Cyber Warefare Simulations with the MITRE ATT&CK Framework

Cameron Noakes | 001106490

I. Abstract

Cyber security plays an important role since the protection of systems governs the cyber future of any organisation. Each system should use industry standard security practises to minimise the attached risk to any digital asset.

This article overall concludes cretiques and summaries of various literature articles which were published so we can infer how the Mitre Attack Framework operates throughout the sector of cyber security. This framework serves as a blueprint for cyber professionals when it comes to possible attack vectors and techniques that could be conducted. Analysis of chosen performance metrics have also been assertained and compared.

Key words: *Red Teaming Techniques, Security Procedures & Practices, Cyber Warefare, Exploitation of Internal Infrastructure.*

II. Introduction

The Mitre Attack (Att&ck) Framework was started by the Mitre Corporation in 2013, it was officially realised in May of 2015. It is a mixture of tactics and techniques used by industry professionals to conduct cyber analysis and security audits of various digital assets and services (networks, web applications, mobile applications). Digital Guardian. (2018). What is the MITRE ATT&CK Framework? [online] Available at: https://digitalguardian.com/blog/what-mitre-attck-framework.

The Mitre Attack Framework is a commonly used industry standard for cyber security offensive and defensive referencing and implementation, it is commonly used in performing and engaging in security assessments, more commonly known as Penetration Tests. These security assessments can use the Mitre Attack Framework and can be exclusively used to identify vulnerabilities within an enterprise/corporate network and finalise into a professional commercial-grade report assessing the infrastructure or application in scope.

The Mitre Attack Framework is used throughout the cyber security industry for various other cyber professions such as threat hunting, system administrators, SOC analysts and defense security officers. It can be used as a good reference for what attacks could potentially be executed to allow cyber employees to secure systems to a higher level. Depending on the role of the cyber professional will depend on the way you perceive the Mitre Attack Framework.

The motivational reasoning behind choosing Mitre Attack Framework for this research is that of a professional advantage. I believe it is crucial to adopt a framework that clearly outlines explicit attack techniques for security researchers to conduct successful audits, since every solution is not impenetrable and requires thorough testing to conclude secure pathways.

Conclusively, I have adopted said framework in the past for various extracurricular security passions such as certifications and vulnerable labs so I am aware of how prevelant it is and its potential.

It is ideal to also assess performance of said framework to conclude my research with official metrics to outline and evidence my study. the security performance metrics I have chosen to analyse for Mitre Attack Framework are: **unambigious, general quality, end goal and informative.**

Where ***umambigious*** determines how straight forward the framework is to understand and how difficult it is to transfer the theory from the framework into implementation. ***General quality*** is referring to the overall structure of the framework and if it does a sufficient job at explaining each step to a high standard. The ***end goal*** is outlined by how each project that uses the framework as a reference was completed and to what standard it was completed to. ***Informative*** breaks the framework into how in-depth the framework is and how accurate the material is when referring to.

This paper will outline key fundamental and complex details as to why we need the Mitre Attack Framework, identifying analysis on said performance metrics, literature reviews and concluding with an overall summary and references.

III. Related work

1. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework

Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors, [online] 21(9), p.3267. Available at: https://www.mdpi.com/1424-8220/21/9/3267/htm

The concentration of this research paper is cyber warfare simulations for training offense and defense teams for real world cyber scenarios, in order to relate the Mitre Attack Framework to such a sector we first need to outline the cyber security culture of the Mitre Attack Framework. This includes but is not limited to: **knowledge**, **methodology**, **assumptions** with all respect to cyber security. This is the reasoning behind choosing this article, to create a strong argument before relating the framework to a specific niche.

Summarising this paper gives insight into where the Mitre Attack Framework can be used and how it serves to relate to a cyber culture, resulting in presented research from the similarity between security culture and adversary tactics and threats. It has also exhibited how it can assess the implementation of the Mitre Attack framework for corporate enterprises.

This research paper also elaborates highly on the history of the Mitre Attack framework, explaining how there are various bi-products of the framework for specific use cases such as ‘Attack for ICS’ being to better secure Industrial Control Systems, allowing a concise condensing of information for a historical introduction.

The paper spoke about subtechniques, the child tactics within each parent sector that most papers seem to overlook, which is informational and outlines key areas of more in-depth knowledge when performing offensive attacks.

