International Journal of Research in Science And Technology http://www.ijrst.com/
(IJRST) 2011, Vol. No. 1, Issue No. III, Oct-Dec **ISSN: 2249-0604**

ANALYZING THE COMPUTER SECURITY IN THE MODERN ERA

***Rajesh Kumar, #Dr. G.P. Singh**

**Ph.D. Research Scholar, Singhania University*

#Associate Prof. Govt Dungar College, Bikaner

ABSTRACT

A thriving new field of information security economics provides valuable insights not just into 'security' topics such as privacy, bugs, spam and phishing, but into more general areas of system dependability and policy. This research programme has recently started to interact with psychology. One thread is in response to phishing, the most rapidly growing form of online crime, in which fraudsters trick people into giving their credentials to bogus websites; a second is through the increasing importance of security usability; and a third comes through the psychology-and-economics tradition. The promise of this multidisciplinary research programme is a novel framework for analyzing information security problems—one that is both principled and effective.

INTRODUCTION

The term computer security is used frequently, but the content of a computer is vulnerable to few risks unless the computer is connected to other computers on a network. As the use of computer networks, especially the Internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources.

The major technical areas of computer security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability. Confidentiality means that information cannot be access by unauthorized parties. Confidentiality is also known as secrecy or privacy; breaches of confidentiality range from the embarrassing to the disastrous. Integrity means that information is protected against unauthorized changes that are not detectable to authorized users; many incidents of hacking compromise the integrity of databases and other resources. Authentication means that users are who they claim to be. Availability means that resources are accessible by authorized parties; "denial of service" attacks, which are sometimes the topic of national news, are attacks against availability. Other important concerns of computer security professionals are access control and non repudiation. Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access. Non repudiation implies that a person who sends a message cannot deny that he sent it and, conversely, that a person who has received a message cannot deny that he received it. In addition to these technical aspects, the conceptual reach of computer security is broad and multifaceted. Computer security touches draws from disciplines as ethics and risk analysis, and is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and identity and anonymity in cyberspace.

While confidentiality, integrity, and authenticity are the most important concerns of a computer security manager, privacy is perhaps the most important aspect of computer security for everyday Internet users. Although users may feel that they have nothing to hide when they are registering with an Internet site or service, privacy on the Internet is about protecting one's personal information, even if the information does not seem sensitive. Because of the ease with which information in electronic format can be shared among companies, and because small pieces of related information from different sources can be easily linked together to form a composite of, for example, a person's information seeking habits, it is now very important that individuals are able to maintain control over what information is collected about them, how it is used, who may use it, and what purpose it is used for.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.[1]

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

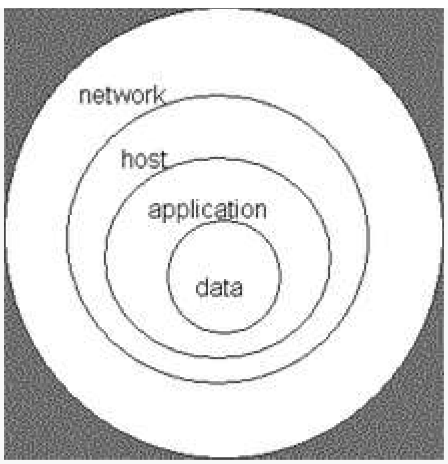
Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

DEFENSE IN DEPTH



Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

REVIEW OF LITERATURE

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over. Public clouds are available from Google.com, Amazon.com, Microsoft, Oracle/Sun, Canonical/Eucalyptus and many other vendors. Private cloud technologies, where the cloud software is loaded on local or in-house server hardware, are available from VMware, Eucalyptus, Citrix, Microsoft, and there are thousands of vendors offering cloud solutions of all sorts. A search for private cloud hosting on Google.com produced 581,000 page results. With all of the hyperbole has come a large swell of early-adopters and developers. This paper is concerned with discovery of the vulnerabilities in the landscape of clouds, discovery of security solutions, and finding evidence that early-adopters or developers have grown more concerned with security.

Security Issues and Solutions in Cloud Computing

This paper concerns security issues and solutions in cloud computing. Cloud computing is a catch-all phrase that covers virtualized operating systems running on virtual hardware on untold numbers of physical servers. The cloud term has consumed High-Performance Computing (HPC), Grid computing and Utility Computing. The Cloud Security Alliance has adopted the definition developed by NIST; a computing in the cloud is a model exhibiting the following characteristics, on-demand self-service, Broad Network Access, Resource pooling, and Rapid elasticity and Measured service (*Cloud Security Alliance Guidance Version 2.1*, 2009, p. 15). This is an area that appears to be growing larger and more pervasive as the benefits of cloud architectures become better understood. More organizations start their own cloud projects and more application developers sign on for cloud development as the hyperbole is shaken out and the real parameters of the key technologies are discovered and perfected. The basic areas of cloud vulnerability are similar to the standard issues that surround networking and networked applications. The issues specific to cloud architectures include network control being in in the hands of third parties and and a potential for sensitive data to be available to a much larger selection of third-parties, both on the staff of the cloud providers, and among the other clients of the cloud.

