electronics

Article

Improving Attack Graph Visual Syntax Configurations

Askhat Sherzhanov [1], Hany F. Atlam [1,*], Muhammad Ajmal Azad [2] and Harjinder Singh Lallie [1]

[1] Cyber Security Centre, WMG, University of Warwick, Coventry CV4 7AL, UK; askhat.sherzhanov@gmail.com (A.S.); hl@warwick.ac.uk (H.S.L.)
[2] School of Computing, Birmingham City University, SteamHouse, Belmont Row, Birmingham B4 7RQ, UK; muhammadajmal.azad@bcu.ac.uk
* Correspondence: hany.atlam@warwick.ac.uk

Abstract: As technology advances and cyber threats become increasingly sophisticated, the task of recognising and understanding malicious activities becomes more complex. This persistent issue is widely acknowledged and extensively documented within the cybersecurity community. Attack modelling techniques (AMTs), such as attack graphs, have emerged as valuable tools in aiding cyberattack perception. These visualisation tools offer crucial insights into the complex relationships between various components within a system or network, shedding light on potential attack paths and vulnerabilities. This paper proposes an attack graph visual syntax method to improve cyberattack perception among experts and non-experts. The proposed approach was developed to streamline complexity and enhance clarity, thus augmenting the interpretability for users by enhancing visual structural components, such as hue, chromaticity, and line parameters. The proposed attack graph (*pag*) was empirically evaluated against the adapted attack graph (*aag*) presented in the literature. The empirical evaluation (n = 83) was conducted through a 3 × 2 × 2 factorial design and two-way analysis of variance (ANOVA) with repeated measures. The participants were classified according to their respective background cohorts into expert and non-expert (expert n = 37, non-expert n = 46) and then grouped into two groups: proposed attack graph (*pag*) and adapted attack graph (*aag*) (*pag* n = 41, *aag* n = 42). The empirical results demonstrated that while the proposed attack graph (*pag*) implemented various visual modifications such as brighter hues, denser line structures, and varied shapes, these enhancements did not significantly improve the perception of cyberattacks among individuals who lack expertise in the field, including corporate executives. Moreover, the use of variables such as colour, tone, and line width/density/structure did not help objects in the graph be distinguished more effectively. This paper provides significant insights into the impact of visual enhancements on cyberattack perception, highlighting that visual enhancements alone may not be sufficient to improve cyberattack perception for individuals lacking expertise in the field.

Keywords: attack graph; visual syntax; cyberattack; cybersecurity; attack modelling

check for updates

Citation: Sherzhanov, A.; Atlam, H.F.; Azad, M.A.; Lallie, H.S. Improving Attack Graph Visual Syntax Configurations. *Electronics* **2024**, *13*, 3052. https://doi.org/10.3390/electronics13153052

Academic Editors: Li Pan, Ning Liu and Conghui Zheng

Received: 21 June 2024
Revised: 26 July 2024
Accepted: 29 July 2024
Published: 1 August 2024

1. Introduction

There is an increasing need for refined and efficient techniques in the modelling of cyberattacks and the visualisation of event sequences. The simulation and visualisation of cyberattacks serve to enhance comprehension of the susceptibility of a network or host to cyberattacks, as well as to identify their weaknesses. Such simulations offer decision-makers and non-experts alike the opportunity to gain insight into the potential vulnerabilities and the methods to mitigate them [1]. However, there are currently a substantial number of non-standardised methods, leading to different interpretations of key aspects. This research attempts to improve user perception by reducing complexity and increasing the visibility of attack modelling techniques (AMTs).

Individuals involved in the administration and operation of computer networks may not possess a comprehensive understanding of the technical ramifications of cybersecurity, which is attributed to inadequate awareness and inadequate training [2]. This frailty is attributed to the fact that an incomplete comprehension of security measures can lead to inadvertent errors and disruptions in cybersecurity. Despite advancements in technology systems, susceptibility to cyberattacks will remain prevalent in the near future and depend heavily on individuals involved in decision-making processes. This has been highlighted by several researchers, including [2–5], who suggest that challenges with understanding cybersecurity reports are linked to the methods used for modelling and visualising, rather than the fallibility of individuals. Ref. [2] also found that an inadequate understanding of cybersecurity is often due to the intricacies of visualising the analysis and understanding complex patterns.

