DATA SECURITY

V.J. RAJA KUMAR[1] ,V.SANTHOSHAMARNATH[1],SWETHA.R[2],
Assistant Professor, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu,India[1]
Student, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[2]
Student , Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[3]

Abstract—A Data security is about keeping your data safe from accidental or malicious damage.Security is a consideration at all stages of your research, particularly if working with disclosive or licensed data. The responsibility to protect data from theft, breach of confidentiality, premature and unauthorized release, and ensure secure disposal is an essential part of a research data management strategy. Nowadays, datum playing vital role in the world economy. So keeping our data is an important aspect.

Keywords: Data, security

I. INTRODUCTION

Data security is about keeping your data safe from accidental or malicious damage. Security has different dimensions. Physical security refers to the status of devices on which data are stored and accessed. Consequently, ensure access to rooms, cupboards, and drawers where data is stored is controlled and anyone with access to disclosive data should sign a non-disclosure agreement outlining the nature of confidentiality, storage conditions, and data retention policies. This will provide formal assurance of secure data handling.

Computers should be password protected, with file permissions controlled so users, depending on their status, can “read only”, “write”, or “execute” files. Enable computer firewalls and keep anti- malware software up-to-date and operational. Computers connected networks should not store sensitive data, unless that data is encrypted, so to minimize network vulnerabilities. Consult with your IT support to establish a digital data security procedure or ask us if you are unsure what support to ask for.

II. PASSWORDS

Passwords are a foundation of security. Getting a good one is a great basis for keeping your data safe, but a weak password is like an unlocked door.

A good password is between eight to fifteen characters long; the more characters in the password the harder it is to guess. Using upper and lower case letters, numbers, and punctuation symbols significantly increases the variation, and thus the strength of your password, although that variation is minimized by picking common letters like vowels, or lower numbers (1, 2, 3), and sequences. Therefore, the more randomly distributed the characters in your password, the better.

A password generator site is useful for randomizing characters and offering hints to remember that password, and if you are unsure about using a computer-generated password, you can always tweak the suggested password by changing a character or two.
An alternative to passwords are pass phrases. Pass phrases are sequences of words or text and are attractive because they are easier for the user to remember, and in terms of complexity and variation, produce longer character strings. However, using an obvious common phrase reduces security. It is better to use a phrase that has private personal meaning and is not in common usage.

Whether it is a pass phrase or password, both suffer from the trade-off between ease of recall and security. A simple password is easy to remember but easier to guess; a harder one is difficult to guess but difficult to remember. It is sensible to adopt a risk strategy with your passwords. The more valuable the content behind the password, the greater the security steps to choose and store a password. Writing down passwords is a solution, but taking care of where you store passwords is a consideration. Possessing a nice, long, normally distributed random password means nothing if written on a post-it note stuck to your monitor. The easiest way to obtain access is not by “brute force attack” but obtaining the password itself through carelessness or deceit. For that reason, if you do write down a password keep it somewhere safe and away from the machine.

III. ENCRYPTION

Encryption is a great research data management tool for secure storage and transmission of files and it is good practice to encrypt any disclosive files and machines or devices that store data.

Encryption maintains the security of data and documentation through an algorithm to transforming information into something unreadable requiring a “key” to decrypt and return to comprehension.

Programs like SafeHouse, TrueCrypt, AxCryptoffer free cross-platform encryption software.

SafeHouse creates a "container" that appears to be just a drive on your computer allowing you to use it as you would use any normal drive. When encrypting a drive, the key size determines the strength of encryption as the number of "brute force" guesses that an attacker needs to make in order to guess the decryption key increases. Advanced Encryption Standard (AES) is a widely recognized encryption standard with key sizes of 128, 192 and 256 recognized as sufficient levels as encryption.

If you are unsure about what to encrypt, a good rule to apply is this: encrypt anything you would not happily send on a postcard. Encryption not only protects files as they transfer between machines, it also ensures files on lost or stolen machines and drives are unreadable to anyone without the encryption key. After all, to lose a machine or memory stick may be regarded as a misfortune; to lose your data looks like carelessness.

