Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 23 No. 1-2018
ISSN:1813-1786 (Print) 2313-7770 (Online)

A Framework for the Privacy and Security Issues of Web Based Systems

G. Qaisar[1], S. Farid[2], M. Pasha[3], M. Qadir[4], M. Alam[5]

[1,3] *Information Technology Department, Bahauddin Zakariya University, Multan, Pakistan*
[2,4] *Computer Science Department, Bahauddin Zakariya University, Multan, Pakistan*
[5] *ICCC, Informatics Complex, H-8, Islamabad, Pakistan*
[2]shahidfarid@bzu.edu.pk

Abstract-Along with tremendous increase in use of web applications, the vulnerabilities associated with Web Based Applications Systems (WBAS) are also arising. As Internet is fundamental for accessing web based systems which is inherently an insecure medium. Hence, websites are potential target for various types of cybercrime activities including data breaches, buffer overflow, ransom ware, and fake technical support scams. Therefore, this study intends to identify crucial security challenges and threats encountered by the WBAS. Furthermore a taxonomy classifying the identified challenges into two major categories including client side and website attacks has been formulated. Additionally, a framework has been proposed in order to prevent various security threats on both client and website perspectives. Intensive literature has been conducted to collect the appropriate literature by deploying various devised search strings on the targeted databases. More than 40 research articles, case studies and observations of the researchers published in well renowned journals and conferences have been critically reviewed for the categorization of security threats into respective dimensions. Significance of the proposed framework for the theory and practice is also discussed.

Keywords-Web system, Client Side Security, Server Side Security, System Security, Security Threats, Secure Framework.

I. INTRODUCTION

Advancement in information technology has connected the people through Internet. Internet and the web technologies are the sources of communication, online earning and information sharing. The World Wide Web has occupied a prime place in society, facilitating incredible amount of information to diversified groups of people [i][ii]. Various services like e-banking, e-business, e-learning, e-commerce and etc. have been provided utilizing web to extend their services and facilities to the general people. At the same time, there is rise in the number and types of cyber-attacks due to rapid inclination to the adoption of these online services [iii]. Online applications or technologies are typically exposed to security threats such as worms, crackers, viruses, spoofing, and password-sniffing [iv].

Internet is growing rapidly and web applications have become a common way to provide vital services to the users and customers. On the other hand, they also become an attractive target for attackers. People are sharing their sensitive information like ID's, passwords, transactions codes and personal information. If their system is vulnerable, their information can be compromised by the intruder or attacker. According to Security report by Symantec Corporation one in eight web applications is seriously vulnerable [v]. Different attacks are arising from time to time to expose vulnerabilities and flaws in the web applications. It has been claimed in a recent report of Internet Security Threat that approximately more than 229,000 attacks are being launched against websites daily and unpatched vulnerabilities are being contained by 76 percent websites [iv]. Therefore, various counter measures are deployed for making the system secure but still there are lots of vulnerabilities. In order to develop and deploy a secure environment for both client and server communication, the threats that could be encountered by the web applications must be identified first. After successful identification of security threats countermeasures could be devised for making system secure. The traditional web based systems is being depicted by Fig. 1 in which user and server are connected through internet. User sends request to server and server will reply back to user or client. In this scenario, the vulnerabilities are expected to arise both in communication channel and within the network as well. User or client side threats are different whereas server side threats can be different. Therefore, this study intends to formulate a taxonomy classifying the identified challenges into two major categories including client side and website attacks following a systematic literature review which has never been done in this scenario. Distinctive methodologies are required to be utilized to exterminate various threats. This study describes client side attacks and server side attacks and their measures.