Current attack modelling techniques, such as attack trees and fault trees, have limitations that hinder their effectiveness. These techniques often lack standardisation, leading to inconsistent interpretations and applications. Different analysts may construct attack trees or fault trees differently, using varying levels of detail and terminology, making it difficult to compare and share findings across teams or organizations. This inconsistency can lead to misinterpretations and hinder collaborative efforts in threat assessment and mitigation.

Moreover, traditional visualisation methods can be overly complex, making it difficult for users to discern important details and relationships within the data. Attack trees, for instance, can become unwieldy and intricate, particularly when representing large-scale systems with numerous potential attack vectors. This complexity often results in cluttered diagrams where critical paths and nodes are obscured, thus failing to highlight the most pertinent vulnerabilities and attack sequences.

Visualisation methods like attack trees and fault trees also suffer from limited scalability. As systems grow in size and complexity, the models become increasingly difficult to manage and interpret. This scalability issue not only impacts the efficiency of threat analysis but also impairs the ability to communicate findings effectively to stakeholders, particularly to non-experts who may not be well-versed in technical details.

While there is a prevailing notion that the cybersecurity domain poses challenges for observers to comprehend [3], it is equally essential to facilitate the understanding of cybersecurity for decision-makers [6]. To ensure the security of a system, it is necessary to establish best practises that determine the minimum set of security measures. The ultimate goal is to develop technology that suits an individual’s physical and cognitive abilities and further customises the task to the person. Enhancing cybersecurity accessibility involves improving user-friendliness and fostering better perception and understanding.

Therefore, this paper proposes an attempt to refine the visual syntax of the attack graph to improve the perception of cyberattacks. The proposed approach was developed to streamline complexity and enhance clarity, thus augmenting the interpretability of the user by enhancing visual structural components, such as hue, chromaticity, and line parameters, like structure, density, and width, in the attack graph’s visual syntax. The *proposed attack graph* (“*pag*”) is based on the attack graph visualisations devised by [1] to effectively improve the perception of cyberattacks. The proposed attack graph was empirically evaluated against the *adapted attack graph* (“*aag*”) also presented in [1] to evaluate its effectiveness in various scenarios.

The selection of an attack graph technique was based on its efficacious functionality, extensive recognition in academic circles, and its utility for creating attack analysis models and then testing them. The primary objective of the testing is to gauge the efficacy of the attack graph method in shaping the comprehension of cyberattacks among both professionals and laypeople. It is incumbent upon both experts and non-experts to have a grasp of cybersecurity, the ability to peruse cybersecurity reports, and the readiness to tackle a serious cyberattack. This paper works with two attack graph methods: the *aag* method derived from [1] and the proposed *pag* method. The effectiveness of these methods was evaluated by assessing the respondents’ proficiency in accurately answering questions that required interpretation of the visual syntax from one of the two approaches. Consequently, perception was gauged using a test. The paper demonstrates the capabilities of AMTs to improve the perception of cyberattacks and proposes a modification to the attack graph visual syntax method proposed by [1] by augmenting visual structural components.

The proposed visual syntax is designed to cater to different user groups. While technical experts may work with detailed attack graphs to deal with cyberattacks daily, corporate executives are more interested in understanding the business impact and timeline for risk mitigation. Thus, the visual representation must be sophisticated enough to cover comprehensive details for technical experts and yet be intuitive for non-experts to understand the overall risk and mitigation strategies quickly.

The rest of this paper is organised as follows: Section 2 provides an overview of the topic to highlight AMTs and their applications, Section 3 outlines related work, Section 4 presents the proposed attack graph, Section 5 illustrates the experiment design and procedures followed by the participants, Section 6 presents results and analysis, Section 7 provides a discussion to highlight the research contribution, and Section 8 is the conclusion.

2. Background

This section provides the essential background of utilising attack graphs to improve the perception of security threats. It highlights the significance of situational awareness to provide valuable insights into the security posture of an information system and discusses various AMTs and their significance in the cybersecurity domain.

