A Study of Data Security in Information Management

S. Christal Anand
Assistant Professor, Lourdes Mount College of Engineering and Technology
christalanands@gmail.com

Abstract: - Information security requirements within a society have changed a lot in the last few years. In this era of Face book, Whats App, Twitter and Google maps, where anyone can upload anything in the social media and track anyone's location using GPS, everything is possible. However, we need to be more conscious in security. The introduction of distributed system and the use of networks and communication facilities for carrying data between the terminal user and computer affected the security of information. Network security measures are needed to protect data during their transmission.

I. INTRODUCTION

In the corporate world, various aspects of security are historically addressed separately - notably by distinct and often non communicating departments for IT security, physical security, and fraud prevention. Today there is a greater recognition of the interconnected nature of security requirements, an approach variously known as holistic security, —all hazards management, and other terms.

Inciting factors in the convergence of security discipline include the development of digital video surveillance technologies and the digitization and networking of physical control systems. Greater interdisciplinary co-operation is further evidenced by the February 2005 creation of the Alliance for Enterprise Security Risk Management, a joint venture including leading associations in security (ASIS), information security (ISSA, the Information Systems Security Association), and IT audit (ISACA, the Information Systems Audit and Control Association).

In 2007 the International Organization for Standardization (ISO) released ISO 28000 - Security Management Systems for the supply chain. Although the title supply chain is included, this Standard specifies their requirements for a security management system, including those aspects critical to security assurance for any organization or enterprise wishing to manage the security of the organization and its activities. ISO 28000 is the fore most risk-based security system and is suitable for managing both public and private regulatory security, customs and industry-based security schemes and requirements.

Perception of security may be poorly mapped to measurable objective security. For example, the fear of earthquakes has been reported to be more common than the fear of slipping on the bathroom floor although the latter kills many more people than the former. Similarly, the perceived effectiveness of security measures is sometimes different from the actual security provided by those measures. The presence of security protections may even be taken for the safety itself.

For example, two computer security programs could be interfering with each other and even canceling each other's effect, while the owner believes s/he is getting double the protection. Security Theater is a critical term for deployment of measures primarily aimed at raising subjective security without a genuine or commensurate concern for the effects of that action on real safety. For example, some consider the screening of airline passengers based on static

databases to have been Security Theater and the Computer Assisted Passenger Prescreening have created a decrease in objective security.

II. DATA SECURITY

Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users.[1]

1. Data security technologies

1.1 Disk encryption

Disk encryption refers to encryption technology that encrypts data on a hard disk drive. Disk encryption typically takes form in either software (see disk encryption software) or hardware (see disk encryption hardware). Disk encryption is often referred to as on-the-fly encryption (OTFE) or transparent encryption.

1.2. Software versus hardware-based mechanisms for protecting data

Software-based security solutions encrypt the data to protect it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offer very strong protection against tampering and unauthorized access.

Hardware based security or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS#11 may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two factor authentications). However, dongles can be used by anyone who can gain physical access to it. A newer technology in hardware-based security solves this problem offering full proof security for data.

Working of hardware-based security: A hardware device allows a user to log in, log out and set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as hard disks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by hard disk and DVD controllers making illegal access to data impossible. Hardware-based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on hard disks can be corrupted after a malicious access is obtained. With hardware-based protection, software cannot manipulate the user privilege levels. It is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or performs unauthorized privileged operations. This assumption is broken only if the hardware itself is malicious or contains a backdoor.[2] The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware-based security and secure system administration policies.

1.3 Backups

Backups are used to ensure data which is lost can be recovered from another source. It is considered essential to keep a backup of any data in most industries and the process is recommended for any files of importance to a user.

1.4 Data masking

Data masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel.[3]

This may include masking the data from users (for example so banking customer representatives can only see the last 4 digits of a customer's national identity number), developers (who need real production data to test new software releases but should not be able to see sensitive financial data), outsourcing vendors, etc.

1.5 Data erasure

Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused...