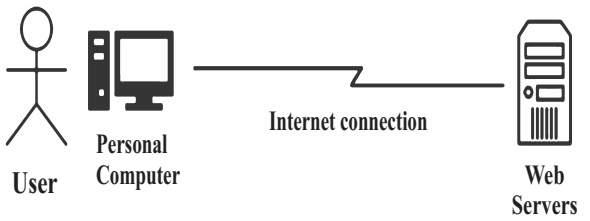

Fig. 1. Traditional web based system

A lot of studies have been conducted in order to gage security of web based system. Various researchers have addressed diverse aspects of security issues. They have tried to make a larger or complete picture of the security issues. An effort is made by [i] but for accessibility perspective only, highlighting the client side attacks. The cryptographic and access control mechanism are being highlighted by [vi],[vii]. Whereas [viii] only deals with the computer viruses. However, [ix] delineates about social engineering attacks and the preventions with the help of seminars and social awareness programs. A study has been presented by [x] in order to protect web applications, by keeping networks secure from possible attacks. Some authors have proposed a security model that implements confidentiality and authentication with Zero Knowledge Protocol (ZKP) and Advanced Encryption Standards (AES) enabling to prevent against Man in Middle attack. Moreover, a security model has been proposed by [xi] that improves the access control and Internet security, with cryptographic techniques and defensive programming practices. Furthermore, various security threats have been explored by [xii] that discusses cyber security technologies for protecting the Internet. The authors also suggest a privacy risk model to assist the upcoming risks. In [xiii] authors describe the two sides of security like browser security and web application security. But the effort of authors is a bunch of tips and techniques that should apply to web based application to keep them secure against vulnerabilities. Owing to lack of wide perspective in information security our contribution is proposition of the taxonomy for the security issues encountered by the web based application systems. Moreover, a framework is also proposed in order to prevent the web based applications from possible security threats and vulnerabilities.

This paper is composed as Section 2 illustrates materials and methods adopted to conduct this study. Section 3 delineates results and discussions comprising of a) formulation of the Taxonomy of security issues of web based applications and b) proposition of framework for the prevention of web based applications from security threats and Section 4 describes the concluding remarks.

II. Materials and Methods

An intensive literature review regarding security and privacy issues of WBAS has been conducted. Various synonyms with different combinations of searching strings were formulated in order to identify maximum issues reported in the literature. More than 40 published research articles, case studies from different well-renowned conferences and journals were reviewed to gather the targeted issues encountered by the security of WBAS.

A. Search String

Following search strings are formulated to explore the state of the art literature;

{Security} AND {(issues) OR (challenges) OR (vulnerabilities) OR (hurdles) OR (barriers) OR (risks) OR (threats)} AND {of} AND {(web based) OR (online) OR (real time)} AND {systems}

B. Search Databases

Well-renowned data bases were explored in order to identify as many as published articles of the targeted domain of this study. The targeted databases are illustrated in Table I.

TABLE I
Targeted Databases

Source	Acronym
IEEE Software	IEEE SW
ACM	TOSEM
Springer Link	SL
Science Direct	Elsevier

III. Results and Discussion

This work explores main security threats and attacks those are challenge for web based systems. The identified challenges are classified into client side and website attacks to develop a taxonomy. Finally a framework has been proposed in order to prevent various security threats and attacks on both client and website perspectives. Identified issues along with respective dimensions are summarized in Table 2 and Table II given in Appendix-A.

A. Taxonomy of Security Issues

A taxonomy of the critical security issues encountered by the web based application systems has been devised. There are two major stakeholders in a web based system that are clients and websites. Therefore attacks on web based system have been categorized in these two major dimensions. These dimensions are client's side and web site side attacks and are illustrated in Fig. 2. Furthermore, the taxonomy is designed on the basis of categorization of attacks. The identified issues are placed in these categories on the basis of observations, experiences and opinions of the researchers from state of the art literature. These dimensions are elaborated in detail in next sub-sections

Attacks on web based system have been categorized in two major dimensions on the basis of observations, experiences and opinions of the researchers from state of the art literature. Furthermore, the taxonomy is designed on the basis of categorization of attacks. These dimensions are client's side and web site side attacks and are illustrated in Fig. 2. These dimensions are elaborated in detail as follows;

i. Client Side Attacks

The threats that clients have to face in web based system are named as client side attacks. Some of the common attacks that a client has to face are described in this section.

a) Social engineering: The term "social engineering" is very famous in information security system. It is a psychological manipulation in which a person can access information from another person [xiv]. The goal of a social engineer is to have access sensitive information about protected data. Social engineer can be a hacker that can manipulate the user and can hack the information. Dumpster diving known as trashing is a technique like social engineering in which the information can be gathered form trash like recycle bin and this is due to poor operational security [xv].