AMTs are used to simulate and analyse potential cyberattacks on information systems. These techniques help security professionals understand the vulnerabilities, attack vectors, and potential impacts of various threats. AMTs aid in the comprehension of cyberattacks for both experts and laypersons and can assist organisations in conserving time, finances, and other essential resources [1,7]. Various forms of AMTs are employed to simulate and analyse cyberattacks and to visualise the sequence and amalgamation of events. These include kill chains [8], the OWASP threat model [9], Diamond Model [10], Petri nets [11], misuse cases [12], fault trees [13], and attack graphs [14]. AMTs are primarily formulated to foster an understanding of vulnerabilities in a host or network and serve as a preventive measure [1], utilising visual rhetoric [15], visual syntax [14], or visual grammar [16]. The visual syntax configuration encompasses modelling systems such as fault trees and Petri nets, which are standardised models [17].

One common approach to graph attack modelling is the attack tree approach [18]. In attack trees, vertices and edges are assigned various parameters describing the number of resources used by the attacker, such as complexity, cost, and time. Attack tree-based models have the advantages of visibility, scalability, adaptability, and versatility. However, these models have certain shortcomings, such as lack of dynamic modelling capabilities and difficulties in modelling cyclic attacks.

Only a few studies have endeavoured to evaluate the efficacy of AMTs in assisting decision-makers in understanding an attack. Ref. [17] contrasted the attack graph with the fault tree to determine which of the two methods was more beneficial in promoting cyberattack comprehension. There are numerous types of attack models, but the most commonly used models are those based on graphs, particularly attack graphs [19]. Ref. [14] provided a comprehensive depiction of the visual representation of an attack through semantic techniques in both the attack tree and attack graph models. The visual syntax configuration is utilised to visualise the fundamental components of a cyberattack and utilises symbolic means of expression. However, attack graphs suffer from a distinct lack of standards, which can result in issues with common approaches and visual syntax methodology.

AMTs have several applications across different areas of cybersecurity, e.g, risk assessment, security architecture design, penetration testing, security awareness, and training and incident response. Several researchers have highlighted the significance of AMTs in explaining and visualising security threats. Ref. [20] found that providing a graphical means of documenting, explaining, and identifying security threats and risk scenarios is crucial in reducing the time and cost of security risk analysis. Developing a graphical approach aids in understanding the overall security risk and obtaining a quick understanding of the overall risk picture.

Several studies elucidate the predicament concerning the perceptions of cyberattacks amidst individuals lacking expertise in the field [3–5]. Ref. [3] addresses the consequences of chief executive officers (CEOs) not understanding cybersecurity due to its complexity. Their work specifically emphasises the keys for sufficiently training high-level executives on cybersecurity. The authors noted that more than 90% of CEOs are unprepared to handle a serious attack, as they cannot read cybersecurity reports. Ref. [21] assert that the visualisation of graphs necessitates a synergistic interweaving of modelling approaches.

3. Related Work

Attack graphs are a powerful tool for visualising security threats as they provide a clear and comprehensive representation of potential attack paths and vulnerabilities within a system. Several research studies were conducted to illustrate the effectiveness and significance of visual syntax in attack graphs. Ref. [22] demonstrated that the visual aesthetics of cybersecurity are crucial and identified significant elements for visual syntax design, such as shape, size, position, colour, meaning, texture, and orientation. Ref. [23] have also likened these elements to the periodic table in chemistry as they are fundamental to graphic design. The author indicated that the modelling language incorporates a syntax comprising elements and relations, along with a set of composition rules. Ref. [24] established a positive correlation between the intuitiveness and semantic transparency of variable labels. Furthermore, perceived intelligibility has a positive interaction effect and cognitive correspondence has a positive or negative interaction effect on semantic transparency. However, the authors did not specify the precise factors that this depends upon. Ref. [25] conducted a study on the cognitive efficiency of notation, which is indicated by its intelligibility, through a syntactic analysis based on the principles of notation physics. Objective measures, such as interpretative speed and accuracy, and a subjective measure of ease of use were used to measure the intelligibility of the dependent variable. Ref. [26] argued that denotations become intelligible when the independent variables are interpreted with perceptual intelligibility, semiotic clarity, complexity management, semantic transparency, visual expressiveness, cognitive integration, graphic economy, dual coding, and a cognitive approach.

