Computer Software and Media Applications (2023) Volume 6 Issue 1
doi: 10.24294/csma.v6i1.3769

ORIGINAL RESEARCH ARTICLE

Software security: Threats, solutions and challenges

Himani Mittal

Goswami Ganesh Dutta Sanatan Dharma College, Chandigarh 160030, India; research.himani@gmail.com

ABSTRACT

Software security is of great concern as computers have entered almost all walks of life and people at large have become dependent on technology for not only entertainment and communication but for performing tasks involving money and a lot of stake. Software security not only involves securing the software but also user data and communication media. This paper states the several types of security threats that exist since the time networking has evolved, namely, malware, Trojans, viruses, denial of service attacks, and many more. This paper reviews several measures to address these threats. It includes logging, anti-malware, network security methods, and encryption methods. It has been identified that a lot of work has been done to deal with security threats, and it is not only limited to the protection of software but also extends to the protection of data and networks. The existing methods make extensive use of artificial intelligence, and it is identified that there is a need to develop a model that is able to identify known as well as unknown threats. There is a huge scope for research in this area.

Keywords: malware; social engineering; encryption; network security; malware detection

ARTICLE INFO

Received: 20 December 2023
Accepted: 2 January 2024
Available online: 21 February 2024

1. Introduction

Software security is of great concern as computers have entered almost all walks of life and people at large have become dependent on technology for not only entertainment and communication but for performing tasks involving money and a lot of stake. Software security includes an umbrella of security issues. The software includes the system software and application software. Application software is both stand-alone and network based software. Another type of software is Mobile App. Software security involves all the threats possible to any of these. The software is not free from design faults, and cybercriminals exploit these faults to gain illegal access to systems. Software security can be defined as securing the software, user data, and communication media.

In this paper, the variety of security threats, namely malware, denial of service attacks, phishing, spoofing, and many other types of attacks, are explained, and real life attacks are listed and categorized in Section 2. The existing solutions to mitigate the effects of these threats are included in Section 3. Section 4 includes the conclusions.

2. Review of security threats

There have been several security threats that have happened since the time networking came into existence. Many attacks that happened in the span of 2011–2020 have been discussed in Negrea's thesis[1]. Some of the attacks included Negrea's thesis[1] are discussed here. Operation Aurora (2009) was an attack on Google and Adobe to steal sensitive data from their users. The RSA Security Breach (2011) targeted at RSA encryption based software security solutions company. The attacker in this event got hold of the security keys of multiple customers. The source of this attack was emails from the attacker with attachments, which on-click obtained control of the victim's machine. Sony PSN Outage (2011) was an attack on the gaming application of Sony. The attacker exploited the vulnerabilities of the software and network to gain access to the sensitive data of the company. Another email breach was the Epsilon Email Breach (2011). LinkedIn security breach (2012), where the passwords of 6.5 million users were stolen. The thesis includes a discussion of 50 such reported incidents that exploited the vulnerabilities of software and networks. These are enumerated in **Table 1**.

Table 1. List of 35 attacks discussed in Negrea's thesis[1] and categorizing of the attacks.