b) Hacking: Hacker is the person who has knowledge of low level language. He is proficient in compromising a client's system [xvi]. If a hacker can gain access to a computer system, he can modify the confidential data [xvii]. Hacker is a person whose intention is to breach security and exploit vulnerability in computer systems.

c) Viruses: Computer virus is program that is created to harm computer system. Viruses are most dangerous for the client's computer system. These can harm computer functionality. They can build insecurity for the computer system. There are different types of viruses, like Trojan horse, email virus, boot sector virus and many others that can harm a computer's functionality and integrity of data can be compromised [xviii] [xix] [xx].

d) Session hijacking: Session hijacking, also called cookie hijacking is the way to misuse of a legal computer session. Attacker hijack the session to have unauthorized access to the computer system or information [ii]. In session hijacking, when user's session has been accessed through permitted way, attacker then masquerade as that legal user and attacker can do anything that authorized user can do on the network [xxi].

e) Weak authentication: Authentication based on the password is the extensively used mechanism in the individual as well as distributed environments. People normally used easy to recall passwords that are weak passwords [xxii]. Many attacks like dictionary attack can break these types of passwords (easy to recall) [xxiii].

ii. Website Attacks

This section describes attacks that create malfunctioning in the web system. In given taxonomy different categorized threats under this category are mentioned in Fig 2.

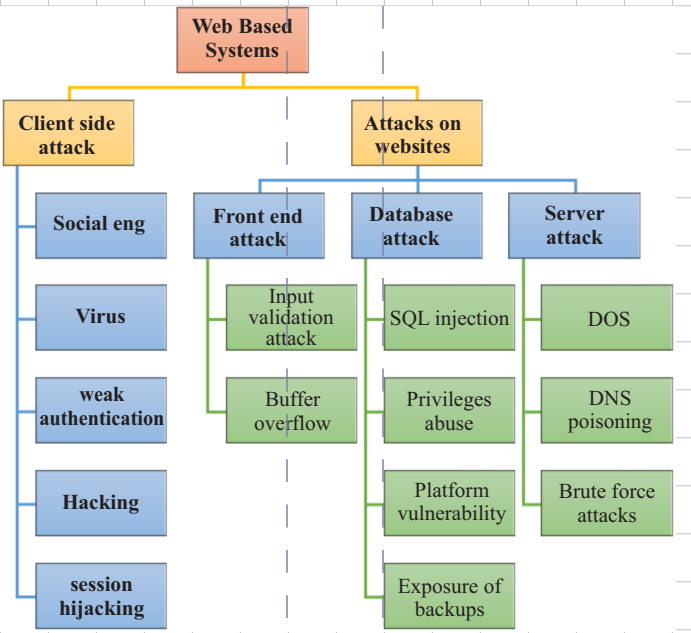

Fig. 2. Attacks on web applications

a) Front end attacks: Attacks that are related to the front end of the system are named as front end attacks. In this section, we describe some common attacks on front end.

Input validation attacks: Input validation attack is very common attack in web based applications. In this type, attacker deliberately sends unfamiliar input for creating malfunctioning in the web based system. This attack occurs when the data from the web desires is not legalized before used by web based system. This attack is attempted to compromise the back end of the web based system by an attacker [xxiv].

Buffer overflow: Buffer overflow is the type of anomaly that deals with a program, when writing input in the buffer overflow. The data will overflow and overrun's the boundary of the buffer. Owing to this problem, the adjacent memory will overwrite. This is the way to violate the memory safety [xxv]. Buffer overflow attacks when the program or software writes extra information or data rather than the assigned memory. Buffer overflow attack is really simple and attacker can easily exploit system with this attack [xxvi]. Conventional buffer overflow attacks are used to disrupt the common execution of the program. This attack can redirect a normal program to the infected code that was not written by the original programmer [xxvii].

b) *Database Attacks:* Different types of attacks on database to create malfunctioning are discussed below.

SQL Injection: SQL injection is the injection attack on web system, in which intruder or attacker execute malicious SQL statements that control the database server. SQL injection targets the dynamic web system that contains database services too [xxvi]. In this attack, intruder gives larger queries to the web server that disturbs the normal execution, and the result will be also different from the original one [xxix].

