VIOLATES COMPUTER SECURITY FOR LITTLE REASON BEYOND MALICIOUSNESS OR FOR PERSONAL GAIN

***Rajesh Kumar, #Dr. G.P. Singh**
**Ph.D. Research Scholar, Singhania University*
#Associate Prof. Govt Dungar College, Bikaner

ABSTRACT

Illicit tempering of computer systems (computer misuse) takes many forms and the most common are probably hacking and computer viruses. Hacking generally refers to activity of gaining unauthorized access to a computer system or network. Computer viruses generally refer to programs which replicate themselves, delete stored information or alter the stored information from the infected computer. Hacking is often the first step in a computer misuse instance. Once a hacker has managed to gain unauthorized entry to a computer system he or she can then try to reprogram the system, delete or modify the data contained therein.

INTRODUCTION

Information brokers have been around for decades, however, a new breed of information broker has emerged in recent years; the kind that sells personal information to anyone requesting it electronically via the Internet.

People search and genealogy websites have come under fire and some consumers are concerned that personal information online can be used to commit identity theft. Privacy advocates have become extremely concerned about the ease with which people can obtain personal information online.

The Impact of hacking activities on internet infrastructure can also be broadly classified into different categories viz. DNS Hacking Attacks, Routing Table Poisoning Attacks, Packet Mistreatment Attacks, Denial of Service (DoS)Attacks.

DNS attacks have illustrated the lack of authenticity and integrity of the data held within DNS as well as in the protocols that use host names as an access control mechanism.

Routing tables are used to route packets over the Internet. They are generated by exchange of routing information or updates between routers. Poisoning attacks refer to the malicious modification or "poisoning" of routing tables. This can be achieved by maliciously modifying the

routing information update packets sent by the routing protocols. This can result in wrong entries in the routing table and could lead to a breakdown of one or more domains of the Internet.

In packet mistreatment attacks the malicious router mishandles packets, thus resulting in congestion, denial of service, and so on. The problem becomes intractable if the router selectively interrupts or misroutes packets resulting in triangle routing, i.e. loop formation.

In Denial-of-Service-Attack, the packets are routed correctly but the destination becomes the target of the attackers. In a typical DoS attack, the attacker node spoofs its IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks are typically used to take important servers out of action for a few hours, resulting in DoS for all users served by the server. It can also be used to disrupt the services of intermediate routers.

There are various state-of-the-art technologies for information security includes Biometric security solutions, Honey Pot Decoys and Padded Cells, Tokens, Cryptography and Digital signature technologies etc.

Biometric technologies are available today that can be used in security systems to help protect assets. Biometric technologies vary in complexity, capabilities, and performance and can be used to verify or establish a person's identity. Leading biometric technologies include Facial recognition, Fingerprint recognition, Hand geometry, Iris recognition, Retina recognition, Signature recognition, Vein recognition, Voice recognition, DNA Fingerprint, Deep tissue illumination & Keystroke pattern etc. Biometric technologies have been used in federal applications such as access control, criminal identification, and border security.

In Honey Pot Decoys and Padded Cells the anonymity of the Internet that allows identity thieves to hide conceal their true identity so effectively can be a double-edged sword used against them.

A token is a hardware or software device carried by, or in possession of, a computer user. The token contain an electronically recorded and encrypted password. Alternatively, it may have an on-board processor that can store and retrieve such a password when needed.

Cryptography has a variety of purposes and requires different kinds of key management for its three applications in communications, storage, and digital signatures. In communications, communicators use cryptography to protect information in transit when it is particularly vulnerable (i.e., going through the cyberspace) because the senders and receivers typically do not have control over the communication route. This application requires short-term protection by encrypting the information before it is sent, and decrypting it upon arrival. Sender's systems may generate keys or receive keys from the intended receiver for short-term use.

REVIEW OF LITERATURE

The various technologies used for information security have been studied and a novel biometric approach used for combating terrorism has been proposed. A review of the digital signatures based on PKI technology has been made. A review of Information Technology Act 2000 and various sections of the act related to digital signatures, their legal meanings, digital signature

certificates, issue/suspension/revocation of digital signature certificate and various certifying authorities for Information Technology rules have been reviewed.

In the field of information technology, there is always possibility for improvement and progress especially with respect to authentication, cryptography and privacy enhancing systems. As a step forward, certain ongoing projects like graphical password, Enhanced Token and Multi-Modal Biometrics provide the provision of a higher level of security that minimizes the risk of hacking the identity on the internet.

Graphical passwords which claim to be more memorable to users. The HumanAut project at Carnegie Mellon University requires the user to choose the pictures he/she has memorized from a sequence of images.

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.

MATERIAL & 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.

RESULTS

The various technologies used for information security have been studied and a novel biometric approach used for combating terrorism has been proposed. A review of the digital signatures based on PKI technology has been made. A review of Information Technology Act 2000 and various sections of the act related to digital signatures, their legal meanings, digital signature certificates, issue/suspension/revocation of digital signature certificate and various certifying authorities for Information Technology rules have been reviewed.