IV.DATA AND DOCUMENTATION DESTRUCTION

When a project ends, your research data management responsibilities do not. Disposing of paper or digital copies of data is not as simple as dumping paper into a waste paper basket or pressing the "Delete" key. If sensitive data is no longer needed, paper copies need to be shredded in a crosscut shredder, while digital storage devices need to be overwritten to scramble files.. Overwriting is sufficient; however, it remains the case that the sure secure way to dispose of sensitive digital data is physical destruction of the storage medium. Your institution should offer a service for disposing of confidential waste.

V. DATA BACK-UP

We all run the risk of losing or compromising data through some form of storage failure, but you can - and must - act to mitigate the risk.

Identify a data back-up strategy involving creating multiple copies of data and documentation of which at least one should be an external or off-site back up. Identify important data and documentation to be backed up on a daily basis to a different computer in an off-site location, and consolidate back-ups over time into weekly (for example, keep every seventh day) and monthly (keep the first day of the month) back-ups.

Institutions should have a back-up strategy for data stored on institutional servers, but consultation with institutional IT support is vital to not only identify and address your needs but to highlight possible risks endangering your data.

Never assume your data is being backed-up; verify it is being backed-up. It is good practice to attempt periodically a recovery of previous versions of a file or the data collection. For example, creating a simple test file to save, back-up, delete, and then attempt to recover the data from a back- up version of your data.

There are two principal objectives: secrecy, to prevent the unauthorized disclosure of data; and authenticity to prevent the unauthorized modification of data.Information transmitted over electronic lines is vulnerable to passive wiretapping, which threatens secrecy, and to active wiretapping, which threatens authenticity Passive wiretapping refers to the interception of messages, usually without detection. Although it is normally used to disclose message contents, in computer networks it can also be used to monitor traffic flow through the network to determine who is communicating with whom. Protection against disclosure of message contents is provided by enciphering transformations, and by the cryptographic techniques. Protection against traffic flow analysis is provided by
controlling the endpoints of encryption.

VI. SECURE WORKING STORAGE AND SHARING DURING RESEARCH

Research is increasingly collaborative and characterized by cross-institutional and cross-national collaboration. With the opportunities technology allows for increased collaboration, there come research data management challenges to address. Where you store and how you share your data while you are working on it is one such challenge.

A) External hard disk drives:

While the cost of external hard drives fall, their capacity increases. This means we can store large-scale social science data cheaply and easily. As a short-term solution, external hard drives are a useful storage device. However, a hard disk usually has a life span of three to five years, but one of the factors this depends on is the number of times it is used. Consequently, hard disk drives are not a long-term storage solution.

B)Optical media:

Optical media are writable CD and DVD disks. Optical media has a smaller storage capacity, but is more mobile than external hard drives. The quality of disks varies according to price, but again, even the best are not reliable for long-term storage of more than five to ten years, depending on use. Optical media are also subject

to scratches and dust corrupting the ability to read the disc, while the plastic covering and aluminium in the disc may separate rendering the device useless.

C) Flash devices:

Flash based devices like USB memory sticks are unlike optical and hard disk media because they have no moving parts and simple to connect and disconnect to a computer. Therefore, they are convenient, but their capacity is much smaller, and as a flash device, have a finite number of times upon they can be written/re-written. Furthermore, convenience means they are often poorly stored as everyday items carried around in bags and pockets, which can lead to the device breaking, or being lost. Flash drives are a poor form of storage for anything other than the short-term transfer of files between machines.

D) E-Mail :

Email may feel an intuitive means for easy storage and instant data sharing. However, it produces vulnerability in preserving the confidentiality of data. While sending an email feels analogous to sending a letter by post, it is not. When you click “send”, you are starting a process of copying your message and attachment five or six times to different servers - your host server, your Internet service provider’s content delivery network, then, eventually, the recipient’s computer. For this reason, never email disclosive data unencrypted.

E) “Cloud” based storage:

These are increasingly popular options for researchers, as they are easy to use, access, and often automate useful research data management practices like version control. However, with services like Dropboxor GoogleDrive, be careful to examine “terms of service” agreements. While they may not claim ownership of content, they may claim using the service gives them license to copy and distribute content. Furthermore, your files may be stored on third party servers in places not covered by your national or EU law. Additionally, whilst unlikely, these are commercial services and therefore not necessarily permanent or secure and certainly not suitable for long-term preservation. Check to see if your institution runs its own online storage service.