Shapes are often used in visual representations of cyberattacks, such as attack graphs, to help distinguish different nodes or entities. However, as [14] mentioned, it is important to consider the visual distance between shapes to ensure clarity and avoid confusion. In addition to shape, other variables like colour, texture, and value can also be used to distinguish objects and improve visual distance. The research undertaken by [14] also acknowledged that merely altering the hue or texture of the edge does not yield a perceptible visual separation. Consequently, there must be a logical justification for employing a specific colour and utilising it in an effective manner. Imagery should not impose a substantial external burden in an endeavour to achieve cognitive efficiency; rather, it should be practical and straightforward to implement [27]. Ref. [28] queried whether aesthetic principles furnish prescriptive knowledge for designers and whether they facilitate the production of a model that is easy to comprehend and peruse. Ref. [29], therefore, concentrated on identifying evidence-based principles that would yield valuable diagrams, which enhance the accuracy, ease, and speed of information processing by humans.

While [30] discussed the challenges of visualising large attack graphs, they did not mention primitive graph clustering methods or advanced visualisation capabilities leading to performance problems. Instead, they proposed a method for automatically simplifying and abstracting complex attack graphs to make them more manageable for human analysis. They argued that this approach can improve users' understanding and interpretation of the graph by presenting a more high-level view of the attack scenario while still capturing important details. Ref. [31] highlighted the potential benefits of using virtual worlds as a tool to enhance cyber situational awareness through visualisation. By creating a more intuitive and immersive environment, the virtual world can help users better understand

and analyse large and complex datasets. This can lead to more effective decision making and responses to cyber threats. Ref. [32] also suggested that visualisation systems can help military personnel better understand the impact of cyber threats on their operations by using 3D models to simulate different scenarios. This approach allows them to identify the assets that are most vulnerable to cyberattacks and the resources that must be protected in order to carry out mission-critical tasks. By visualising these scenarios in a more immersive way, personnel can better understand the risks and take steps to mitigate them. The author highlights the potential of visualisation tools for improving cybersecurity in military contexts. Similarly, Ref. [33] highlighted the importance of visualisation in achieving situational awareness in cyberspace. They developed a comprehensive model for gathering data related to cyberattacks and used visualisation techniques to help individuals better understand the situation. According to their findings, visualisation plays a critical role in improving awareness and response to cyberattacks. Ref. [7] determined that forecasting potential threats or modelling cyberattacks is a pivotal issue in safeguarding any corporate network. However, while the authors' study enumerated and briefly analysed various types of attack modelling techniques, Ref. [1] focused on evaluating the efficacy of attack graphs in enhancing the understanding of cyberattacks. The attack graph approach is distinguished by its symbolic construction and data flow and proves to be more effective for understanding cyberattacks [1]. The author contends that the use of attack graphs as a mechanism for presenting information flow necessitates a standardised methodology. Additionally, they determined that to enhance cybersecurity practitioners' comprehension, the attack graph technique requires further research and an improved visual syntax. Ref. [17], which conducted a study to address vulnerabilities and recommend an attack graph visual syntax, concurred that there are numerous benefits to using attack graphs for preventing cyberattacks. The author performed an analysis that offers a comprehensive examination of the visual syntax used in attack modelling. Ref. [1] revealed that there is a growing demand across various professions for methods that enable a faster and more effective comprehension of cyberattacks. In a subsequent investigation, the author emphasised that attack graphs are useful for non-experts as a means of representing cyberattacks. Moreover, the author established that inadequate design can result in inefficiencies and make it difficult for observers to understand complex attack sequences, owing to the fact that the aforementioned models have not been tested for effectiveness. These findings are supported by [34], who affirm that visual appearance is a critical aspect of cybersecurity and recognise variables such as shape, size, position, colour, value, texture, and orientation as key elements of visual syntactic design, analogous to the periodic table's role in chemistry.

