International Journal of Advanced Research in Engineering Technology & Science

ISSN: 2349-2819

Email: editor@ijarets.org Volume-8, Issue-6 June- 2021 www.ijarets.org

TO STUDY SYSTEM SECURITY-THREATS USING MULTI-AGENT SYSTEM PLANNING

Shri Gurinder Singh,

Research Scholar,

Dept. of Computer Science and Information Technology, Kalinga University

Dr. Yash Pal Singh,

Professor,

Dept. of Computer Science and Information Technology, Kalinga University

ABSTRACT

These days, software systems are at the heart of every aspect of technology around the globe. Nobody had ever foreseen that software would play such a crucial role in every aspect of modern life, whether it is in banking systems, communication networks, defence technology, or other experimental endeavours. This led to the software industry's recent exponential expansion, which has transformed the globe in inconceivable ways. Because computers were typically isolated functional islands with little to no connectivity in the past, software systems and networks offered no or very few security issues. According to the CERT Coordination Centre, Software Engineering Institute, Carnegie Mellon University, there has been a sharp increase in vulnerabilities and security breach incidents over the last few years as a result of the complexity of software systems, incredible level of interconnectivity, and infusion of new technologies. Furthermore, attackers today aren't just careless hackers; instead, they plan, organise, and target their attacks in order to obtain money, which adds further layers of complexity to security issues. A change to a more rigorous software development process that concentrates on the security component of software systems is required, keeping in mind the security requirements of the current threat environment and the elevated dangers for software users. Therefore, in order to maintain fundamental security attributes, a lot of security specialists have improved the current software development life cycle by combining numerous security strategies into each of its phases. In order to further this field of study and develop a threat-oriented security model as part of proactive risk management, we have been driven to incorporate a variety of proactive and cutting-edge security strategies. Furthermore, these new security measures have been created to best prevent threats in order to meet the demands of CEOs who want to minimize security risks while working with a limited budget in this shifting economic environment.

KEYWORD: Software Systems, Economic Environment, Security, Incredible

INTRODUCTION

Imagine a scenario in the year 2020 where a number of different zero-day malware programmes are spreading widely on the internet and affecting critical infrastructure, telephone networks have crashed, satellites have lost control, SCADA systems that control power grids are unresponsive, ATC management and railway traffic control systems have failed, security systems at oil refineries have become erratic, financial services have collapsed, and a tri-service exercise of the armed forces is taking place. The situation covered above has been demonstrated to be a fact. Technology development has an impact on how war and conflict are fought. Recently, the idea of "No Contact War" (NCW), in which there shall be no kinetic or physical activity across boundaries, has evolved. In order to attack the rival and accomplish political goals, the operations are carried out discreetly utilizing agents in the information domain. Because there are many interconnected and interdependent sectors in cyber security, multilayered activities and responses are encouraged. Cyber security is now essential to safeguard the use of essential IT resources for the good of mankind given the rapid growth of IT and the ease with which applications are being commercialized. The main engine of the Indian economy is information technology (IT). As a result of a paradigm shift in attack vectors and the way they are launched, it is necessary to examine our procedures, technology, governance structure, and assure compliance with the quickly evolving security and threat landscape. Regulations and legal obligations must also be followed.

Our cyber space is growing exponentially as a result of the rapid technological progress. This expansion also broadens the attack surface, making it more challenging to dynamically secure a specific area with the resources at hand. Each piece of hardware and software in an IT device carries some level of vulnerability. Security verticals have the responsibility of making sure that these risks-exposed vulnerabilities are fixed as soon as possible. However, the attackers take advantage of these flaws long before they are fixed. Investigations and attribution are very difficult because of the anonymity and virtual nature of cyberspace. There is an underground industry today that is booming and uses money like Bitcoin. Mafia, botnet owners, spammers, and phishers are the actors. A significant source of worry is the intricate relationship between various governments, darknet (underground elements), and people.