2. International laws and standards

2.1 International laws

In the UK, the Data Protection Act is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. This is particularly important to ensure individuals are treated fairly, for example for credit checking purposes. The Data Protection Act states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared. Data Privacy Day is an international holiday started by the Council of Europe that occurs every January 28.[4]

2.2 International standards

The international standard ISO/IEC 17799 covers data security under the topic of information security, and one of its cardinal principles is that all stored information, i.e. data, should be owned so that it is clear whose responsibility it is to protect and control access to that data. The Trusted Computing Group is an organization that helps standardize computing security technologies. The Payment Card Industry Data Security Standard is a proprietary international information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM and POS cards.[5]

3. Industry and Software

There are several data security software available to be used by consumers and one of the most used data security software with a U.S issued patent is Folder Lock.

III. DATA PRIVACY

Information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Ethnicity
- Privacy breach
- Location-based service and geolocation
- Web surfing behavior or user preferences using persistent cookies

The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information. The fields of computer security, data security and information security design and utilize software, hardware and human resources to address this issue. As the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast of any changes in the law and continually reassess compliance with data privacy and security regulations.[6]

1. Information types

Various types of personal information often come under privacy concerns.

1.1 Internet

The ability to control the information one reveals about oneself over the Internet, and who can access that information, has become a growing concern. These concerns include whether email can be

stored or read by third parties without consent, or whether third parties can continue to track the web sites someone has visited. Another concern is web sites which are visited collect, store, and possibly share personally identifiable information about users.

The advent of various search engines and the use of data mining created a capability for data about individuals to be collected and combined from a wide variety of sources very easily. The FTC has provided a set of guidelines that represent widely accepted concepts concerning fair information practices in an electronic marketplace called the Fair Information Practice Principles. In order not to give away too much personal information, e-mails should be encrypted and browsing of Webpages as well as other online activities should be done trace-less via anonymizers, or, in cases those are not trusted, by open source distributed anonymizers, so called mix nets, such as I2P or Tor - The Onion Router. Email isn't the only internet use with concern of privacy. Everything is accessible over the internet nowadays.[7][8][9]

However, a major issue with privacy relates back to social networking. For example, there are millions of users on Face book and regulations have changed. People may be tagged in photos or have valuable information exposed about themselves either by choice or most of the time unexpectedly by others. It is important to be cautious of what is being said over the internet and what information is being displayed as well as photos because this all can search across the web and used to access private databases making it easy for anyone to quickly go online and profile a person.

1.2 Cable television

The ability to control the information one reveals about oneself over cable television, and who can access that information. For example, third parties can track IP TV programs someone has watched at any given time. “The addition of any information in a broadcasting stream is not required for an audience rating survey, additional de-vices are not requested to be installed in the houses of viewers or listeners, and without the necessity of their cooperation, audience ratings can be automatically performed in real-time.”[10]

1.3 Medical

A person may not wish for their medical records to be revealed to others. This may be because they have concern that it might affect their insurance coverages or employment. Or it may be because they would not wish for others to know about medical or psychological conditions or treatments which would be embarrassing. Revealing medical data could also reveal other details about one’s personal life. Privacy Breach There are three major categories of medical privacy: informational (the degree of control over personal information), physical (the degree of physical inaccessibility to others), and psychological(the extent to which the doctor respects patients’ cultural beliefs, inner thoughts, values, feelings, and religious practices and allows them to make personal decisions).[11] Physicians and psychiatrists in many cultures and countries have standards for doctor-patient relationships which include maintaining confidentiality. In some cases, the physician-patient privilege is legally protected. These practices are in place to protect the dignity of patients, and to ensure that patients will feel free to reveal complete and accurate information required for them to receive the correct treatment. The United States has laws governing privacy of private health information, see HIPAA and the HITECH Act.[12]

1.4 Financial

Information about a person’s financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be sensitive. If criminals gain access to information such as a person’s accounts or credit card numbers, that person could become the victim of fraud or identity theft. Information about a person’s purchases can reveal a great deal about that person’s history, such as places he/she has visited, whom he/she has contacted with, products he/she has used, his/her activities and habits, or medications he/she has used. In some cases, corporations might wish to use this information to

target individuals with marketing customized towards those individual's personal preferences, something which that person may or may not approve.