F) Institutional servers:

If you are a researcher, you should have a storage space provided on your institution’s network server for file storage. The advantage of an institutional server is that it should be professionally backed-up, have reliable access, and be more secure than most alternatives. However, the institution may apply a quota to limit space on servers. Additionally, storage on institutional servers can be problematic for collaborative research particularly when it involves cross-institutional collaboration, as providing access to a network to users from other institutions is complicated. Speak to your IT support to see what institutional support they can provide.

CRYPTOGRAPHIC SYSTEMS

This section describes the general requirements of all cryptographic systems, thespecific properties of public-key encryption, and digital signatures.
A cryptographic systemhas five components:

1. A plaintext message space, if/.

2. A ciphertext message space, C.

3. A key space, .K.

4. A family of enciphering transformations, EK: ~ ~ C, where K ~ .K.

5. A family of deciphering transformations, DK: C ~ ~, where K ~ .K.

Digital signature:

Data security mostly use the digital signature algorithm for security purpose.
A digital signature is a property private to a user or process that is used for signing messages. Let B be the recipient of a message M signed by A. Then A's signature must satisfy these requirements:

1. B must be able to validate A's signature on M.

2.It must be impossible for anyone, including B, to forge A's signature.

3. case A should disavow signing a message M, it must be possible for a judge or third party to resolve a dispute arising between A and B.

Public-key authentication systems provide a simple scheme for implementing

digital signatures. Because the transformation D A is private to A, D A serves as A's

digital signature. The recipient B of a message M signed by A is assured of both sender and data

authenticity. It is impossible for B or anyone else to forge A's signature on another message, and impossible for A to disclaim a signed document. The
inverse transformation E A is public, the receiver B can readily validate the signature, and a judge can settle any disputes arising between A and B.

1. A signs M by computing C = DA(M).

2. B validates A's signature by checking that EA(C) restores M.

3. A judge resolves a dispute arising between A and B by checking whether EA(C) restores M in the same way as B.

Important of data security:

- Physical threats such as a fire, power outage, theft or malicious damage
- Human error such as the mistaken processing of information, unintended disposal of data or input errors
- Exploits from corporate espionage and other malicious activity
- Who has access to what data
- Who uses the internet, email systems and how they access it
- Who will be allowed access and who will be restricted
- Whether or not to use passwords and how they will be maintained
- What type of firewalls and anti-malware solutions to put in place
- Properly training the staff and enforcing data security.

CONCLUSION

There are so many data protection techniques are there. Need to keep our data safe and we should not give our personal details in the internet and should not share our passwords to anyone. Should give strong passwords to our emails to protect our data.

REFERENCES:

[1] Administrators and the Responsible Conduct of Research (n.d.). Collaborative Research.http://ori.dhhs.gov/education/products/rcradmin/topics/colscience/open.shtml

[2] Carusi, A., & Reimer, T. (2010): Virtual Research Environment Collaborative Landscape Study. http://www.jisc.ac.uk/publications/reports/2010/vrelandscapestudy.aspx.

[3] JISC (2013): Infokit: Implementing a virtual research environment(VRE). http://www.jiscinfonet.ac.uk/infokits/vre/.

[4] Katz, J. S., & Martin, B. R. (1997): What is research collaboration? Research Policy, 26(1), 1–18. doi:10.1016/S0048-7333(96)00917-1.

[5]SURF (2011): VRE Starter's Kit. http://wiki.surf.nl/display/VRE/VRE+Starters+Kit.

[6] Westfall, J.E., et al. Locking the virtual filing cabinet: A researcher's guide to Internet data security. International Journal of Information Management (2012), http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.005.

[7]Waksman, Adam; Sethumadhavan, Simha (2011), "Silencing Hardware Backdoors" (PDF), Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, archived (PDF) from the original on 2013-09-28

[8]https://www.staysmartonline.gov.au/Protect-yourself/Doing-things-safely/backups

[9] "Data Masking Definition". Archived from the original on 2017-02-27. Retrieved 1 March 2016.

[10]"data masking". Archived from the original on 5 January 2018. Retrieved 29 July 2016.