Cyber security is one of the ever-growing concerns with regard to several important fields like defence, banking, aerospace, insurance, and many other government & private machinery. Among these stakeholders, aerospace and defence have the highest market share. Sensitive information must increasingly be protected for the benefit of the public, corporate, and governmental sectors. The development of the Internet of Things (IoTs) has created multiple opportunities for cybercriminals to break into different end point devices, which has dramatically increased the number of cyber attacks. In addition, the proliferation of mobile devices at work in support of Bring Your Own Device (BYOD) trends and the thriving cloud-based services have both significantly expanded the attack surface. Today's Advanced Persistent Threats (APTs) provide a significant problem for all organizations, whether they are public or private; this calls for a thorough investigation and support for research and development in cyber security products and services. The demand for cyber security is also increasing due to factors like the need for unified cyber solutions; the risk associated with safeguarding sensitive data, the evolution of cloud computing, and better workplace mobility.

MOTIVATION

Virtually all computers in the internet era—servers, desktop PCs, and more lately, cell phones, pocket-sized gadgets, and various form factors like AutoPC and embedded systems—are linked together. Although it has contributed to the creation of numerous opportunities for developers and organizations, this extraordinary degree of interconnection has also increased risk for all software users by creating a significant threat environment. The problem of software security is still escalating despite the use of modern security technologies. Due to this, security measures that can prevent threats by minimizing vulnerabilities as much as possible throughout the design phase for safeguarding software systems have had to evolve. The methods for safeguarding software systems described above, however, have inherent limits and are therefore deemed insufficient to address the security concerns of the present. In order to secure applications, the penetration and patch method is frequently used. However, addressing bugs after a software product has been deployed can be 100 times more expensive than doing it during the development process. According to data from Barry Boehm's research, fixing a flaw early in the life cycle is less expensive than doing it later.

REVIEW OF LITERATURE

The April 2013 release of a Trend Micro white paper titled "Countering the Advanced Persistent Threat Challenge with Deep Discovery"20 reveals that targeted attacks are capable of getting past conventional security measures and the majority of IT professionals now think that their companies have been targeted. According to Mathew Schwartz's piece, "APTs employ a low-and-slow technique that is challenging to detect but has a high probability of success. Attackers must learn how to deceive a victim into running malware that uses a zero-day vulnerability to gain access to not only the victim's PC but potentially the entire corporate network. These threats are extremely clever and use a highly specialized and personalized strategy to access their targets, as was demonstrated by the review of successful APT attacks. To address the vulnerabilities that these threats exploit, next generation security measures are necessary. It is crucial that enterprises incorporate the defence strategy against APTs as part of the project scope as they prepare their IT security initiatives.

The "Emerging Cyber Threats Report 2014" from the Georgia Institute of Technology reveals that nation-state hackers compromise businesses, governmental organizations, and non-governmental organizations to build espionage networks and steal information. Cybercriminals continue to develop new ways to profit from victims. In addition to increasing cybercrimes and cases of espionage, the internet's wide use in personal life and numerous sectors, including business enterprises, government apparatus, and private manufacturing or service-based industries, has surprisingly also made it easier to quickly adopt new techniques. Data has been rapidly exported outside the firewall, the traditional security barrier, as a result of the use of mobile devices at work and the use of tablets and mobile phones from anywhere to access workplace cloud services. Companies and governmental organizations will study more data during the coming ten years in order to generate information that can be used to simplify operations, make better decisions, and spot abnormalities that might be signs of a threat. Attackers will need to develop strategies to evade statistical analysis and anomaly detection as the adoption of such big data analytics grows. The possibility exists that even the data utilized for big data analytics may be contaminated. Defenders must be able to spot extremely slow data changes and flag them as suspicious in order to fight against such attacks. With the development of technology, organizations have become more and more reliant on smart ICT (Information and Communication Technology) devices, work-from-home policies, the Internet of Things, and the bring-your-own-device culture, which has led to a significant increase in threats and the need for big data analytics.