1.5 Location Tracking

As location tracking capabilities of mobile devices are increasing (Location-based service), problems related to user privacy arise. Location data is indeed among the most sensitive data currently being collected. A list of potentially sensitive professional and personal information that could be inferred about an individual knowing only his mobility trace was published recently by the Electronic Frontier Foundation.[13]

These include the movements of a competitor sales force, attendance of a particular church or an individual's presence in a motel or at an abortion clinic. A recent MIT study[9] by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.[14][15]

1.6 Political

Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not known to anyone other than the voter them self—it is nearly universal in modern democracy, and considered to be a basic right of citizenship. In fact, even where other rights of privacy do not exist, this type of privacy very often does.

1.7 Educational

In the United Kingdom, in 2012 the Education Secretary Michael Gove described the National Pupil Database as a "rich dataset" whose value could be "maximized" by making it more openly accessible, including to private companies. Kelly Five ash of The Register said that this could mean "a child's school life including exam results, attendance, teacher assessments and even characteristics" could be available, with third-party organizations being responsible for anonymized any publications themselves, rather than the data being anonymized by the government before being handed over. An example of a data request that Gove indicated had been rejected in the past, but might be possible under an improved version of privacy regulations, was for "analysis on sexual exploitation".[16]

2. Legality

The legal protection of the right to privacy in general - and of data privacy in particular - varies greatly around the world. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. — Universal Declaration of Human Rights, Article 17 There is a significant challenge for organizations that hold sensitive data to achieve and maintain compliance with so many regulations that have relevance to information privacy.

3. Safe Harbor Program and Passenger

Name Record issues The United States Department of Commerce created the International Safe Harbor Privacy Principles certification program in response to the 1995 Directive on Data Protection (Directive 95/46/EC) of the European Commission. Directive 95/46/EC declares in Chapter IV Article 25 that personal data may only be transferred from the countries in the European Economic Area to countries which provide adequate privacy protection. Historically, establishing adequacy required the creation of national laws broadly equivalent to those implemented by Directive 95/46/EU. Although there are exceptions to this blanket prohibition - for example where the disclosure to a country outside the EEA is made with the consent of the relevant individual (Article 26(1)(a)) – they are limited in practical scope. As a result, Article 25 created a legal risk to organizations which transfer personal data from Europe to the United States.[18] The program has an

important issue on the exchange of Passenger Name Record information between the EU and the US. According to the EU directive, personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.[19]

The European Commission has set up the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries. [20]

The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbor Principles were the result. Notwithstanding that approval, the self-assessment approach of the Safe Harbor remains controversial with a number of European privacy regulators and commentators. [21]

The Safe Harbor program addresses this issue in a unique way: rather than a blanket law imposed on all organizations in the United States, a voluntary program is enforced by the FTC. U.S. organizations which register with this program, having self-assessed their compliance with a number of standards, are "deemed adequate" for the purposes of Article 25. Personal information can be sent to such organizations from the EEA without the sender being in breach of Article 25 or its EU national equivalents. [22]

The Safe Harbor was approved as providing adequate protection for personal data, for the purposes of Article 25(6), by the European Commission on 26 July 2000. The Safe Harbor is not a perfect solution to the challenges posed by Article 25. In particular, adoptee organizations need to carefully consider their compliance with the onward transfer obligations, where personal data originating in the EU is transferred to the US Safe Harbor, and then onward to a third country. The alternative compliance approach of "binding corporate rules", recommended by many EU privacy regulators, resolves this issue. In addition, any dispute arising in relation to the transfer of HR data to the US Safe Harbor must be heard by a panel of EU privacy regulators. In July 2007, a new, controversial, Passenger Name Record agreement between the US and the EU was undersigned. A short time afterwards, the Bush administration gave exemption for the Department of Homeland Security, for the Arrival and Departure Information System (ADIS) and for the Automated Target System from the 1974 Privacy Act.[23]

In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs, complained about the US bilateral policy concerning PNR. The US had signed in February 2008 a memorandum of understanding (MOU) with the Czech Republic in exchange of a VISA waiver scheme, without concerting before with Brussels. The tensions between Washington and Brussels are mainly caused by a lesser level of data protection in the US, especially since foreigners do not benefit from the US Privacy Act of 1974. Other countries approached for bilateral MOU included the United Kingdom, Estonia, Germany and Greece.