Year	Name	Method of attack	Effect
2011	Operation Aurora	Malware	- Data theft
2012	RaGas Shamoon Malware attack		- Overwrites user files and loss of data leading to dysfunctional organization
2013	Saudi Aramco Shamoon Attack		- Infected the destination using phishing. Overwrites data and makes 35 k systems unusable.
2013	Target Data Breach		- Loss of 110 million credit card details
2013	Belgacom Attack		- Attack on Telecom Solutions providers network and used for national security breach
2013	South Korea Banking Cyber Attack		- Financial data of users breached and banking infrastructure like ATM rendered dysfunctional.
2014	Sony Pictures Hack		- attackers accessed unreleased films, employee data and sensitive emails.
2015	Black Energy Attack		- Ukraine's power distribution system was broken into using malware.
2015	TV5 Monde Attack		- Attack on famous TV network and disrupted network and blackout.
2011	RSA Security Breach	Email	- Encryption key theft
2011	Sonly PSN Attack	Software Vulnerability	- Data theft
2012	LinkedIn Security Breach		- Data theft
2013	Adobe Breach of 2013		- Attack on Adobe source code by breaking its encryption model.
2013	Snowden Revelations and NSA		- US National Security Agency is able to perform surveillance of many citizens without their knowledge by intercepting their telecom networks.
2014	Heartbleed Vulnerability of OpenSSL Library		- Threat to all users using OpenSSL for security and attacker got access of their systems.
2011	DigiNotar Certificate Fraud	Security Certificates Authority	- Third Party security Certificates Authorities got manipulated and all customers who accessed the web resources based on these digital security certificates got trapped.
2012	South Carolina Department of Rvenue Breach	Phishing	- Data of 6.4 million citizens was stolen.
2014	e-bay Data Breach	Compromising Passwords	- Loss of customer data and their financial information.
2014	JPMorgan Chase Breach		- Loss of financial data of the bank
2015	Anthem Health Insurance		- Loss of customer data of 78.8 million.
2014	OPM Security threat	Network Attack	- Loss of data of federal employees and general public in US Government.
2016	DNC Attack		- Access to US official documents and emails leading to its use in elections.
2016	SWIFT Banking Attacks		- Banks that depended on the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network for secure messaging and financial transactions were affected. The attackers used advanced techniques to compromise bank systems and fraudulently transferred funds.
2015	Ashley Madison Data Breach	Vulnerable Website	- Website for Extramarital affairs was breached by attacker and all its users were compromised.
2016	Yahoo Data Breach		- Stealing of Yahoo email users' data.

Table 1. (*Continued*).

Year	Name	Method of attack	Effect
2015	US IRS Breach	Authentication Breach	- Attacker exploited the vulnerabilities of Authentication process and got access to revenue data of US citizens.
2016	Bangladesh Bank Heist	Spoofing	- Stealing of money by imitation as another bank entity of international importance.
2016	Dyn DDOS Attack	Denial of Service Attack	- A DNS server was overloaded.
2017	WannaCry	Ransomeware	- Get hold of user data and make it inaccessible to the user. Then ask for money in return of data.
2017	Not Petya		- Similar to WannaCry and asked for money in bitcoin specially targeted Ukraine.

Some of the common methods of attack used by hackers as discussed in Humayun et al. and Kramer and Bradfield's studies[2,3] and as identified in **Table 1** are explained below:

1) Malware: It includes malicious software that gets installed on regular software and then infects all the system and user files[4]. Here the machine of the real user is controlled completely or partially by the hacker. They can access the sensitive data as well as harm the machine and interrupt with normal working of the machine. The variants where the control is not gained by the attacker are Trojan and Virus. Trojan is infected software that hides inside other executables and infects the user's machine. Virus is infected software that creates copies of itself. Both of these can generate spurious files, interfere normal working of other application programs and harm the hardware like disk crashing and damaging the RAM. Some of the common virus that can be found on Google Search by writing keywords "famous virus and trojans" are: Iloveyou, Mydoom, Melissa—email virus, Chernobyl Virus (1986)-damages the hardware; and many more. The other type of malware is the one that gains control of the user machine. They are categorized as Ransomeware, Spyware, Adware and Rootkits. Ransomeware is software that locks the user device until the ransom is paid by the user. Spyware steals user data and user loses the control of the machine. Adware is software that displays unwanted advertisement in your system. Rootkits gain control over a system by injecting malware.
2) Denial of Service (DOS) attack: It is a network server attack that generates spurious requests for server and it is unable to handle the load[5]. Some examples are Github attack in 2015, Mirai Botnet Attack in 2016, Github attack in 2018, AWS attack in 2020 and many more as reported in https://socradar.io/top-10-ddos-attacks/#:~:text=The%20Largest%20Reported%20HTTP%20DDoS,June%202022%20by%20over%2054%25.
3) Social media attack: Collection of user data from social media platforms and using this information to create a user profile and guess sensitive passwords. It also involves selling of such sensitive data. It includes attacks namely fake give away, impersonation and many more.
4) Session Highjacking: It is a method of hijacking a web user's session and redirects them to phishing websites[6].
5) Bots: These are automated scripts that perform spurious network activities like fake purchases, stealing data through fake accounts, etc[7–9]. A famous bot attack identified in 2016–Methbot. It stole the IP addresses of the US-based service providers. It went ahead to create 6000 domains and created content for these domains. Then they lured advertisers to publish adds on this content which they sent their own softbots to watch several times, thus fooling the advertisers (https://www.humansecurity.com/learn/blog/9-of-the-most-notable-botnets) .
6) Social engineering: It is contacting real users through social platforms and then manipulating them to release control of their systems, accounts and sensitive information[10].

