Selecting a Disk Encryption Vendor

Introduction

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. Encryption is used to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

Scope

Due to the thefts of machines that contain company sensitive and proprietary data throughout the company, we have been tasked with the responsibility of locating, testing, recommending and implementing a disk encryption vendor. Evaluation of a number of recent thefts of company owned laptops suggests that some of the thefts were targeted not at the PC itself, but at the information contained on it. Disclosure of this type of data outside of the company could have significant financial impact on the company. This is especially true if competitive information finds its way into the hands of our competitors.

There is a need for a data encryption suite that provides comprehensive encryption functionality for PC's, e-mail and file sharing on servers. The disk encryption software should target all file types that contain data or temporary data storage. Implementation of this product will provide the mechanism to protect all company proprietary and sensitive data on PC's. Implementation of this product suite should meet the data protection requirements established by Information Security. The implementation of this layer of data security will, to the greatest extent possible, ensure the security of company proprietary and sensitive data.

Data Protection Requirements/Request For Proposal (RFP)

There are several requirements that will drive this project; following are some of the requirements that were included in the RFP:

- Compatible with Windows NT and 2000
- Support of double-byte OS
- Can product be integrated into the office 2000 suite of products
- Does product contain a master key?
- Ability to encrypt large files without significant performance degradation
- Does product allow for a secure method to centrally administer user keys?
- Does product allow users to access encrypted data when either connected to the network or when working offline?
- Is product compatible with SMS 2.0?
- Is product scalable to meet a growing company with over 10,000+ users?
- Are any files excluded from being encrypted

- Are there products that conflict with your product?
- Does product comply with international laws in the countries where we operate?
- Provide hardware requirements
- Provide method to revoke a user's key, preventing further access to encrypted data
- Provide delivery timeframe

Responses

RFP's were sent out to ten vendors, which included, but we not limited to the requirements listed above. RFP also indicated that this project would run in phases; phase one was to cover the disk encryption portions, future phases would cover e-mail and server encryption. Of the ten vendors, we received four responses, which indicated to us at this point in the project that they could meet all of our requirements.

Testing

A lab was set up which contained desktops, laptops and servers all running NT or Windows 2000. A testing script was created and users from different departments were asked to test against this script. We needed to get buy-in from these departments that the product selected was by far the best product to protect company sensitive and proprietary information.

Testing will occur in phases: Phase one will consist of the test bed testing—high level testing for each vendor product. This will allow us to eliminate any vendor that can't meet our testing requirements. Phase two will consist of our user acceptance test (UAT); this testing will enable our test bed testers to test the software in detail against our applications and 3rd party software. Phase three will consist of the pilot testing; this will consist of about 100 users. These 100 users will be our audience as we roll out the product via an executable, SMS, CD or dial up connection. They will be testing on their own laptops whereas in phase one, the equipment was in a controlled environment to not disturb production data. The users in the pilot testing will include the CIO, directors, VP's and representatives from each of our departments. This phase will bring out any problems that were not discovered in our controlled lab environments.

Encryption Types—Pros/Cons

File \folder level encryption
Pros:

- Better integration with OS
- Good overall security

Cons:

- User education is higher as most users need to be taught on how to save data in protected folders
- More user interaction

- Performance hit

Virtual drive encryption
Pros:

- No performance hit
- Less user interaction (although users will need to be taught to save to encrypted drive versus boot drive or desk top)

Cons:
Reimage of every laptop company wide

Drive/Partition level encryption
Pros:

- No user interaction
- Least performance hit

Cons:

- All users have same access
- Provides no security once user is logged on

Testing Results

The 4 vendors selected for the testing phase 1 will be knows as Vendor A, B, C and D.

Each vendor had a different way to encrypt, the three type of encryption are addressed above. We encountered some major problems with 3 of our vendors, so we are moving forward with our UAT with vendor number 4.

Encryption Vendors—Pros/Cons

Vendor A
Pros:

- No performance issues
- Application encryption is available
- Easy to enforce

Cons:

- May need to touch every system company wide during rollout phase
- Extra Password
- Cannot encrypt desktop

Vendor B
Pros:

- Full disk encryption
- Highly protected
- Works below OS level
- No performance degradation
- Remote challenge for password recovery

Cons:

- Requires additional password

Vendor C

Pros:

- Integrating our SecureID token
- No extra password needed

Cons:

- PCMCIA card is necessary to use encryption offline
- High maintenance setup—need a server
- May need to touch every system company wide during rollout phase
- Encrypts at the folder lever—performance degradation

Vendor D

Pros:

- Easy to implement
- No extra password
- Easy to administer through group policies

Cons:

- Performance degradation
- Cannot encrypt applications
- Heavy user interaction

Encryption Matrix

From the inception of the project, the Encryption Matrix was utilized to score vendors against our specific requirements. Well into the testing we were able to complete the matrix and move forward with the selected vendor.

	VENDORS			
	A	B	C	D
Type of Encryption	**Virtual**	**Drive**	**File**	**File**
Business Requirements				
Encrypt partial or complete data on laptop and desktops	B	A	C	C
Encrypt Online and Offline	A	A	A	A
Easy to use	B	A	C	B
Transparency from user's day-to-day work	B	A	C	C
Encryption services for global users	A	A	A	A
Revoke of user keys	B-	A	B	A-
Master security key to recover encrypted data	A-	A	A-	A-
Password recovery	B	A	B	A

Technical Requirements				
Run under Windows NT and 2000	A	A	C	C
Avoids conflicts with other software	A-	A	B	A
Encrypt large files without significant performance degradation	A	A	C	D
Ease of deployment	D	A	B	A
Scalable for capability of over 10,000 users	A	A	A	A
Ease to administer	B+	A	D	B
Over All Score	**B**	**A**	**C**	**B-**

Conclusion

Needless to say we are moving forward with Vendor B, which scored the highest on our matrix report card. Vendor B utilizes the Blowfish Encryption Algorithm, which is a symmetric block cipher. It takes a variable length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Many cryptographers have examined Blowfish, although there are few published results.

Encryption at the drive level is one of the main reasons this product was selected; this would not allow disclosure of confidential and proprietary data outside of its intended audience.

References

Arnoud "Galactus" Engelfriet , “Security: Encryption: PGP”, June 20, 1998
URL http://www.stack.nl/~galactus/remailers/index-pgp.html

The Insider, Volume 2 Issue 3, March 1998,
URL http://www.ticm.com/info/insider/old/mar1998.html

Spy Technology Agency, PGP Disk
URL http://spytechagency.viamall.com/spytechagency/pgpdisk.html

SC Security Magazine, Now you read it, Now you don’t, August 2000

Copyright Counterpane Internet Security, Inc., 2000, The Blowfish Encryption Algorithm URL http://www.counterpane.com/blowfish.html