Some limitations however, seem to arise with regards to the content of subtechniques, brief mention of them was adequate, however, no in-depth writing was conducted based on examples of such offensive subtechniques. There was acknowledgement and a brief initial overview, but failed to elaborate about specific offensive attack examples.

Another constraint is that the writer deliberately focused on Penetration Testing and Red Teaming, this is accurate and did mention how other areas use it but did not elaborate much beyond this. The writer could articulate more about other areas within cyber security the framework is used for and given some industry examples and information on such sectors.

2. Red Teaming: Regulatory and non-regulatory frameworks used in adversarial simulations

Saarainen, V. (2021). Red Teaming : Regulatory and non-regulatory frameworks used in adversarial simulations. [online] www.theseus.fi. Available at: https://www.theseus.fi/handle/10024/500627

Chapter: ATT&CK – MITRE

The above referenced research paper is heavily dependant on focusing its effort and research onto the Red Teaming side of cyber security, which was explicitly stated to ensure the reader understands its use case within this paper.

"While this paper only focuses on the Red Teaming aspects of the framework..."

With regards to the introduction, it was a strong and concise, to-the-point start about how it develops cyber adversary behavior. The introduction of the framework explained the Mitre Attack Framework without any unnecessary history behind the matter, allowing the reader to only focus on points that make a significant difference.

The research paper continues to then identify an increase in attack vectors due to the Mitre Attack Framework being adopted and expanded for various other Operating Systems and devices such as Linux, macOS, cloud services and mobile devices. It was outlined that the Mitre Attack Framework was orignally used for Windows offensive and defensive tactics.

Key examples were then discussed as to where the Mitre Attack Framework is used outside the realm of Red Teaming, the examples were across the cyber security spectrum, however, a gap in literature review research suggests that each example could have been discussed in more detail rather than just listing the examples. This was one of the limitations in regards to expanding more upon other sectors, even when focusing on Red Teaming.

Visualisation was included for the reader to understand a more reasonable approach of the techniques and tactics which aided in supplementing the research conducted. A few diagrams were included to help visualise the overall approach and to add a different option to understand rather than just reading the research.

This research article spoke about key features of the subtechniques within the Mitre Attack Framework which the previous research paper did not accomplish. The paper identified each subtechnique from the parent technique and decomposed the subtechnique into the corrosponding offensive attacks conducted under its scope. Below is a statement given regarding this.

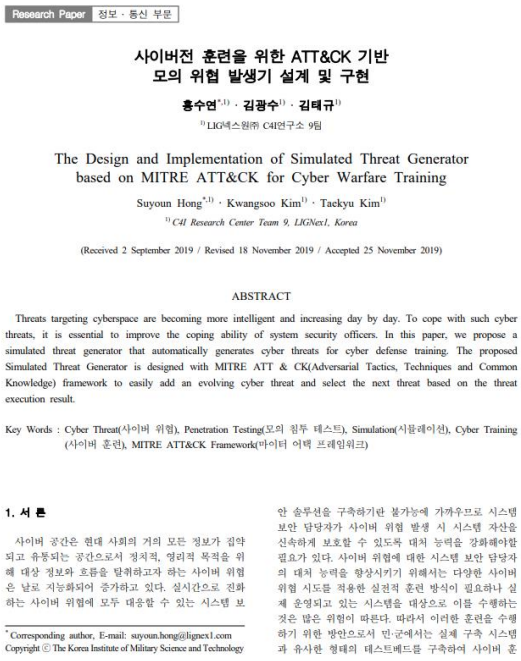
"Sub-techniques contain a detailed explanation of the chosen exploit."

Ville Saarainen included a comparision between frameworks in his paper to assess each, he compared the high level Red Teaming framework TIBER-EU to that of the Mitre Attack Framework. Conclusively, identifying that TIBER-EU focused more on policies and Red Teaming activities whereas the Mitre Attack Framework focuses on using real techniques based off of different tactics.

3. The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training

Hong, S., Kim, K. and Kim, T. (2019). The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training. Korea Institute of Military Science and Technology, [online] 22(6), pp.797–805. Available at: https://www.koreascience.or.kr/article/JAKO201910163249843.page

This Korean paper consisted of using an automation “generator” script to issue simulated threats to train system security officers with practical methods for defensive real world scenarios.