The quick adoption of the cloud model is plain in the success of the Amazon Elastic Cloud Computing (EC^2) product, the buy-in from IBM with their backing of the highly concurrent, massively parallel language X-10 (Saraswat, Vijay, 2010) and Microsoft's investment in its Azure cloud (Qiu et al., 2009). Janine Milne reported that eight of ten businesses surveyed in the UK were opting for private cloud initiatives rather than public cloud projects and they stated the issues of concern to be data security in transit, in storage or during processes (Milne, 2010). It is plain that the field is full and the harvest for the IT security profession and IT in general are excellent.

The literature available on cloud security is plentiful, and there is enough higher-quality work to develop a conceptual framework for security issues and solutions

Data Verification, Tampering, Loss and Theft Solutions

Raj, Nathuji, Singh and England (2009) suggest resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache (Raj, Nathuji, Singh, & England, 2009, p. 80). Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason (Hayes, 2008, p.(Hayes, 2008, p. 11). Would cloud-providers and clients have custody battles over client data?

Privacy and Control Solutions

Hayes (2008) points out an interesting wrinkle here, Allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to a documents if you fail to pay a bill (Hayes, 2008, p. 11). The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

Physical access solutions

One simple solution, which Milne (2010) states to be a widely used solution for UK businesses is to simply use in-house private clouds (Milne, 2010). Nurmi, Wolski, Grzegorczyk, Obertelli, Soman, Youseff, & Zagorodnov show a preview of one of the available home-grown clouds in their (2009) presentation. The Eucalyptus Open-Source Cloud-Computing System (Nurmi et al., 2009).

MATERIAL AND METHODS

These tools are used in minimizing the risk and to make password more memorable to users and include multi-function smart cards that store multiple passwords on a single token.

Enhanced tokens include multi-function smart cards that store multiple passwords on a single token and can perform other tasks, such as employee identification (employee identity card) or cafeteria debit. For wireless convenience, new security tokens will contain a Radio Frequency Identification tags (RFID) or Bluetooth chip, both for wireless detection in the proximity of a reader. PDAs will also be enhanced with hardware and software to securely store passwords and other secure or private information.

New and Multi-modal biometrics attempt to address some of the shortcomings of current biometric solutions. Multi-modal biometrics combine different biometric modalities to strengthen security, reduce false rejections, and provide alternatives to the user. New biometrics includes gait recognition, infrared capture of blood vessel patterns, and implantable chips.

CONCLUSION

Here are three main points which should be discussed in order to improve student's computer security. First of all, students should install and update antivirus programs regularly. Before opening emails, especially those which are from unknown persons, students should scan the attachments first. Passwords should be set for operating systems in computers to avoid others accessing these computers. Afterwards, universities should set up some curriculum on how to protect personal computers. How to operate and maintain antivirus software should be a topic of this curriculum. The existence of security threats from viruses, and how to reduce the risk of these, should also be taught in this curriculum. Students need know not only antivirus programs but also skills for fixing computers.

REFERENCES

Berre, A. J., Roman, D., Landre, E., Heuvel, W. V. D., SkÃ¥r, L. A., UdnÃ¦s, M., Lennon, R., et al. (2009). Towards best practices in designing for the cloud. In *Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications* (pp. 697-698).

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). Cloud security is not (just) virtualization security: a short paper. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 97-102).

Bishop, Matt (2004). *Computer security: art and science*. Addison-Wesley.

Feltus, Christophe (2008). *Preliminary Literature Review of Policy Engineering Methods - Toward Responsibility Concept*. Proceeding of 3rd international conference on information and communication technologies : from theory to applications (ICTTA 08), Damascus, Syria; *Preliminary Literature Review of Policy Engineering Methods - Toward Responsibility Concept*.

McLean, John (1994). "Security Models". *Encyclopedia of Software Engineering*. **2**. New York: John Wiley & Sons, Inc. pp. 1136–1145.

Allen, Julia H. (2001). *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley.

Krutz, Ronald L.; Russell Dean Vines (2003). *The CISSP Prep Guide* (Gold Edition ed.). Indianapolis, IN: Wiley.

Layton, Timothy P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications. .

McNab, Chris (2004). *Network Security Assessment*. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.

Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: Auerbach publications.

Peltier, Thomas R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.

White, Gregory (2003). *All-in-one Security+ Certification Exam Guide*. Emeryville, CA: McGraHill/Osborne. ISBN 0-07-222633-1.

Dhillon, Gurpreet (2007). *Principles of Information Systems Security: text and cases*. NY: John Wiley & Sons. ISBN 978-0471450566.