Encryption Technologies And University Campus Needs

Dr. V.A. Athavale*, Prof. Santosh Singh**
NRIITM, Gwalior(M.P),
*santosh32m@sify.com, **vijay.athavale@gmail.com

Abstract-Many Universities in the country are aiming at implementing a plan to secure sensitive information across campus. This necessitates use of various encryption technologies. This paper is an attempt to help such institutions to lay down organizational setup for this purpose. It will need formation of several committees at all levels of the private Universities / Deemed Universities, to advise, identify, and direct data security activities at the enterprise level.

Keywords: Breach, Compliance, Evaluation, Privacy, Protection, and Sensitive Data.

1. INTRODUCTION

A. Overview

Government of India is giving stress on developing private universities in the country. It is a result of years of experimentaion with Institution providing Higher Education lagging behind the ever-changing requirements of industry, prime employer of the trained manpower in the country. This has resulted in rapid growth of private Universities / Deemed Universities. Private universities have less bureaucratic, more flexible structure capable of offering up-to-date course curriculum as per the needs of the industry. With the state run Universities having a long history of service are not fully computerized. On the other hand, private universities are increasingly using computerization as a means to 1) reduce manpower requirement 2) reduce operational cost 3) reduce impact of high turnover of manpower by applying knowledge management techniques 4) Provide online registration, education and testing etc. This demands consistency, which can only be achieved if the system is properly secured.

B. Why We Need to Encrypt

Protection of data has always been an important concern for colleges and universities, but as we shift to virtual university using electronic communication, online data collection, digital storage, and e-commerce transactions; securing confidential information becomes even more complicated. It is critical for the preservation of the institution’s reputation and integrity to protect the privacy of its constituents. "In today's computerized economy, customers trust companies with a lot of sensitive personal and financial information. Any breach of data security that would compromise that trust can have a devastating impact on the company's reputation." In addition to the growing demands placed on institutions to protect sensitive information, security risks and breaches are increasing as a result of mobile computing. Over the past several years, government organizations, universities and corporations have made

headlines when laptops containing constituent records were hacked, exposing thousands to potential identity theft. Encryption is the only solution to this paradox of security and convenience. By preventing unauthorized access, encryption will protect the data even if the laptop or other mobile storage device is lost or stolen.

C. Security Committee Structure

With growing threats and challenges to the protection of sensitive data, Universities must create a committee to develop a comprehensive strategy for integrating security within its information services. The committee must be divided into relevant different areas and must be incorporated into the structure of the Senate Council (Executive Council) for Information Services, which sets university-wide information services policies.

Figure 1 Outlines the structure of the council for information. This council has two main sub councils. 1. Data standard council 2. Data security council. The data standard council ensures adherence of data standards. It is proposed that the Data Standards Council has two sub councils for the standardization of data namely, 1. Public data 2. Private data. The data security council ensures security of data and framing policies for protecting data. This council has three sub councils. 1. sub council for users policies maker. 2. sub council for Data encryption / Decryption 3. sub council for Firewall.

II. PROCESS AND RECOMMENDATION

A. Encryption Subcommittee Charge

The charge of the Data Encryption Subcommittee is to examine current encryption technologies to determine the method of encrypting PCs and other portable devices, and backups. The committee may comprise of system analysts, the information system officer, computing consultants, a database manager, an enterprise information consultant, and Client Services team leaders.
B. Subgroups

Because of the wide variety of devices and systems to be evaluated, subgroups have to be formed to address the following:
- Desktop PC & Laptop encryption (Windows and Linux)
- Encryption of UNIX, Linux and Windows files
- Removable media
- Encryption of Software & Hardware
- Backups (Windows and Enterprise)
- Encryption of network traffic
- SQL Server security
- Management of Encryption keys
- Management for LAN, WAN, Wi-Fi Network
- End-user training

C. Issues and Concerns

Following is a representative list of issues and concerns:
- Cost of software and hardware for centralized management
- Ability to recover data on encrypted drives
- Management of encryption keys
- Classification of data by security level
- Limitation of file/folder encryption only
- Dependent upon users’ compliance
- Hidden or “forgotten” data
  - Temporary files
  - Windows swapfile or pagefile
  - Recycle bin
- Management of shared encrypted resources

D. Evaluation Process

The first step in the evaluation process will be periodical research of available products and of current practices at other institutions. Calls to vendors for additional information as well as discussions with individuals from other institutions will help us to determine the products we would be testing. Encryption software testing and evaluation will involve both whole-disk encryption as well file and virtual disk encryption.

User education is vital to the success of the encryption initiative. An encryption web page may be developed along with data security seminars to help clients understand the importance of privacy, to recognize the type of data that is considered sensitive, and to offer suggestions regarding how they can use existing software and resources to encrypt confidential files.