RESEARCH METHODOLOGY

For the study, both primary and secondary data were employed. Primary information was gathered from selected respondents in the organizations. The secondary material was gathered from newspapers, numerous magazines, organization websites, and CERTs from different nations. The core data was gathered using the questionnaire survey approach. The secondary data was acquired through online desk research. The information produced is both quantitative and qualitative. The qualitative data are the non-numerical data made up of views and observations, whereas the quantitative data are primarily the numerical data gathered from records and questionnaire replies. Since they are complementary and do not compete with one another, both sorts of data have been employed in analysis. Non-probability restrictive sampling with a purposive version has been employed as the sampling framework. This method assisted in choosing informed and experienced respondents who could provide pertinent information. It has been confirmed that the sample technique chosen resulted in a reasonably minimal sampling error and aided in more effectively controlling the systematic bias.

RESUTLS AND DATA INTERPRETATION

AVOIDING THREATS USING MULTI-AGENTSYSTEM PLANNING

The most crucial quality of a security mechanism today to handle sophisticated threats in a changing security environment is "intelligence." To achieve the objective of threat avoidance for software security, MASPTA has evolved by integrating the ideas of Threat modeling process, Hierarchal Task Network approach (HTN), and Goal Oriented Action Planning (GOAP). To address the needs of the shifting economic landscape, a two level strategy called MASPTA-O: Multi-Agent System Planning to Avoid Threats Optimally has also been developed in this chapter. The Layered Threat Elimination model is used in the first level of MASPTA-O to identify the ideal number of threats that need to be mitigated, whereas the Mitigation Plan Generation algorithm and multi-attribute decision-making techniques are used in the second level to generate the most promising mitigation plan for each threat that has been identified. Then, to best avoid risks, agents are only introduced on the attack vectors in accordance with the chosen mitigation plan.

MULTI-AGENT SYSTEM PLANNING (MASP)

A method to a planning problem with complex goals known as "multi-agent system planning" divides the problem into smaller, more manageable parts and gives each agent control over one of these sub-problems. In this method, the solutions to the individual problems must be merged afterwards to produce a comprehensive, workable answer to the main issue. Multiple autonomous agents collaborate to solve a problem in a dynamic environment by coordinating their activities. Each agent builds their strategy in this planning process somewhat independently, but there is also a need to coordinate these plans.

GOAL ORIENTED ACTION PLANNING TECHNIQUE (GOAP)

Goal-oriented action planning is known as GOAP. It is a planning method that simply considers activities, such as a set of prerequisites and a set of outcomes. It provides dynamic issue solving that can recognize an agent's surroundings and respond logically. It is a method that generates a series of deeds (referred to as a plan) to achieve a desired objective state. Goals and actions are the main GOAP objects. Relevant world state attributes explain a goal. An action's consequences on the world state and its world state prerequisites are how it is described. A part known as a planner creates a plan of action (or plans of actions).

HIERARCHICAL TASK NETWORK PLANNING TECHNIQUE (HTN)

Hierarchical task network technology is known as HTN. A set of operators and a set of methods are the inputs for the HTN planner. There is a starting state and a goal that needs to be accomplished; the objective, which is referred to as a goal task, is not a collection of states. On a non-primitive job (also known as a compound task), which is an abstract task, this strategy is employed. Methods divide non-primitive jobs into a number of smaller tasks. A group of less abstract jobs known as these sub-tasks might be either non-primitive or primitive in nature. Actions are the concrete tasks referred to as primitive tasks. If a method is assigned to solve a specific non-primitive task and its precondition is true, the method can be applied to that non-primitive work. A method may contain a variety of restrictions that imply some sort of connection between the method's component tasks. One type of restriction is an ordering restriction, which dictates that one subtask must be completed before another subtask. An operator is used whenever a simple job is faced. An operator transitions a state in a predictable manner. For an operator to be employed, its precondition must also be true. When faced with a non-primitive problem, a method is utilized to break it down. Until a primitive task is encountered, this is repeated. At that point, an operator is used to update the current state so that the primitive task can be inserted as a task to complete in the plan list. The process continues in this way until all of the decomposition tree's jobs are primitive tasks, and each primitive task has had an operator applied to it. Total ordered, partial ordered, and GOAP planning strategies can all be used for HTN planning.

