Secure Password Storage

Shelby Reeves

Secure Password Storage

Shelby Reeves

August 14, 2001

GSEC Practical Requirements (v.1.2e) (December 2000)

The Challenge

Passwords. The keys to our networks. Safeguards of our information privacy, financial transactions, intellectual property - sometimes even our physical security!

How do we store and protect these keys, yet present them immediately for use when:

- a Sysadmin takes up extreme sports – with disastrous results -- and is no longer there to help, even over the phone?
- the "big one" finally hits and the IT staff are headed for a recovery hot site?
- a critical password is simply forgotten or lost?

This is a challenge that faces IT shops of almost any size. Passwords/authentication methods must be protected from unauthorized disclosure and tampering but must also be readily available to allow fast recovery in the event of a service interruption or loss of personnel.

Coming up with a secure method to archive and retrieve passwords for my company has become one of my personal goals. Our current environment (handwritten passwords stored in a fire safe which is locked by a key stored in the main Data Center) leaves us exposed to a number of hazards, including:

1. Accidental loss or disclosure of a critical password if it is not returned promptly to its storage place
2. Inadvertent exposure of the entire password file if the safe is left unlocked
3. A single access point for password retrieval that cannot be reached from all points on the network. Sysadmins who need passwords -- typically at midnight! -- for systems that are not physically located in the same facility as the fire safe must make a trip to the storage site to retrieve the password before moving on to work on the system that has failed.
4. No granularity of control to password access. All super users -- Sysadmins, DBAs, Network staff and data center personnel -- have access to all passwords since there is no way to secure them separately. (We are operating on the honor system)
5. Unnecessary compromise of data center access rules simply because access to passwords is required.
6. No physical or electronic backup of passwords to help us recover in the event of a disaster.

Some of these hazards are more hair-raising than others, to be sure. However all of them must be addressed in the password archival solution that is selected.

The Options
The options for dealing with this challenge range from *replacing* traditional passwords with more complex authentication systems - such as biometrics and smart cards - to extremely low-tech, insecure solutions such as filing written passwords in separate locked drawers and manually transcribing them for disaster recovery purposes.

However, since the complexity and cost of implementing a new authentication system is beyond the reach of most IT organizations today – including mine -- the focus of this paper will be the secure *electronic* storage and retrieval of traditional passwords.

The Search for a Product
Faced with literally hundreds of devices and applications and an IT staff working in a 24x7 environment, I began the search for a commercially available solution that would meet my requirements. The product would have to offer, at minimum, the following features:

- Confidentiality
- Integrity
- Availability
- Scalability
- Simple implementation
- Ease of use
- Reasonable cost.

Web searches for key words “secure password storage” using sophisticated search engines repeatedly yielded the same list of candidates. I checked each of them against my criteria, with the following results:

Password Safe by Counterpane Systems (http://www.counterpane.com/passsafe.html) Freeware. This appears to be a robust personal password management tool with very strong encryption (Blowfish) and a wide range of features, providing for backups, segmented databases, save/delete prompts upon minimization, a safety lockout after three attempts, etc. Password Safe does not appear to be scalable to an enterprise-wide deployment. However it would be my product of choice as a personal password management tool.

Password Keeper 99 by Wolff Software (www.wolff-software.de/passkeep_en.html)
Pro version is $20.00; Light version is freeware. Very little information was directly available online concerning this product. Features are mentioned as one line items on the website (password generator, search function, printing, expiration dates, etc.) However, Hans Wolff responded very promptly to my request for product information, stating that Password Keeper 99 uses a 448 bit Blowfish encryption algorithm to encrypt the password databases and referred me to the Counterpane.com website for more information on the encryption method. He went on to say that there are no "back doors" buried in the software, no secret checksums, etc., and referred me to the help file on the actual executable for more information.. I was reluctant to actually download an executable from an untrusted site, so I chose not to delve into this product further since

it appears -- like the others -- to be a personal password management program and is probably not suitable as a solution in an enterprise environment.