Research Paper 정보 · 통신 부문

사이버전 훈련을 위한 ATT&CK 기반
모의 위협 발생기 설계 및 구현

홍수연*[1] · 김광수[1] · 김태규[1]

[1] LIG넥스원㈜ C4I연구소 9팀

The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training

Suyoun Hong*[1] · Kwangsoo Kim[1] · Taekyu Kim[1]

[1] *C4I Research Center Team 9, LIGNex1, Korea*

(Received 2 September 2019 / Revised 18 November 2019 / Accepted 25 November 2019)

ABSTRACT

Threats targeting cyberspace are becoming more intelligent and increasing day by day. To cope with such cyber threats, it is essential to improve the coping ability of system security officers. In this paper, we propose a simulated threat generator that automatically generates cyber threats for cyber defense training. The proposed Simulated Threat Generator is designed with MITRE ATT & CK(Adversarial Tactics, Techniques and Common Knowledge) framework to easily add an evolving cyber threat and select the next threat based on the threat execution result.

Key Words : Cyber Threat(사이버 위협), Penetration Testing(모의 침투 테스트), Simulation(시뮬레이션), Cyber Training (사이버 훈련), MITRE ATT&CK Framework(마이터 어택 프레임워크)

1. 서 론

사이버 공간은 현대 사회의 거의 모든 정보가 집약되고 유통되는 공간으로서 정치적, 영리적 목적을 위해 대상 정보와 흐름을 탈취하고자 하는 사이버 위협은 날로 지능화되어 증가하고 있다. 실시간으로 진화하는 사이버 위협에 모두 대응할 수 있는 시스템 보안 솔루션을 구축하기란 불가능에 가까우므로 시스템 보안 담당자가 사이버 위협 발생 시 시스템 자산을 신속하게 보호할 수 있도록 대처 능력을 강화해야할 필요가 있다. 사이버 위협에 대한 시스템 보안 담당자의 대처 능력을 향상시키기 위해서는 다양한 사이버 위협 시도를 적용한 실전적 훈련 방식이 필요하나 실제 운영되고 있는 시스템을 대상으로 이를 수행하는 것은 많은 위험이 따른다. 따라서 이러한 훈련을 수행하기 위한 방안으로서 민·군에서는 실제 구축 시스템과 유사한 형태의 테스트베드를 구축하여 사이버 훈

* Corresponding author, E-mail: suyoun.hong@lignex1.com

A cyberspace was explained and what is referenced. A clear, concise explanation of how these simulations work is shown through a test bed simulation that requires the cyber professional to analyze the situation and take action on the threat to remove or isolate it. This method can be unique in training cyber professionals and to also help mitigate overall risk of an internal infrastructure network.

The cyber warfare threat simulation is explained to be for Blue Team (defense) but some applications for Red Teaming depending on refactoring the purpose since Blue Teaming is about stopping threats and the simulation performs Penetration Testing scenarios to aid in Blue Team training to prevent cyber warfare.

The paper continues to summarise what Penetration Testing is and its common responsibilities to outline more about how the simulation can be adapted for more commercial purposes. It speaks about how Penetration Tests actively evaluate infrastructure to secure environments and how the generator automation provides real world training for such security audits.

Brief overview mention of the Mitre Attack Framework was detailed as a result of the threat simulations being modelled after the framework to provide key, up-to-date real world scenarios of exploitation relating to the Mitre Attack Framework. The Mitre Attack Framework played a key part in the designing and development of the testbed cyber threat simulation.

The simulation uses machine learning for full automation to continue the life and generations of the most successful cyber threats in the simulation to actively prepare cyber professionals to the best of their ability. A list of common threats was made based on the Mitre Attack Framework techniques to apply them to the testbed simulation for cyber warfare.

One limitation is that of how no examples were mentioned in the introduction for where Mitre Attack Framework is also used within the industry and how it was a short paragraph that could have been expanded to include some information on Mitre Attack Framework and its association with this research not just for the testbed simulation.

4. Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training

Onghwa Kim, Kim, Y., Ahn, M.-K., Lee, H., First and Kim, D. (2020). Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training. Korea Society of Computer and Information, [online] 25(9), pp.71–80. Available at: https://www.koreascience.or.kr/article/JAKO202028662597165.pdf

This Korean research paper has a intelligible introduction in the Mitre Attack Framework section about the historical outline for the framework and brief mention of the pre-Att&ck model, providing a good section to diving into Mitre Framework.

The simulation was subsequently based on the Mitre Attack Framework to gather a list of potential simulated attacks and threats to perform. Such attacks and threats would download and execute malicious code and payloads to continue the spread of the attack while Blue Team defenders have to mitigate the risks, stop, prevent or isolate the malware/attack.