Privileges Abuse: Users are granted privileges to access the database. When the user exceeds from these privileges it is called privilege abuse. The privileges can be abused for the malicious purpose and to harm database server [xxx].

Platform Vulnerability: Vulnerable operating system and software can lead to the data corruption and DoS. Viruses and worms can also spread due to platform vulnerability. Unauthorized access and privileges abuse are due to platform vulnerability [xxxi].

Exposure of Backup: We create backup of database for any emergency case. In some cases, backup database in which it is stored is often kept completely vulnerable from attack. If the backup of data is theft, then the all sensitive information will be breached [xxxii].

c) *Server Attacks:* Server attacks are used to breach the security of server. It has severe effect and can halt the complete system as server is the controlling component of WBAS. These attacks are attempted to have illegal access to the sensitive or complex data or information and to disrupt normal communication between client and user.

DoS: DoS (Denial of Service) is an attack type that is used to destruct access to the network applications and data is not accessed to the original users. DoS may be formed with the help of many techniques like Ping-of-death and the teardrop attacks are used for exploiting the system [xxxiii]. In DoS attack, attacker crash server normal communication with the intended user.

DNS Poisoning: DNS spoofing or DNS cache poisoning is the type of attack in which incorrect IP address is sent to the DNS server. A DNS server interprets the human readable domain name to IP address. IP address is used to direct communication between intend nodes. If the server doesn't know the request of the user, it will redirect the request to another server. For saving time server will remember that request in its cache and another request will follow for that particular address. Then server will reply him/her from saved address. When server gets the false translation and saves that translation into its cache then it is measured as poisoned and it will answer the incorrect reply to the user. This type of attack is used to redirect the user from the authentic site to attacker's site. Attacker spoofs the IP address from the targeted site and replace it with that IP that is under control of him [xxxiv].

Brute Force Attacks: Brute force attacks are the type of attack in which attacker tries to get information from illegal method by a software or program to decrypt message like secure passwords [xxxv]. Dictionary attacks can also be used to get decrypted data [xxxvi].

B. Proposed Framework

Possible prevention methods that can help to tackle threats and vulnerabilities encountered by web based system can be avoided by adopting the proposed security framework.

Different countermeasures can be adopted for both the client and website attacks that are illustrated in

Fig. 3. The proposed framework deploys various techniques to confront vulnerabilities from possible threat to web based systems. A client encounters various attacks like social engineering, hacking and viruses, however, these can be mitigated with proper training, utilizing security firewalls, protecting with anti-viruses and awareness about fraudulent activities on the Internet [xxxvii][xxxviii][xxxix].