DISCUSSION

Minimizing Recurrences: Guidelines for Information Disclosure

(i) People are encouraged to request and use password-protected credit cards, and bank and phone accounts. To avoid using easily available information like their mother's maiden name, their birth date, the last four digits of their SSN, their phone number, or a series of consecutive numbers.

(ii) People must refrain from giving out their personal information on the phone, through emails, or over the Internet unless they have initiated the communication or are sure they know who they are dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information. Before consumers share any personal information, they must confirm that they are dealing with a legitimate organization.

(iii) People should be careful when storing their financial records, birth date, and bank account numbers on their computer, and should ensure that virus protection software should be updated regularly, and patches for the operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of their computer files or passwords. Ideally, virus protection software should be set to automatically update each week.

(iv) People are recommended to use firewall programs, especially if they use a high speed Internet connection like cable, DSL that leaves their computer connected to the Internet 24 hours a day. The firewall program will allow them to stop uninvited and unauthorized access to their computer.

(v) It is advisable not to open files sent from an unknown source or a stranger, or click on hyperlinks or download programs from untrustworthy sources. People should be careful about using file-sharing programs. Opening a file could expose their system to a computer virus or a program known as "spyware", which could capture their passwords or any other information as they type it.

(vi) Consumers and businesses are encouraged to use a secure browser and encryption software when entering into online transactions or sending their personal information to trusted sites.

PROPOSED WORK

A novel approach based on biometric that can be used for combating terrorism has been proposed. The proposed solution presents a simplified travel plan for passengers based on biometrics and also elaborates how biometric data sharing can be done among different airports. A security scheme based on biometric screening based on multi-pass security checks has been depicted. The present thesis deals with the various threats related to information security.

CONCLUSION & FUTURE WORK

In the field of information technology, there is always possibility for improvement and progress especially with respect to authentication, cryptography and privacy enhancing systems. As a step forward, certain ongoing projects like graphical password, Enhanced Token and Multi-Modal Biometrics provide the provision of a higher level of security that minimizes the risk of hacking the identity on the internet.

Graphical passwords which claim to be more memorable to users. The Human Aut project at Carnegie Mellon University requires the user to choose the pictures he/she has memorized from a sequence of images.

REFERENCES

1. Sterling, Bruce (1993). "Part 2(d)". *The Hacker Crackdown*. McLean, Virginia: IndyPublish.com. p. 61. ISBN 1-4043-0641-2.
2. Blomquist, Brian (May 29, 1999). "FBI's Web Site Socked as Hackers Target Feds".*New York Post*. Retrieved on October 21, 2008.
3. S. Raymond, Eric. "Jargon File: Cracker". Retrieved 2010-05-08. "Coined ca. 1985 by hackers in defense against journalistic misuse of hacker"
4. Tim Jordan, Paul A. Taylor (2004). *Hacktivism and Cyberwars*. Routledge. pp. 133–134.ISBN 9780415260039. "Wild West imagery has permeated discussions of cybercultures."
5. Thomas, Douglas. *Hacker Culture*. University of Minnesota Press. p. 90.ISBN 9780816633463.
6. Clifford, Ralph D. (2006). *Cybercrime:The Investigation, Prosecution and Defense of a Computer-Related Crime Second Edition*. Durham, North Carolina: Carolina Academic Press.
7. Wilhelm, Douglas. "2". *Professional Penetration Testing*. Syngress Press. p. 503.ISBN 9781597494250.

8. Moore, Robert (2005). *Cybercrime: Investigating High Technology Computer Crime*. Matthew Bender & Company. p. 258. ISBN 1-59345-303-5.Robert Moore
9. Moore, Robert (2006). *Cybercrime: Investigating High-Technology Computer Crime*(1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 9781593453039.
10. Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press.ISBN 9780816633463.
11. Andress, Mandy; Cox, Phil; Tittel, Ed. *CIW Security Professional*. New York, NY: Hungry Minds, Inc.. p. 638. ISBN 0764548220.
12. "Blue hat hacker Definition". *PC Magazine Encyclopedia*. Retrieved 31 May 2010. "A security professional invited by Microsoft to find vulnerabilities in Windows."
13. Fried, Ina (June 15, 2005). ""Blue Hat" summit meant to reveal ways of the other side".*Microsoft meets the hackers*. CNET News. Retrieved 31 May 2010.
14. Markoff, John (October 17, 2005). "At Microsoft, Interlopers Sound Off on Security". *New York Times*. Retrieved 31 May 2010.
15. Hacking approach
16. "Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution ..." (Press release). United States Attorney's Office, Central District of California. 9 August 1999. Retrieved 10 April 2010.
17. Boyd, Clark (30 July 2008). "Profile: Gary McKinnon". BBC News. Retrieved 2008-11-15.
18. Staples, Brent (May 11, 2003). "A Prince of Cyberpunk Fiction Moves Into the Mainstream". *The New York Times*. Retrieved 2008-08-30. "Mr. Gibson's novels and short stories are worshiped by hackers"[*dead link*]