Recently, there has been a proliferation of cyberattack detection methodologies that are grounded in artificial intelligence (AI) [35]. The comprehensive research conducted by [35] on AI, alongside their innovative attack detection framework, posited that the attack graph model effectively portrays the intricate interplay between network vulnerabilities and information systems. However, they also engaged in a comparative analysis between the attack graph and the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) model. Ref. [35] asseverated that the MITRE ATT&CK model engenders a more nuanced and readily exchangeable knowledge model. Nevertheless, the findings derived from [36]'s empirical study, which sought to discern the superior facilitator of cyberattack perception between the attack graph and MITRE ATT&CK, unequivocally favoured the attack graph across all evaluated metrics. Their investigation enabled participants from diverse backgrounds to self-declare their preferred approach to enhance their comprehension of cyberattacks. Notably, the attack graph emerged as the favoured method, suggesting that it instilled a heightened self-assurance in participants, facilitated their grasp of cyberattacks with greater ease of navigation, and presented an enhanced visual syntax. Ref. [37] also proposed a novel automatic attack graph generation framework tool known as attack dynamics, similarly endorsing the notion that an aesthetically pleasing and minimalist design can effectively convey information through the utilisation of specialised node types and other visual elements. Their work further demonstrates that this type of system, owing to its human-readable outputs, caters to both novices and experts alike, thereby serving as a valuable educational resource.

In conclusion, after investigating the literature, it is clear that there is a need for further investigation and improvement in the visual syntax and effectiveness of attack graphs for understanding and representing cyberattacks. The literature highlighted the significance of visual aesthetics and identifies various elements for visual syntax design, such as shape, size, position, colour, texture, and orientation. However, there is a lack of specific factors determining the effectiveness of these elements. Also, the need for more empirical studies and frameworks to evaluate and improve the effectiveness of attack graphs in cyberattack perception as well as investigate the potential of AI-based attack detection methodologies were discussed.

4. Proposed Attack Graph

AMTs encompass a collection of methodologies that empower users to confront contemporary and forthcoming challenges in the realm of cybersecurity, augmenting their discernment and assessment. The degree of efficacy substantiates the indispensability of this approach with regard to apprehending cyberattacks. The literature review presented earlier identified the lack of comprehensive research and the need for further investigation into AMTs and visual syntax in the cybersecurity domain. Existing methodologies empower users to confront cybersecurity challenges, but limited scholarship exists in this domain. The main focus is on the efficacy of attack graphs in understanding cyberattacks, with a need for standardised methodology and improved visual syntax. In addition, further research is needed to enhance comprehension and address vulnerabilities as well as the complexity of enterprise network systems analysis, and the importance of preemptively understanding cyberattacks needs to be further investigated. AMTs are crucial in anticipating potential attacks and fostering awareness of network vulnerabilities. In addition, one of the other issues identified in the literature is the lack of visual syntax design, such as shape, size, position, colour, texture, and orientation in the developed attack graph.

Therefore, this paper provides an effective solution to address these issues by proposing an effective attack graph visual syntax method to improve cyberattack perception among experts and non-experts. The proposed approach aims to simplify intricacy and improve clarity, ultimately boosting user comprehension by enhancing visual elements in the attack graph's structure. This involves refining attributes such as hue, chromaticity, and line characteristics such as structure, density, and width, which collectively enhance the overall visual syntax of the attack graph. The proposed approach is dubbed the "proposed attack graph" (*pag*) throughout the paper. This paper will leverage the adapted attack graph method developed by [1] to refine the attack graph approach by simplifying its intricacies and augmenting its perceptibility and empirically evaluate the efficacy of the proposed attack graph against it. Throughout this paper, the term "adapted attack graph" (*aag*) will be employed to refer to this method.

This paper is an extension to the work presented in [1], where the author proposed a methodology that enables researchers to measure the effectiveness of visual information flow methods. The paper provided an empirical evaluation between an adapted attack graph method and the fault tree standard to determine which of the two methods is more effective in aiding cyberattack perception. The author utilised *aag* to denote attacks/exploits/edges and events representing a change in status. The technique utilises a rectangle to represent the precondition and an ellipse to represent the exploit, along with two distinct symbols to signify them. The *aag* approach utilises the presence (AND) or absence (OR) of an arc to denote precondition logic and primary and secondary notations. The *aag* method features a total of two symbols, and events flow in a top-down direction. Figure 1 provides an illustration of the *aag* example, showcasing an attack with a sole target—user (2)-level access (grey rectangle), with two pathways leading to the achievement of this goal. Ref. [1] indicates that the conjunctive precondition relationship necessitates the fulfillment of all related preconditions for an exploit to be successful.