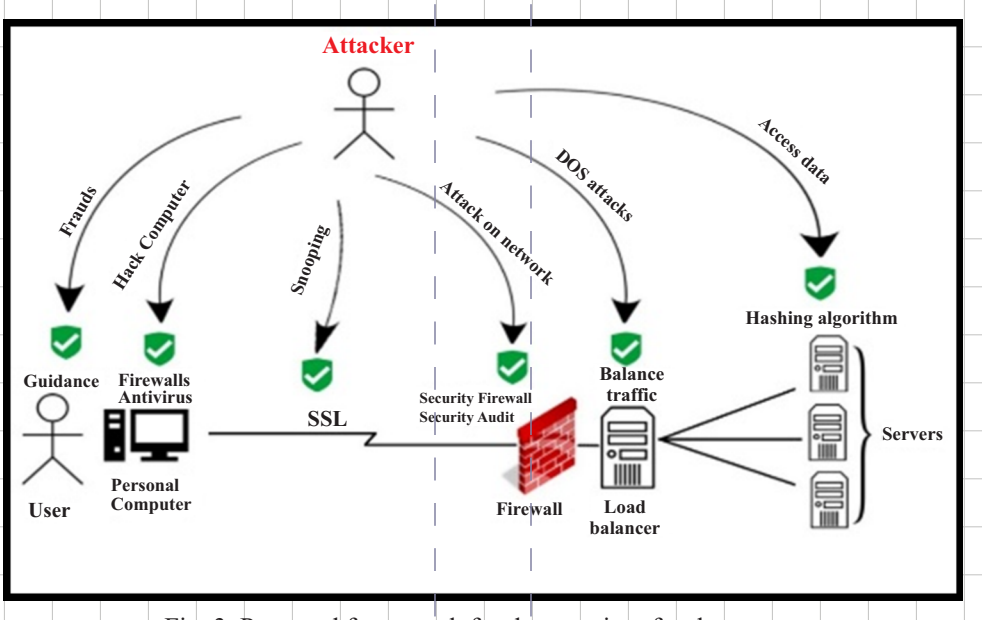

Fig. 3. Proposed framework for the security of web systems

Attacker attempts to snoop network and access sensitive information of user. The SSL provide secure transmission of data on network by using HTTPS. HTTPS (secure hypertext transfer protocol) is a communication protocol that transmits encrypted data from client computers to World Wide Web [xl]. On server side security firewalls and strong security audit can protect the intruder's attacks. Load balancer and IPsec can protect against DoS attack [xli]. Secure authentication and secure password policy can protect against unauthorized access of the intruder. If the system is compromised by the attacker the cryptographic techniques [xlii] and hashing algorithms can keep these safe [xliii]. Secure browser can prevent from the attacker to breach your system security [xliv].

a) Significance

Proposed security framework is applicable for both stakeholders' clients and websites. Clients can access WBAS without any fear while software engineers can get guideline for a secure web based application. Software engineers, web designers or web developers may get benefit considering the week points highlighted by the proposed framework while designing a secure web based application. On the other hand devised framework can act as a road map for an ordinary user in order to understand the possible loop holes from where an intruder can breach the security and privacy of information.

IV. Conclusion

The internet environment is globally open, hence the attackers are omnipresent. Various types of cyber-attacks and vulnerabilities are there in web based environment. Now a days web is widely used for many reasons like e- commerce, e- learning and e- banking. There are many threats that a client has to face on internet. For protecting the privacy and security of the client, the web application is necessary. A protected web based system has to deploy security dimensions to handle the vulnerabilities. If we meet the security dimension, we can protect the customer as well. To tackle security attacks and threats is really a big task. In this paper, we have described different threats on the web based system and the counter measure for those threats. A secured platform not only protects the assets of the client but also increases the trust for that web application.

Reference

[i] J. B. D. Joshi, W. G. Aref, A. Ghafoor and E. H. Spafford, "*Security models for web-based applications",* Communications of the ACM, 2001. 44(2): p. 38-44.

[ii] M. Zviran, C. Glezer, and I. Avni, "*User satisfaction from commercial web sites: The effect of design and use".* Information & management, 2006. 43(2): p. 157-178.

[iii] P. L. Eswari, "*A process framework for securing an e-learning ecosystem". International Conference forInternet Technology and Secured Transactions (ICITST), 2011*. 2011. IEEE.

[iv] M. D. Vivo, G.O. de Vivo and G. Isern, "*Internet security attacks at the basic levels"*. ACM SIGOPS operating systems review, 1998. 32(2): p. 4-15.

[v] A. A. Noureddineand M. Damodaran,"*Security in web 2.0 application development"*. Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services. 2008. ACM.

[vi] A. Herzberg, Y. Mass, J. Mihaeli, D. Naor and Y. Ravid. "*Access control meets public key infrastructure, or: Assigning roles to strangers"*. 2000 IEEE Symposium on Security and Privacy, 2000. S&P 2000. IEEE.

[vii] L. F. Cranor, "*Internet privacy"*. Communications of the ACM, 1999. 42(2): p. 28-38.

[viii] X. Chen, M. J. P. Jimenez and L. V. Cabrera. "*Computing with viruses"*. Theoretical Computer Science, 2016. 623: p. 146-159.

[ix] F. Mouton, L. Leenen, and H.S. Venter, "*Social engineering attack examples, templates and scenarios"*. Computers & Security, 2016. 59: p. 186-209.

[x] A. L. A. Bajjariand L. Yuan, "*Optimized authentication scheme for web application"*. 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA), 2016. IEEE.

[xi] A. M. Osman, A. D. Allah, and A.A.M. Elhag,"*Proposed security model for web based applications and services"*. 2017. IEEEInternational Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), 2017.

[xii] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, and B. Lepri (2018), *"The Privacy Implications of Cyber Security Systems: A Technological Survey*". ACM Computing Surveys (CSUR), 51(2), 36.