7) Man-in-the-middle attack: This is an attack of eavesdropping or sniffing the network traffic and stealing user data. It involves threats like replay old messages[11].
8) Spoofing: It is making a real user believe he is talking to the original person but it is impersonating a person or institute[12].
9) Phishing: Redirecting user to malicious websites[13,14].
10) Password attacks: To exploit the vulnerabilities of software system to break into the system[15].
11) Information extortion: Stealing sensitive information and asking for money.
12) Bluetooth attacks: Making use of Bluetooth channels to gain control over device.
13) There are many other forms of attack but these are most important. The methods namely, encryption, removing system vulnerability, network security and vigilance are the main methods to deal with these threats. These methods are discussed in next section.

3. Software security solutions and challenges

The most effective way of controlling the security threats is vigilance among users. Apart from vigilance the following measures are helpful.

3.1. Malware detection

The malware threat is increasing and the modern day malware hides itself using obfuscation method. There is anti-malware software available in market. The malware is evolving at a faster speed than anti-malware. Anti-malware detection methods prior to 2005 were based on syntax of instructions generated by malware. In Christodorescu et al.'s study[16], the author made use of instruction semantics to detect malicious software. In an improved method the malware detection was based on data mining techniques namely, feature extraction and classification[17]. In the review of Sen et al.[18], author identifies use of Artificial Intelligence techniques namely, Genetic Programming, Machine Learning (SVM) and Naive Bayes in detection of malware. According to Aslan and Samet[19], there are multiple methods to detect malware namely, signature-based and heuristic-based. These methods are successful only to detect known malware. The unknown malware cannot be detected by these methods. Though there are many other methods based on Cloud, IoT, deep-learning and behaviour based detection methods but the performance of these methods is still not successful for all types of malwares as the malware is evolving at a fast rate. In the work of Gaurav et al.[20] a survey of several machine learning based malware detection methods in IoT setup are discussed. According to Gopinath and Sethuraman[21], Deep Learning based methods for malware detection is promising in detection of malware. Since malware is evolving at a fast rate, still the unknown malware detection remains a challenge.

3.2. Logging

This method records all the actions taken in the system in a log file so that forensics can investigate what all files are opened a what passwords are broken before the sensitive data was released.

3.3. Firewall

Firewall is an installation of extra filtering unit in middle of the real user and outside world to detect all types of attacks and malicious data flow. Mukkamala and Rajendran[22] survey several firewall technologies-Packet filtering, Circuit level gateways, Stateful inspection, Proxy firewalls, Next Generation firewalls and Cloud based firewalls. These are discussed below.

- Packet filtering firewall: This is a rule based firewall that does not allow any packet to flow through that fails a rule. But the drawback of this method is simplicity and ease to bypass. There can be conflicts in the rules which also lead to failure of this method.

- Circuit level gateways firewall: This is a TCP handshake based method but it is time consuming method.
- Stateful inspection firewall: An improvement over the previous two methods, it makes use of session tables to keep track of packet flow between interacting nodes.
- Proxy firewalls: This firewall scans the content of each packet for presence of malware.
- Next Generation firewalls: It also scans the content and uses machine learning based methods to flag the malware.
- Cloud based firewalls: It is similar to proxy firewall and enhances the scale of operation.

Apart from the firewall discussed in Mukkamala and Rajendran[22], there are distributed firewalls[23], next gen firewall[24] and petrinets based firewalls[25].