Figure 1's attack graphs demonstrate how an attacker can acquire user (2)-level privileges. The graphs commence with four initial preconditions presented at the attack graphs' top: user (3) (presented twice), sshd (3,1), and sshd (3,2). The graph in Figure 1 depicts that the sshd_bof (3,1) exploit can be triggered only if two preconditions are met: sshd (3,1) and user (3). Ref. [1] further notes that disjunctive linking of preconditions necessitates the fulfillment of any one or more of the linked preconditions for the exploit to be successful. Likewise, the attacker can take advantage of the second event stream. Hence, either of the two exploits (sshd_bof (3,2) or sshd_bof (1,2)) must be utilised to gain the user (2) status on the target machine. Therefore, by relying on conjunctive preconditions, exploits can be thwarted by the absence of at least one of them.

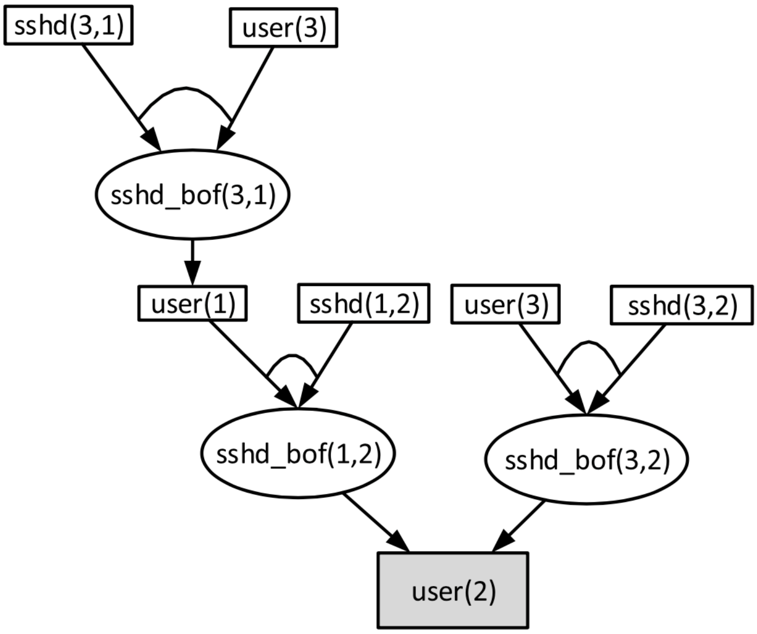


Figure 1. Cyberattack scenario 1, represented using the *aag* method [1].

The proposed approach *pag* is based on the attack graph visualisations in which shapes, such as circles, rectangles, and ellipses, are employed for portraying cyberattacks. The proposed approach *pag* employs rectangles and ellipses to designate preconditions/postconditions and exploits, respectively. The *pag* technique is depicted in Figures 2 (right) and 3 (right) compared with the adapted attack graph (*aag*) that was developed by [1]. Additionally, an octagon is used to signify the overall attack objective. The preconditions/postconditions and exploits are linked by conjunctive/disjunctive (AND/OR) relationships, representing the flow of events. In order to illustrate these connections, joint lines were employed to represent AND relationships, whereas separate lines were used to signify OR relationships. In the proposed *pag* graph, orange rectangles represent preconditions/postconditions. Exploits are shown as ellipses in a shade of reddish-purple, whereas the main objective of the attack is portrayed by a vermilion octagon, as seen in Figures 2 and 3. The differences between the proposed approach *pag* and *aag* can be seen in Table 1.