[xiii] I, Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. A. A. Qudah, and A. A. Omari, "*Web and Database Security*". Practical Information Security. Springer, Cham 2018. pp. 139-157.

[xiv] T. Thornburgh, "*Social engineering: the dark art"*. Proceedings of the 1st annual conference on Information security curriculum development. 2004. ACM.

[xv] K. D. Mitnick, and W.L. Simon, "*The art of deception: Controlling the human element of security"*. 2011: John Wiley & Sons.

[xvi] S. Furnell, and M.J. Warren, "*Computer hacking and cyber terrorism: The real threats in the new millennium?"*. Computers & Security, 1999. 18(1): p. 28-34.

[xvii] R. W. Taylor, E.J. Fritsch, and J. Liederbach, "*Digital crime and digital terrorism"*. 2014: Prentice Hall Press.

[xviii] R. Peluso, A. Haase, L. Stowring, M. Edwards and P. Ventura, "*A Trojan Horse mechanism for the spread of visna virus in monocytes"*. Virology, 1985. 147(1): p. 231-236.

[xix] S. R. White, J.O. Kephart and D.M. Chess,"*Computer viruses: A global perspective"*. Proceedings of the Fifth International Virus Bulletin Conference, Boston. 1995.

[xx] L. S. Liebovitch, and I.B. Schwartz, "*Information flow dynamics and timing patterns in the arrival of email viruses"*. Physical Review E, 2003. 68(1): p. 017101.

[xxi] I. Dacosta, S. Chakradeo, M. Ahmad and P. Traynor, "*One-time cookies: Preventing session hijacking attacks with stateless authentication tokens"*. ACM Transactions on Internet Technology (TOIT), 2012. 12(1): p. 1.

[xxii] A. Adams, and M.A. Sasse, "*Users are not the enemy"*. Communications of the ACM, 1999. 42(12): p. 40-46.

[xxiii] C. L. Lin, H.M. Sunand T. Hwang, "*Attacks and solutions on strong-password authentication"*. IEICE transactions on communications, 2001. 84(9): p. 2622-2627.

[xxiv] V. Sunkari, and C.G. Rao, "*Preventing input type validation vulnerabilities using network based intrusion detection systems"*. 2014. International Conference on Contemporary Computing and Informatics (IC3I), 2014 IEEE.

[xxv] S. Gupta, "*Buffer Overflow Attack"*. IOSR Journal of Computer Engineering, 2012. 1(1): p. 10-23.

[xxvi] K. N. AlHarbiand X. Lin, "*Preventing stack buffer overflow attacks"*. 2016, Google Patents.

[xxvii]A. Miele, "*Buffer overflow vulnerabilities in CUDA: a preliminary analysis"*. Journal of Computer Virology and Hacking Techniques, 2016. 12(2): p. 113-120.

[xxviii]G. Deepa, , P. S. Thilagam, A. Praseed and A. R. Pais, "*DetLogic: A black-box approach for detecting logic vulnerabilities in web applications"*. Journal of Network and Computer Applications, 2018.

[xxix] S. Som, S. Sinha, and R. Kataria, "*Study on sql injection attacks: Mode detection and prevention"*. International Journal of Engineering Applied Sciences and Technology, Indexed in Google Scholar, ISI etc., Impact Factor: 1.494, 2016. 1(8): p. 23-29.

[xxx] S. Mathew, S. Upadhyaya, D. Ha and H. Q. Ngo, "*Insider abuse comprehension through*

capability acquisition graphs. 2008. 11th International Conference on Information Fusion, 2008 IEEE.

[xxxi] R. A. Martin, "*Managing vulnerabilities in networked systems"*. Computer, 2001. 34(11): p. 32-38.

[xxxii]C. A. Blackwell, R. Lakshmanan, and M. Subramanian, "*Central computer backup system utilizing localized data bases"*. 1987, Google Patents.

[xxxiii]R. K. Chang, "*Defending against flooding-based distributed denial-of-service attacks: a tutorial"*. IEEE communications magazine, 2002. 40(10): p. 42-51.

[xxxiv]B. Yan, F. Binxing, L. Bin and W. Yao, "*Detection and defence of DNS spoofing attack"*. Jisuanji Gongcheng. Computer Engineering, 2006. 32(21): p. 130-132.