- The ordering of method subtasks is ostensibly fixed in HTN with total ordered decomposition. As a result, the problem's expressiveness is constrained.
- HTN with partial ordered decomposition is costly since no specific order of tasks is used, resulting in the generation of all possible combinations.
- HTN with GOAP produces an effective search space where only the legitimate paths that can assist in achieving the objective are generated, and the invalid paths are pruned from the search space.

MULTI-AGENT SYSTEM PLANNING FOR THREAT AVOIDANCE

As its name suggests, MASPTA is a system that operates in a multi-agent setting. The main focus of this strategy is on identifying and avoiding dangers to software systems posed by malicious users or hackers. By combining the ideas of the threat modelling method, HTN, and GOAP approach as described in earlier sections, MASPTA has come into existence.

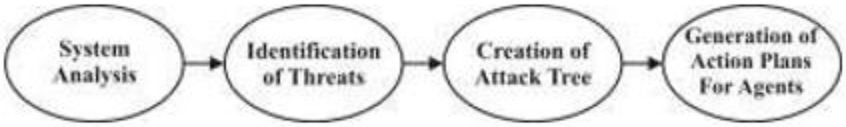
System Analysis
Identification of Threats
Creation of Attack Tree
Generation of Action Plans For Agents

FIGURE -1: GRAPHICAL REPRESENTATION OF MASPTA

Understanding and analyzing the system to be defended against threats is the initial stage. Using the threat modeling process described, possible risks to the system are detected in the second phase. In the third step, potential attacks for each threat are listed in order to build an attack tree using the HTN approach. An attack path is a path an attacker can take to get from a leaf condition to the root threat in this attack tree, where the root node represents the threat that needs to be mitigated. Action plans are created for each agent in the final step utilising the GOAP approach. In a multi-agent environment, these agents cooperate to carry out their planned action plans in order to avoid hazards. The following is a detailed explanation of each MASPTA phase.

MITIGATION OF THREATS OPTIMALLY USING MASP

With the aid of the methods listed below, each danger is then optimally mitigated in this level once the ideal number of threats has been established using LTEM.

1. Creation of a threat mitigation tree using the threat tree as a guide
2. Development of all feasible mitigation strategies utilizing the MPG Algorithm
3. Choosing the most effective mitigation strategy and incorporating agents into it to best counter the danger.

TABLE-1: DECISION MATRIX FOR ASSESSMENT OF REMEDIAL PLANS

Attributes Mitigation Plans	Mitigation_Cost	Mitigation_Time	Mitigation_ Feasibility	Security_ Policy_ Compliance

MP1	y11	y12	y13	y14
MP2	y21	y22	y23	y24
MP3	y31	y32	y33	y34
MP4	y41	y42	y43	y44
Weights	w_1	w_2	w_3	w_4

Decision Lowest mitigation cost, shortest threat mitigation time, highest level of technical viability, and degree to which selected plan complies with organization security policy are the criteria for choosing the optimal remedial plan. Therefore, a collection of qualities C is composed of these four factors.

Therefore, designers and developers can use any of the aforementioned techniques based on the system's complexity and security policy. In the event where more than one mitigation plan in Method-I requires the same minimum number of agents for threat avoidance, multi-attributes in the second method can be employed to choose the best mitigation plan. Then, agents are selectively introduced along the attack vectors in accordance with the most effective corrective plan determined above; as opposed to MASPTA where agents were placed at all leaf nodes to accomplish the same goal. Since this method uses a multi-attribute approach to evolve the most promising strategy, it offers a special optimal solution for threat avoidance to prevent the system from being compromised in the current economic environment. We can state that MASPTA-O offers the best option for avoiding threats, although it has its own drawbacks. This security technique provides the best defence in situations where the same attack is not a component of many threats; otherwise, it may lead to overlap in the countermeasures used to avoid threats. The need for multiple copies of the same security measure in that situation could lead to an overestimation of the cost. The process for identifying the best countermeasures, which is presented in the following chapter, has addressed this restriction.