By taking into account all attacks from the Mitre Attack Framework, the authors were able to put together a complex, comprehensive threat model to base the simulation on. This was a detailed use of the Mitre Attack Framework and did well to serve its simulation design and implementation purpose.

A limitation with the paper is that it spoke about Mitre Attack Framework Blue Teaming and some Red Teaming (Penetration Testing) but did not elaborate to explain how the framework can be used in other sectors.

Another literature limitation is that it refused to delineate the pre-att&ck model which is a sub-model of the Mitre Attack Framework, brief mention was only stated and it may have complicated reader thoughts as not enough information was given.

Overall it spoke highly of the Mitre Attack Framework and apart from the opposing limitations, did well at providing research of outstanding attack and threat simulations.

IV. Analysis and Discussion

Performance Metrics: **unambigious, general quality, end goal and informative.**

Providing qualititative analytics based on the above mentioned performance metrics will help to aid an overall resolution of the framework and if the success factors outweigh any potential limitations. Such metrics will be described in relation to the papers reviewed and the knowledge obtain from each in regards to the Mitre Attack Framework.

The first performance metric **unambigious** is in terms of how explicit the framework is described in the papers and how precise the framework is for cyber security professionals. From the presented research papers above, which managed to identify key aspects of each section of the framework, have a clear understanding of the methodology and subtechniques and tactics with regards to specific, varied scenarios and cyber industry positions. As for the official Mitre Attack Framework, each section is organised accordingly to the methodology order of which a Penetration Test should be conducted, allowing a linear approach as well as detailed subtechniques of offensive attacks.

With regards to **general quality**, the methodology of the Mitre Attack Framework provides in-depth knowledge and perspective for each subtechnique, outlining clear attack vectors and tactics. The overall general quality possessed in each paper is high for that of the framework and defined with various informatonal pieces such as historical context of the framework.

Every **end goal** of a specific security audit is to have a robust, secure system for which information is kept regardless of the infrastructure service. That being said, analysis of the Mitre Attack Framework would assume such a successful end goal would be achieved. I do feel the framework is adequate, intelligent and radiant, full of information to refer to when necessary and contains explicit types of attacks for further referencing or implementation.

Information must be **informative** and the Mitre Attack Framework does a successful job at outlining explicit information relating to the industry and cyber security as a whole. Each research paper discussed also mentions the Mitre Attack Framework in-depth and to an extent of providing enough informaiton to conclude their summaries. The framework has subsections with various attack techniques which are corrolated into technical sections such as reconnaissance. A more informative methodology could have been a good addition to the framework in order to more clearly outline a set of ordered steps to perform successful audits.

Each performance metric, once composed together, forms an overall summary of such a solution in order to conclude a finalised perspective of the framework and gauge relevancy for future operations.

V. Conclusion

By all accounts for each individual research paper discussed and critiqued, there is no doubt that the Mitre Attack Framework is an excellent model for cyber professionals to based their work on and refer to when needed. The Mitre Attack Framework operates successsfully throughout each profession in cyber security regardless of the position required to carry out work, due to its nature, any cyber professional can adequately refer to the framework from a difference of perspective and can think from an offense or defense perspective.

If future work was to be conducted on the Mitre Attack Framework I would take into account more of the psychology mindset behind every attacker in order to prioritize certain CVEs to ensure that it covers what is needed for every step an attacker could proceed through.

References

1. Digital Guardian. (2018). What is the MITRE ATT&CK Framework? [online] Available at: https://digitalguardian.com/blog/what-mitre-attck-framework

2. Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors, [online] 21(9), p.3267. Available at: https://www.mdpi.com/1424-8220/21/9/3267/htm

3. Saarainen, V. (2021). Red Teaming : Regulatory and non-regulatory frameworks used in adversarial simulations. [online] www.theseus.fi. Available at: https://www.theseus.fi/handle/10024/500627

4. Hong, S., Kim, K. and Kim, T. (2019). The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training. Korea Institute of Military Science and Technology, [online] 22(6), pp.797–805. Available at: https://www.koreascience.or.kr/article/JAKO201910163249843.page

5. Onghwa Kim, Kim, Y., Ahn, M.-K., Lee, H., First and Kim, D. (2020). Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training. Korea Society of Computer and Information, [online] 25(9), pp.71–80. Available at: https://www.koreascience.or.kr/article/JAKO202028662597165.pdf