[xxxv]J. Owens and J. Matthews,"*A study of passwords and methods used in brute-force SSH attacks"*. USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). 2008.

[xxxvi]A. Narayananand V. Shmatikov, "*Fast dictionary attacks on passwords using time-space tradeoff"*. Proceedings of the 12th ACM conference on Computer and communications security. 2005. ACM.

[xxxvii]S. Granger, "*Social engineering fundamentals, part I: hacker tactics"*. Security Focus, December, 2001. 18.

[xxxviii]A. Muffett, "W*AN-hacking with AutoHack: Auditing Security Behind the Firewall"*. USENIX Security Symposium. 1995.

[xxxix]R. Barber, "*Hacking techniques: The tools that hackers use, and how they are evolving to become more sophisticated"*. Computer Fraud & Security, 2001. 2001(3): p. 9-12.

[xl] A. Herzberg, and A. Jbara, "*Security and identification indicators for browsers against spoofing and phishing attacks"*. ACM Transactions on Internet Technology (TOIT), 2008. 8(4): p. 16.

[xli] J. Mihelich, S. Phamand J. Li, "*Load balancing in a network with session information"*. 2016, Google Patents.

[xlii] A. Verma, P. Guha and S. Mishra, "*Comparative Study of Different Cryptographic Algorithms"*. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2016. 5(2): p. 58-63.

[xliii] J. Wang, T. Zhang, J. Song, N. Sebe and H. T. Shen, "*A survey on learning to hash"*.IEEE Transaction on Pattern Analysis and Machine Intellegence, 2017.

[xliv] N. Malkin,A. Mathur, M. Harbach and E. Egelman, "*Personalized security messaging: Nudges for compliance with browser warnings"*. 2nd European Workshop on Usable Security. Internet Society. 2017.

[xlv] R. W. Elliott, "*Protection against computer viruses"*. Journal of Accountancy, 1991. 171(5): p. 121.

[xlvi] M. Sandirigamaand A. Shimizu, "*Simple and secure password authentication protocol (SAS)"*. IEICE Transactions on Communications, 2000. 83(6): p. 1363-1365.

[xlvii] C. C. Mingand K. W. Chi, "*Stolen-verifier attack on two new strong-password authentication protocols"*. IEICE Transactions on communications, 2002. 85(11): p. 2519-2521.

[xlviii]W. Xu, S. Bhatkar and R. Sekar, "*Practical dynamic taint analysis for countering input validation attacks on web applications"*. 2005, Technical Report SECLAB-05-04, Department of Computer Science, Stony Brook University.

[xlix] Y. Parkand J. Park, "*Web application intrusion detection system for input validation attack"*. 2008. Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT'08. IEEE.

[l] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle and Q. Zhang, "*Stackguard: automatic adaptive detection and prevention of buffer-overflow attacks"*. USENIX Security. 1998

[li] G. Buehrer, B. W. Weide and P. A. S. Sivilotti,*"Using parse tree validation to prevent SQL injection attacks"*. Proceedings of the 5th international workshop on Software engineering and middleware, 2005. ACM.

[lii] Z. Suand G. Wassermann, "*The essence of command injection attacks in web applications"*.ACM SIGPLAN Notices. 2006. ACM.

[liii] Y. W. Huang, S. K. Huang, T. P. Lin and C. H. Tsai, "*Web application security assessment by fault injection and behavior monitoring"*. Proceedings of the 12th international conference on World Wide Web. 2003. ACM.

[liv] A. Shulman and C. C. Founder, "*Top ten database security threats"*. How to Mitigate the Most Significant Database Vulnerabilities, 2006.

[lv] N. Provos, M. Friedl and P. Honeyman, "*Preventing Privilege Escalation"*. USENIX Security. 2003

[lvi] T. F. Lunt, "*Automated audit trail analysis and intrusion detection: A survey"*. 1989: SRI International, Business Intelligence Program.

[lvii] P. G. Neumann, R. S. Boyer, R. J. Feiertag, K. N. Levitt and L. Robinson, "*A provably secure operating system: The system, its applications, and proofs*. Computer Science Laboratory Report CSL-116, 1980.