CONCLUSION

Due to novel danger perceptions that were mostly unheard of in the early stages of the software development life cycle, software security has recently become a major concern. The complexity, extensibility, and incredible interconnection of today's software systems have expanded the scope of security concerns. Additionally, attackers today don't just launch random hacks; rather, they plan, organize, and focus their attacks in order to profit financially. Recent survey results show that in this evolving security environment, traditional security methods are no longer adequate to prevent such threats. Due to the proactive nature of threat management today, drastic corrective action may be necessary to protect against the many-sided threats we now face. As a result, as part of proactive risk management, we have presented a threat-oriented security model to complement existing security measures. To overcome the aforementioned challenges, this model uses a layered design that fuses a variety of current and cutting-edge methodologies. Every layer of this approach improves the security mechanisms already in place, making it extremely difficult, if not impossible, for an attacker to succeed.

If used wisely, the built-in proactive security procedures recommended as layer zero guidelines in this architecture can support defence mechanisms and help offer security cover even if the attacker breaches the system boundary. In addition, this layer offers a way to enter fail-to-secure mode as an additional layer of security in the event that the system is compromised. This work has used the threat modelling technique to identify known dangers. A statistical model and the introduction of research honey tokens have been added to this approach to help with the discovery of unforeseen dangers.

REFERENCES

1. AhnLab (2010, June). White paper on Online Banking: Threats and Countermeasures.
2. AhnLab Inc., Seoul, Korea. Retrieved from www.ahnlab.com.
3. Alexander, I. (2003). Misuse cases help to elicit non-functional requirements. Computing & Control Engineering Journal, IEEE, 14(1), 40-45.
4. Barfar A., & Mohammadi, S. (2007). Honeypots: Intrusion Deception. The Global Voice of Information Security, Information Systems Security Association (ISSA Journal), 28-31.
5. Bedi, P., Gandotra, V., Singhal, A., Vats, V., & Mishra, N. (2009). Avoiding Threats Using Multi Agent System Planning for Web Based Systems. In 1st International Conference on Computational Collective Intelligence – Semantic Web, Social Networks and Multiagent Systems (pp. 709-719). LNAI, Volume 5796/2009, doi: 10.1007/978-3-642-04441-0_62, Wroclaw, Poland: Springer-Verlag Berlin Heidelberg.
6. Bedi, P., Gandotra, V., Singhal, A., Narang, H., & Sharma, S. (2011). Optimal Countermeasures Identification Method: A New Approach in Secure Software Engineering. European Journal of Scientific Research, 55(4), 527-537, ISSN 1450- 216X.
7. Bedi, P., Gandotra, V., Singhal, A., Narang, H., & Sharma, S. (2012a). Threat-Oriented Security Framework in Proactive Risk Management using Multi-Agent System. Journal of Software: Practice and Experience, Wiley Publishers, doi: 10.1002/spe.2133 (In Press).

8. Bedi, P., Gandotra, V., & Singhal, A. (2012b). Innovative Strategies for Secure Software Development, Chapter in Designing, Engineering and Analyzing Reliable and Efficient Software, Pennsylvania, USA: IGI Global Press (In Press).
9. Beznosov, K., & Chess, B. (2008, January-February). Security for the Rest of Us: An Industry Perspective on the Secure-Software Challenge. IEEE Software, 25(1), 10-12.
10. Boehm, B.W. (1988). A Spiral Model of Software Development and Enhancement. ACM Computer Journal, 21(5), 39-45.
11. Brunil, D., Haddad, H.M., & Romero, M. (2009). Security Vulnerabilities and Mitigation Strategies for Application Development. In Proceedings of Sixth International Conference on Information Technology: New Generations (pp.235-240), Las Vegas: IEEE Computer Society.
12. Butler, S. (2002). Security Attribute Evaluation Method: A cost-Benefit Approach. In 24th International Conference on Software Engineering (pp.232-241). Orlando, Florida, USA:ACM.