3.4. Access control and network security

Access control using authentication and authorization is a common method to safeguard the communication media. Depending on the variety of network— 2G, 3G, 4G, 5G, Wi-fi, Volte, Bluetooth and many other the level of network security[26] methods and access control techniques change with the underlying network technology.

3.5. Encryption

Encryption is a way of hiding data from the malicious users from snooping other data. For this the user data is converted in cipher text by using a secret key to encode the data.

- Traditional Encryption methods: There are several robust traditional encryption methods namely, AES, DES, Blowfish, RSA and many more. Some of these are Symmetric Encryption and Asymmetric Encryption methods. By Symmetric key it means that the encryption and decryption make use of the same key. While Asymmetric method means use of different keys for encryption and decryption.
- Image encryption: Useful for multimedia data that is exchanged between users[27,28]. discusses several methods for encryption of images.
- Light Weight Encryption: The devices used today like IoT devices, wearables and other small devices which have energy deficit and cannot run complex algorithms to perform encryption make use of light weight encryption methods namely, Present, Quark, Photon, Simon, Speck, Clefia and many more[29,30].

All the methods of software security discussed above are undergoing changes and evolving according to the ever evolving attacks to real users. The methods make use of Artificial intelligence methods and still models are being developed to identify the unknown and new types of attacks. The field is very dynamic because one method cannot find all the threats.

4. Conclusions and future work

Software security involves the protection of software, data, and communication media as a threat to anyone who puts others in danger. Common threats to a software system are discussed in Section 1, namely, malware, viruses, social engineering, bots, and many more. The common methods of dealing with these kinds of threats are malware detection, encryption, network security, logging, and firewalls. Malware detection methods aim to protect the software; encryption and logging protect the data; and firewall and network security protect the network. All three methods together protect the software system because arm to software, data, or the network all lead to disturbance of the real user operations. There is a growth in the use of methods based on machine learning, genetic algorithms, deep learning, IoT-based methods, and cloud-based methods.

The future work in the field of software security is to develop a model for the security of software, data, and communication media that is able to identify new or unknown attacks. Though the vigilance of the real user is a great asset, technology should also leap to help the real user. It has been identified that there is a need for more research in this area to unearth robust methods to deal with all known and unknown attacks.

Conflict of interest

The author declares no conflict of interest.

References

1. Negrea PC. *A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications* [Master's thesis] Babeș–Bolyai University; 2024.
2. Humayun M, Niazi M, Jhanjhi N, et al. Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering* 2020; 45(4): 3171–3189. doi: 10.1007/s13369-019-04319-2
3. Divya S. A survey on various security threats and classification of malware attacks, vulnerabilities and detection techniques. *International Journal of Computer Science & Applications (TIJCSA)* 2013; 2(04).
4. Kramer S, Bradfield JC. A general definition of malware. *Journal in Computer Virology* 2009; 6(2): 105–114. doi: 10.1007/s11416-009-0137-1
5. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review* 2004; 34(2): 39–53. doi: 10.1145/997150.997156
6. Jain V, Sahu DR, Tomar DS. Session hijacking: Threat analysis and countermeasures. In: Proceedings of 2015 International Conference on Futuristic Trends in Computational Analysis and Knowledge Management; 25–27 February 2015; Greater Noida, India.
7. Orabi M, Mouheb D, Al Aghbari Z, et al. Detection of bots in social media: A systematic review. *Information Processing & Management* 2020; 57(4): 102250. doi: 10.1016/j.ipm.2020.102250
8. Geer D. Malicious bots threaten network security. *Computer* 2005; 38(1): 18–20. doi: 10.1109/mc.2005.26
9. Ferrara E, Varol O, Davis C, et al. The rise of social bots. *Communications of the ACM* 2016; 59(7): 96–104. doi: 10.1145/2818717
10. Koyun A, Al Janabi E. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* 2017; 4(6): 7533–7538.
11. Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials* 2016; 18(3): 2027–2051. doi: 10.1109/comst.2016.2548426
12. van der Merwe JR, Zubizarreta X, Lukcin I, et al. Classification of spoofing attack types. In: Proceedings of 2018 European Navigation Conference (ENC); 14–17 May 2018; Gothenburg, Sweden. pp. 91–99. doi: 10.1109/euronav.2018.8433227
13. Hong J. The state of phishing attacks. *Communications of the ACM* 2012; 55(1): 74–81. doi: 10.1145/2063176.2063197
14. Bhavsar V, Kadlak A, Sharma S. Study on phishing attacks. *International Journal of Computer Applications* 2018; 182(33): 27–29. doi: 10.5120/ijca2018918286
15. Guan A, Chen CM. A novel verification scheme to resist online password guessing attacks. *IEEE Transactions on Dependable and Secure Computing* 2022; 19(6): 4285–4293. doi: 10.1109/tdsc.2022.3174576
16. Christodorescu M, Jha S, Seshia SA, et al. Semantics-aware malware detection. In: Proceedings of 2005 IEEE Symposium on Security and Privacy (S&P'05); 8–11 May 2005; Oakland, CA, USA. pp. 32–46. doi: 10.1109/sp.2005.20
17. Ye Y, Li T, Adjeroh D, et al. A survey on malware detection using data mining techniques. *ACM Computing Surveys* 2017; 50(3): 1–40. doi: 10.1145/3073559
18. Sen S, Aydogan E, Aysan AI. Coevolution of mobile malware and anti-malware. *IEEE Transactions on Information Forensics and Security* 2018; 13(10): 2563–2574. doi: 10.1109/tifs.2018.2824250
19. Aslan O, Samet R. A comprehensive review on malware detection approaches. *IEEE Access* 2020; 8: 6249–6271. doi: 10.1109/access.2019.2963724