[lviii] N. R. Potlapally, S. Ravi, A. Raghunathan and

N. K. Jha, "*A study of the energy consumption characteristics of cryptographic algorithms and security protocols*. IEEE Transactions on mobile computing, 2006. 5(2): p. 128-143.

[lix] D. Eastlake and P. Jones, "*US secure hash algorithm 1"*.(SHA1), 2001.

[lx] K. M. Simand W.H. Sun, "*Ant colony optimization for routing and load-balancing: survey and new directions"*. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2003. 33(5): p. 560-572.

[lxi] B. H. Bloom, "*Space/time trade-offs in hash coding with allowable errors"*. Communications of the ACM, 1970. 13(7): p. 422-426.

[lxii] E. Y. K. Chan, H. W. Chan, K. M. Chan, V. P. S. Chan, S. T. Chanson, M. M. H. Cheung, C. F. Chong, K. P. Chow, A. K. T. Hui, L. C. K. Hui, L. C. K. Lam, W. C. Lau, K. K. H. Pun, A. Y. F. Tsang, W. W. Tsang, S. C. W. Tso, D. Y. Yeung and K. Y. Yu, "*IDR: an intrusion detection router for defending against distributed denial-of-service (DDoS) attacks"*.Proceedings of 7th International Symposium on Parallel Architectures, Algorithms and Networks, 2004. IEEE.

[lxiii] C. L. Schuba,I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni,"*Analysis of a denial of service attack on TCP"*. 1997. Symposium on Security and Privacy. 1997. IEEE.

[lxiv] L. Chappell, "*Inside the TCP handshake"*. NetWare Connection, 2000.

[lxv] X. Suo, Y. Zhu and G.S. Owen,"*Graphical passwords: A survey"*. 2005. 21st annual Computer security applications conference, 2005. IEEE.

[lxvi] L. H. Patil, U. Pateland M.P. Ramtekkar, "*Increasing Security in Click Based Graphical Password with Kerberos"*.IJARCT, 2015. 4(5): p. 1818-1824.

[lxvii] W. Diffieand M. Hellman, "*New directions in cryptography"*. IEEE transactions on Information Theory, 1976. 22(6): p. 644-654.

APPENDIX-A

TABLE I
CLIENT SIDE ATTACKS IDENTIFIED FROM THE EXISTING LITERATURE

	Problems	Possible solutions	References
Client side attacks	• Social Engineering	•Gaudiness	[xxxv]
	• Hack computer	•Firewalls	[xxxvi]
		•Update system regularly	[xxxvii]
		•Security audit	[xxxvii]
	• Viruses	•Antivirus	[xvii]
		•Buy trusted software	[xlv]
		•Don't download untrusted exe files	[xlv]
	• Session hijacking	•One-time cookie (OTC)	[xix]
		•HTTPS	[xix]
	• Weak authentication	•Secure passwords techniques	[xlvi]
		•SAS protocol	[xlvi]
		•OSPA protocol	[xlvii]

TABLE II
POSSIBLE SOLUTIONS FOR WEB APPLICATION

	Problems	Possible Solutions	References
Front end attacks	• Input validation attack	• Strict validation checks	[xlviii]
		• Input checks	[xlviii]
		• Strong authentication	[xlix]
		• Strong data typing	[xlix]
		• Proper error handling	[xlix]
	• Buffer overflow	• Use guard Canaries	[l]
Database security	• SQL injection	• Parsed tree	[li]
		• SQLCheck	[lii]
		• Defensing Coding	[liii]
	• Privileges abuse	• Query-level access control	[liv]
		• Secure authentication mechanism	[lv]
		• Security audit	[lvi]
		• Privacy policies	[lvi]
	• Platform vulnerability	• Update system regularly	[lvii]
	• Exposure of backups	• Secure cryptographic techniques	[lviii]
		• Hashing Algorithms	[lix]
Server Security	• DOS	• Load balancer	[lx]
		• Bloom filter mechanism	[ixi], [xxiii]
		• TCP handshake technique	[lxiii]
	• DNS poisoning	• TCP handshake	[lxiii] [lxiv]
		• SSL/TLS	[xxxviii]
	• Brute force attacks	• Graphics based passwords	[lxv], [lxvi]
		• Cryptographic algorithms	[lxvii]