PassMan by iJEN Software (http://www.ijen.net)
Single user license is $32.95. PassMan is a personal use password management program with screen lockout and intrusion alert features. The product information states that the data "is stored on an encrypted file on your computer" but no data is provided on the encryption algorithm or strength. There does not appear to be a way to extend access to the password file beyond the individual user and there is insufficient information about the security structure of the product to make it a viable candidate for enterprise use.

Password Manager 2.0.5 by eInternet Studios (http://www.password-manager.com)
Freeware. Password Manager 2.0.5 is an oddity among the products I researched. It, too, is aimed at the personal user. However, the product information on the website states that the files are protected "using our custom encrypted data protection method". It also specifically suggests that the types of passwords that could be stored would include PINS, ATM codes, computer user names and passwords - along with "detailed notes, description, hints, and usernames for all of your accounts." These files are then "protected" by a user-selected "unique master password". Ominously, in the feature description of the Master Password is the following statement: "If you should forget your Master Password, contact customer support at suppport@password-manager.com. *We maintain security tools that can recover your password should you forget it."* (italics mine)..

Password Administrator 2.0 by Infintron Software (http://www.infintron.com)
Shareware offered at $12.95. Password Administrator is a personal use password management program with report functions, password generation, database backup, search and access logging features. Product information states that the password database is encrypted, but no data is provided on the encryption algorithm or strength. There does not appear to be any way to extend the functionality of the software to a shared, enterprise-level model, nor is there sufficient information about the security structure to make it a viable candidate for consideration.

Thwarted? Use the tools…and build your own!
Many hours of research later, I was forced to conclude that an out-of-the box secure password storage product – scaled for enterprise-wide use – does not currently exist. Since we still had a need (and giving up was not an option), I sought advice from our network security consulting firm. They suggested using an encryption software program, PGP, as the foundation for building our own secure password storage system and a design structure that will be relatively simple to incorporate into our environment.

An in-depth look at PGP (Pretty Good Privacy) revealed a low cost, well-tested technology with a rich feature set and a solid user base. Originally released in 1991, PGP has evolved to include intuitive GUIs, help screens and administrative tools Currently, PGP is available in freeware versions, distributed by the Massachusetts

Institute of Technology at http://mit.edu/network/pgp.html and commercially from Network Associates at http://www.pgp.com.

This product -- combined with the access controls inherent to our operating systems -- appears to offer us the most viable solution to our password storage woes.

The Design

The proposed storage design is clean, uses strong (128 bit) encryption, leverages the software structures already in place and provides easy – but controlled – access to the password "vault" from the desktop.

Passwords will be stored in a strongly encrypted directory which is compartmentalized by function and level of access. Only a pass-phrase or PGP private-key can decrypt the files. User access to the password directory and its sub-files can (and will) be logged. by the file share system.

Since the password directory itself is protected using 128 bit encryption, it can safely be stored on an NT or Novell file share and be readily accessed by anyone in the company who has the appropriate private key or pass-phrase for that particular share. Those who do NOT possess the appropriate credentials will see only a garbled file.

Implementation

PGP will be installed on the workstation of each user who requires access to the password file directory. Using the PGP software, each user must then create his/her public-private key pair and lock it with a user-selected pass phrase. PGP's built-in password assessment feature will immediately provide a ranking of the strength of the pass phrase chosen by the user – warning the user if his/her chosen pass phrase is too readily "guessable" and should therefore be reconsidered.

In keeping with the hierarchical structure of each of the IT staff units (Development, Systems, Network, Web, etc.), administrative passwords will be partitioned into different access levels based on which groups need access to which systems. A password administrator will be designated for each group and will create a password encryption share for that group. The administrator of that group can then assign users to the shares using their PGP key-pairs and assign rights to them within that share such as "read only" or "read/write" in accordance with the specific user's authorization level.