20. Gaurav A, Gupta BB, Panigrahi PK. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems* 2022; 17(3). doi: 10.1080/17517575.2021.2023764
21. Gopinath M, Sethuraman SC. A comprehensive survey on deep learning based malware detection techniques. *Computer Science Review* 2023; 47: 100529. doi: 10.1016/j.cosrev.2022.100529
22. Mukkamala PP, Rajendran S. A survey on the different firewall technologies. *International Journal of Engineering Applied Sciences and Technology* 2020; 5(1): 363–365. doi: 10.33564/ijeast.2020.v05i01.059
23. Tudosi AD, Graur A, Balan DG, et al. Design and implementation of a distributed firewall management system for improved security. In: Proceedings of 2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet); 21–22 September 2023; Craiova, Romania. pp. 1–6. doi: 10.1109/roedunet60162.2023.10274920
24. Rajkumar B, Arunakranthi G. Evolution for a secured path using NexGen firewalls. In: Proceedings of 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON); 8–10 February 2023; Raigarh, Chhattisgarh, India. pp. 1–6. doi: 10.1109/otcon56053.2023.10113935
25. Madhloom JK, Noori ZH, Ebis SK, et al. An information security engineering framework for modeling packet filtering firewall using neutrosophic petri nets. *Computers* 2023; 12(10): 202. doi: 10.3390/computers12100202
26. Marin GA. Network security basics. *IEEE Security and Privacy Magazine* 2005; 3(6): 68–72. doi: 10.1109/msp.2005.153
27. Guan ZH, Huang F, Guan W. Chaos-based image encryption algorithm. *Physics Letters A* 2005; 346(1–3): 153–157. doi: 10.1016/j.physleta.2005.08.006
28. Alexan W, Elkandoz M, Mashaly M, et al. Color image encryption through chaos and KAA map. *IEEE Access* 2023; 11: 11541–11554. doi: 10.1109/access.2023.3242311
29. Buchanan WJ, Li S, Asif R. Lightweight cryptography methods. *Journal of Cyber Security Technology* 2017; 1(3–4): 187–201. doi: 10.1080/23742917.2017.1384917
30. Hasan H, Ali G, Elmedany W, et al. Lightweight encryption algorithms for Internet of Things: A Review on security and performance aspects. In: Proceedings of 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT); 20–21 November 2022; Sakheer, Bahrain. doi: 10.1109/3ict56508.2022.9990859