4 .Protecting privacy in information systems

As heterogeneous information systems with differing privacy rules are interconnected and information is shared, policy appliances will be required to reconcile, enforce and monitor an increasing amount of privacy policy rules (and laws). There are two categories of technology to address privacy protection in commercial IT systems: communication and enforcement.[24]

4.1Improving Privacy through Individualization

There has been interest in improving computer privacy through individualization. Currently security messages are designed for the "average user", i.e. the same message for everyone. Researchers have posited that individualized messages and security "nudges", crafted based on users' individual differences and personality traits, can be used to further improve each person's compliance with computer security and privacy.[25]

IV. CONCLUSION

There has been interest in improving computer privacy through individualization. Currently security messages are designed for the —average user , i.e. the same message for everyone. Researchers have posited that individualized messages and security —nudges , crafted based on users' individual differences and personality traits, can be used to further improve each person's compliance with computer security and privacy.

REFERENCES

[1] Summers, G. (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.

[2] Waksman, Adam; Sethumadhavan, Simha (2011), "Silencing Hardware Backdoors" (PDF), Proceedings of the IEEE Symposium on Security and Privacy (Oakland, California)

[3] "What is Data Obfuscation".Retrieved 1 March 2016.

[4] Peter Fleischer, Jane Horvath, Shuman Ghosemajumder(2008). "Celebrating data privacy". Google Blog. Retrieved 12 August 2011.

[5] "PCI DSS Definition". Retrieved 1 March 2016

[6] Robert Hasty, Dr Trevor W. Nagel and Mariam Subjally, Data Protection Law in the USA. (AdvocateforInternationalDevelopment, August 2013.

[7] Bergstein, Brian (2006-06-18). "Research explores data mining, privacy". USA Today.Retrieved 2010-05-05.

[8] Bergstein, Brian (2004-01-01). "In this data-mining society, privacy advocates shudder". Seattle Post-Intelligencer.

[9] Swartz, Nikki (2006). "U.S. Demands Google Web Data". Information Management Journal. Vol. 40 Issue3, p. 18

[10] "System for gathering tv audience rating in real time in internet protocol television network and method thereof". FreePatentsOnline.com. 2010-01-14. Retrieved 2011-06-07.

[11] Serenko, Natalia; Lida Fan (2013). "Patients' Perceptions of Privacy and Their Outcomes in Healthcare" (PDF). International Journal of Behavioural and Healthcare Research 4 (2): 101–122

[12] Doctor-Patient Confidentiality: Encyclopedia of Everyday Law Blumberg, A. Eckersley, P. "On locational privacy and how to avoid losing it forever.".EFF.

[13] de Montjoye, Yves-Alexandre; César A. Hidalgo; Michel Verleysen; Vincent D. Blondel (March 25, 2013)."Unique in the Crowd: The privacy bounds of human mobility".Naturesrep.doi:10.1038/srep01376. Retrieve 12 April 2013.

[14] Palmer, Jason (March 25, 2013). "Mobile location data'present anonymity risk'". BBC News. Retrieved 12 April2013.

[15] Fiveash, Kelly (2012-11-08). "Psst: Heard the one about the National Pupil Database? Thought not".The Register.Retrieved 2012-12-12.

[16] A divided Europe wants to protect its personal data wanted by the US, Rue 89, 4 March 2008 (English)

[17] Statewatch, US changes the privacy rules to exemption access to personal data September 2007

[18] Brussels attacks new US security demands, European Observer.See also Statewatch newsletter February 2008

[19] "The Myth of the Average User: Improving Privacy andSecurity Systems through Individualization (NSPW '15) | BLUES". blues.cs.berkeley.edu. Retrieved 2016-03-