Further, this structure will allow us to establish a "super admin" for the password directory. The pass phrase/key for this superuser will be stored at a separate off site location and retrieved only in the event of a disaster. This will eliminate our struggles to keep an offsite password list that is up to date. If a disaster occurs, the current passwords will automatically be included in the files stored off site. By establishing a superuser account and maintaining the superuser pass phrase at one or more different off site locations, we will radically improve our ability to recover systems during disaster recovery efforts and reduce our dependency on the memories and availability of key Sysadmins.

Putting it to use
Once set up, the user who has been included in a password file share will be able to access the passwords to the "assets" within that group by simply clicking on the directory. The user will be prompted to enter the pass phrase that he originally used to lock the private-public key pair on the share. This is the only way he can release his private key to match to the public key stored on the share and successfully decrypt the password file. If he has forgotten the pass phrase or if the private key presented does not fit the public key, the user will be unable to decrypt the password share file. To regain access the user will have to create a new public-private key pair locked with a new pass phrase and ask the group admin for his unit to enter his new key into the access rights for the file share.

Does it fill the bill?
The password storage design described above meets and exceeds our selection criteria in some important ways:

- Confidentiality – The password files are protected with the strongest encryption algorithm currently available in the United States. Two levels of authentication must occur to unlock the data - a private key and a pass phrase.

- Integrity – The two levels of authentication significantly reduce the possibility of casual or even unintentional alteration/destruction of the password data. Further, the user ID's of those who access the file shares are separately logged by the file share access controls inherent to the operating system – which will allow us to determine who was responsible if some negative action does occur.

- Availability – users will no longer need to get up from their desks and go in search of a physical copy of the password. Access will be readily available from anywhere on the network provided that the user remembers the pass phrase that unlocks his or her private-public key pair.

- Scalability – This design takes advantage of the enterprise file structures developed by both Microsoft and Novell to allow user access and file access logging on a broad scale if required.

- Simple implementation – Although "simple" is a relative term, this design structure covers familiar ground for most IT staff. It simply involves a desktop-based software installation and a procedural change.

- Ease of use -- The concept of file access rights, pass phrases and the use of a GUI-based Windows application such as PGP is perceived to be procedurally more "normal" than the introduction of retina scans, fingerprint readers or even token-based cards. And, although the security is not perfect there is slightly less chance that the user's access will be denied (or created redundantly) because he or she forgot the token card at home -- along with the pager, cell phone, access badge, etc.

- Reasonable cost – since we will choose to purchase the commercial version of PGP to have access to all of the latest features, our cost will be approximately $80 per user at the current rate. This seems a reasonable price to pay for securing access to our systems and (potentially) ensuring their recoverability in the event of a disaster.

Summary

The proposed solution is not "perfect"; it does not absolutely close all security holes.

It is still possible that a user with rights to the password shares will write down, disclose or otherwise mishandle his unique pass phrase. The Triple DES encryption algorithm (128 bit) may be cracked in the near term and our entire password database could be exposed. An error could be made, inadvertently adding a bad user to a password share. Our disaster recovery "superuser" password could be disclosed, exposing all of our passwords to a malicious intruder.

With all of its potential warts, however, this PGP-encrypted file shares design seems to address all of our most serious problems with physical password storage and has the added advantage of employing time-proven technologies at a reasonable cost.

I am happy to report that this design proposal has been approved and will be implemented at our company soon.

References

Counterpane Internet Security. "Password Safe" Documentation
URL: http://www.counterpane.com/passsafe.html

Wolff Software "Password Keeper 99 - Pro Version" Documentation
URL: www.wolff-software.de/passkeep_en.html

iJEN Software. "PassMan" Documentation
URL: http://www.ijen.net

eInternet Studios "Password Manager 2.0.5" Documentation
URL: http://www.password-manager.com

Infintron Software "Password Administrator 2.0" Documentation
URL: http://www.infintron.com

PGP Security "An Introduction to Cryptography" White paper.
URL: http://www.pgp.com/products/whitepapers.asp

PGP Security. "PGPdisk Encryption" Documentation
URL: http://www.pgp.com/products/disk-encryption/default.asp

MIT Distribution Center for MIT. Documentation.
URL: http://mit.edu/network/pgp.html