the DISA Wireless STIG and the Appendix: BlackBerry Security Checklists; additionally modified by the Army's SOP for BlackBerry Devices with Bluetooth Capability.
 - (1) The following are standards for acceptable use and risk mitigation within the Army.
 - (a) Five character alphanumeric authenticator with at least one letter and one number.
 - (b) Will be configured with a 30-minute timeout feature.
 - (c) Will wipe the device after 5 incorrect attempts.
 - (d) Will be capable of storing the last 3 passwords in history.
 - (e) Authenticators will expire every 60 days maximum.
 - (2) The device must be upgradeable to support the use of CAC and shall enforce CAC card PIN authentication when Army leadership deems it appropriate or per local commander's discretion. As there are notable technical and usability issues, this should not be undertaken without first piloting the capability locally. A 6-8 digit numeric password is also acceptable in environments that require a CAC to authenticate to the handheld.
 - (3) CAC-enabled devices running pre-handheld 4.0 OS are exempted from the device password requirement, as a significant, unresolved technical issue arises when a password is enforced that is exacerbated when a users migrates to a new CAC. It is strongly recommended that these devices be upgraded to handheld OS 4.0 or greater, as soon as possible.
- **F. Use of Passwords and Passphrases for Remote Access Users:** Access to the Army Networks via remote access shall be encrypted and should be controlled using either a one-time password

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

authentication, a public/private key system with a strong passphrase, a callback system, dynamic password tokens, or use of digital certificates.

G. Passphrases

- (1) Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
- (2) Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
- (3) A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"TheTrafficOnTheI95WasMiserableThisMorning"

(4) All of the rules above that apply to passwords apply to passphrases.

H. Common Access Card (CAC) PIN

- (1) The CAC PIN is a 6-8 digit number that is used to access the data and Public Key Infrastructure (PKI) certificates on the CAC's integrated computer chip. The PIN should be kept secure at all times even though it is useless to an adversary unless they also have physical control of the CAC. The PIN should never be shared, even with trusted co-workers, subordinates, or superiors. Doing so facilitates fraud and identity impersonation. The CAC PIN is considered more secure than any password since it is never on the network; therefore, there is no requirement to mandate changing the PIN, however users have that option when issued a new CAC.
- (2) The cardholder has three chances to enter the PIN correctly. After the third time, the system will lock the cardholder out. The cardholder will need to go to a CAC PIN Reset (CPR) station or return to the nearest CAC issuance site where they will be given the opportunity to prove they are the owner of the card by matching a fingerprint against the fingerprint that was stored on DEERS when the card was issued. If the fingerprint matches successfully, the cardholder can select a new PIN. The Army POC for CPR, cpr.apoc@us.army.mil, can provide assistance locating the nearest CPR workstation.

I. Enforcement

- (1) **CRITICAL ISSUE:** Army CIO/G6 Compliance Verification Team assessment analysis constantly reveals violations of Information Assurance Vulnerability Alerts in references to blank and default accounts on evaluated systems and networks. SA/NAs will perform monthly assessments of their networks and systems with approved scanning tools to verify that default, guest, and administrative accounts are protected.
- (2) SA/NAs will perform password cracking or guessing on a quarterly basis with Command authorization within their authority when passwords are used as the authenticator. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking tools offer the capability to obscure the actual password, and simply identify accounts that are non-compliant to the policy. SA/NA should choose this option when available. Never attempt to

Update: 1 MAY 08

ARMY PASSWORD STANDARDS

Version 2.5

audit password files on an operational network without extensive testing, practice, and experience on a non-operational (test) environment or system.

- (3) Ensure log files and audits are maintained and reviewed for all systems and that authentication (for example, password) policies are audited for compliance.
- (4) Manage, enforce, and audit all account passwords, permissions, inactivity, and suspension policies.
- 6. Products: Currently, there are no identified commercial products on the Army IA Approved Product List. Local acquisition of acceptable products, policy, DAA, and DIACAP certification processes is required. DoD offers John the Ripper (free) at https://iase.disa.mil/techguid/ripper-032202.zip or http://www.openwall.com/john/ to verify compliance to DoD standards.
- **7. Training:** All users must receive IA awareness training tailored to the system and information accessible before issuance of a password for network access.



DEPARTMENT OF THE ARMY OFFICE OF THE SECRETARY OF THE ARMY 107 ARMY PENTAGON WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

NETC-EST-I

MAY 0 1 2008

MEMORANDUM FOR All Army Activities

SUBJECT: Implementation of Information Assurance Best Business Practice (IA BBP) for Army Password Standards

As the Director, Army Office of Information Assurance and Compliance and the Army FISMA Senior Information Assurance Officer (SIAO), the undersigned approves the identified IA BBP(s) in support of Army Regulation 25-2 and the Army Information Assurance Program (AIAP). The BBP is the standard to be implemented throughout the Army for all information systems and networks for the identified purpose.

04-IA-O-0001; Army Password Standards; Version 2.5

MICHAEL J. JONES

Colonel, GS

Director, Army Office of Information Assurance and Compliance