E. Encryption Evaluation

Step 4: Chose the most users friendly and compatible software package, which is widely used for encryption in education market. One such software is PGP. PGP includes Windows Whole-disk encryption solution as well as a Mac client, which performs volume encryption (not whole disk). PGP also currently offers a Windows Vista Client where as WinMagic does not. Comparison of some of the popular encryption software is presented below:

Table 1. Whole-disk encryption software evaluated

<table>
<thead>
<tr>
<th>Software</th>
<th>Supported Platforms</th>
<th>Install Time</th>
<th>Supported Storage Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGP Whole Disk Encryption</td>
<td>Win 2K, WinXP, Vista</td>
<td>80 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
<tr>
<td>Win Magic Secure Doc 4.2</td>
<td>Win 2K, WinXP, Vista, Win 2003</td>
<td>78 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
<tr>
<td>Alert Boot</td>
<td>Win 2K, WinXP, Vista, Win 2003</td>
<td>82 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
<tr>
<td>Drive Crypt</td>
<td>WinNT, WinXP, Win2K</td>
<td>78 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
<tr>
<td>Safe Bit</td>
<td>Win 2K, WinXP, Vista, Win 2003</td>
<td>79 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
<tr>
<td>Cypherix</td>
<td>Windows</td>
<td>76 Min</td>
<td>Hard Disk, USB Flash Drive</td>
</tr>
</tbody>
</table>

Table 2. File/folder/virtual disk encryption

<table>
<thead>
<tr>
<th>Software</th>
<th>Supported Platforms</th>
<th>Encryption Algorithms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrueCrypt 4.3a</td>
<td>Windows, Linux</td>
<td>AES 256, Serpent, Twofish</td>
<td>Fat16, Fat32, NTFS and Linux</td>
</tr>
<tr>
<td>Des-Rsa</td>
<td>Win 2K, WinXP, Vista</td>
<td>AES 256</td>
<td>Fat16, Fat32, NTFS and Linux</td>
</tr>
<tr>
<td>Drive Crypt</td>
<td>All Windows</td>
<td>AES, Triple AES(768), Blowfish 256,448</td>
<td>Fat16,Fat32, NTFS , Up to 4 passwords for unlocking container</td>
</tr>
<tr>
<td>Ax Crypt</td>
<td>All Windows</td>
<td>AES 128</td>
<td>Integrated shredder</td>
</tr>
<tr>
<td>Cyber Angel</td>
<td>All Windows</td>
<td>AES 128,256, Blowfish 128,448, Two fish 128,256, Triple DES and</td>
<td>Encrypted Partition automaticall y expands</td>
</tr>
</tbody>
</table>
F. Recommendations
A typical recommendation is given below:

- Whole-disk encryption for PCs – PGP Whole Disk Encryption
- Virtual Disk and folder/file encryption
  - Encrypted disk images for Macs
  - Folder encryption using Windows EFS encryption or TrueCrypt
  - TrueCrypt for Pocket PCs and removable media
- Password protect Palm devices and Windows Mobile 5 devices
  - SD Cards are not protected, and therefore a concern.
  - Users advised to change passwords immediately if device is lost or stolen to prevent access to accounts accessed with passwords (calendar and email).
- PC Backup encryption
  - EFS Encryption and MS Backup
  - Symantec Ghost w/encryption
- Enterprise backups are secure in machine room and in transit. Options for enterprise backup are being examined.
- Terminal Services should be used when possible for applications involving
- End user training
  - Security awareness
  - Security training
  - Encryption instructions

III. OTHER DATA SECURITY INITIATIVES

A. Network Security Enhancements
   It has implemented a number of network security enhancements as part of the overall security plan, including a campus-wide firewall strategy, IP-source spoof protection software, and secure wireless.

B. Data in Transit
   The Data Encryption Subcommittee has begun testing e-mail encryption. Under consideration is Open PGP for Enigmail, open source software for encrypting and signing confidential e-mail. e-mail must be encrypted to and from university mail server, additionally, VPN (Virtual Private Network) must be used to encrypt data in transit. Furthermore, access to servers containing sensitive data can be restricted to traffic tunneled through the VPN server.

CONCLUSION

University’s must acknowledges the importance of securing sensitive data stored on computer hard drives and other storage devices. In order to protect privacy, sustain system integrity, and assure availability of data to the appropriate users, Data Encryption Subcommittees must evaluate encryption solutions and recommend a comprehensive approach to implementing a campus-wide encryption policy.

A centrally managed whole-disk encryption solution supplemented with file and folder encryption will help protect the privacy of constituents while minimizing changes to user workflow and behavior. Other initiatives are to increase security awareness, offer additional security training, and to provide solutions for e-mail encryption and digital signatures.

REFERENCES