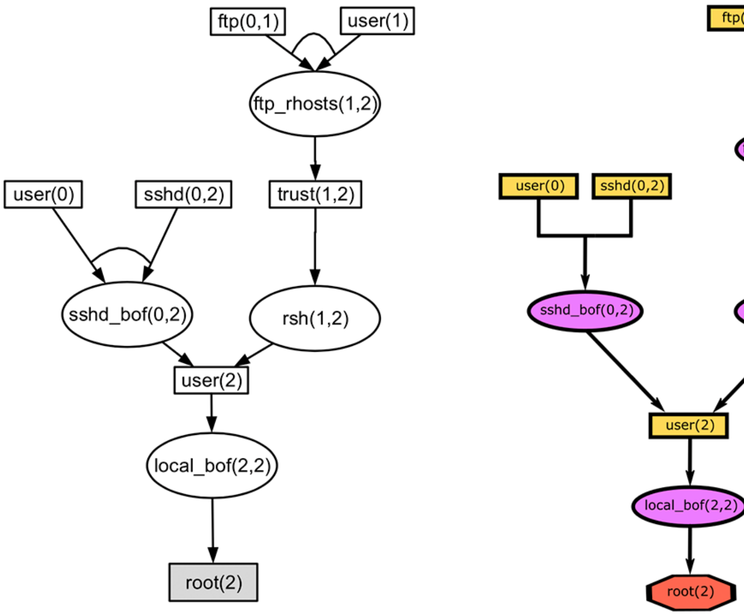


Figure 2. Cyberattack scenario 2, represented using the *aag* method (**left**) and the *pag* method (**right**).

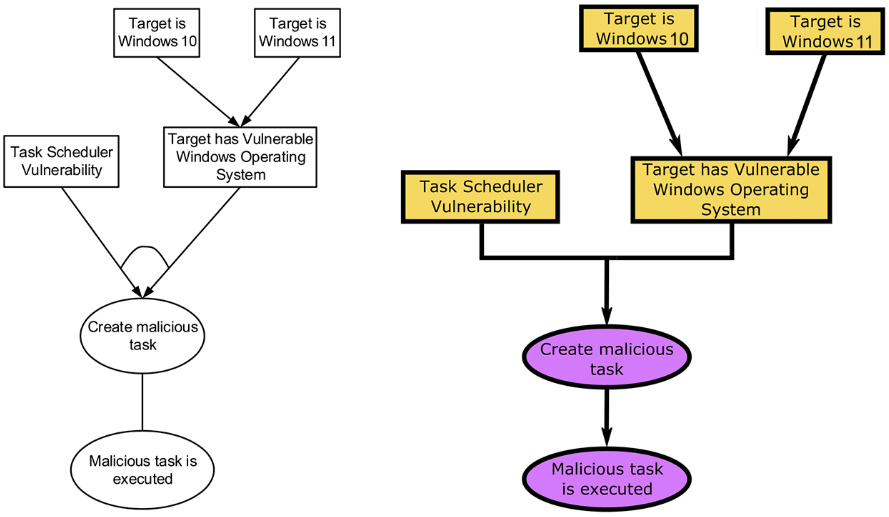
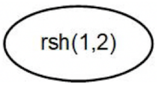
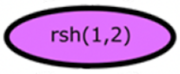
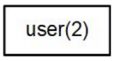
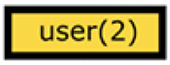
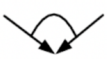
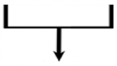
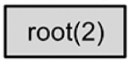
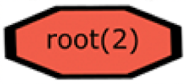

Target is Windows 10
Target is Windows 11
Task Scheduler Vulnerability
Target has Vulnerable Windows Operating System
Create malicious task
Malicious task is executed

Figure 3. A section of cyberattack scenario 3, represented using the *aag* method (**left**) and the *pag* method (**right**).

Table 1. The proposed attack graph method compared with the work presented in [1].

Construct	Adapted Attack Graph	Proposed Attack Graph
Exploit	 rsh(1,2)	 rsh(1,2)
Precondition	 user(2)	 user(2)
And		
Overall attack goal	 root(2)	 root(2)

5. Experiment Design

Subsequent to a thorough examination of literature sources, a theoretical framework was devised. Following the design of *pag*, data were collected from multiple cohorts of participants, consisting of both experts and non-experts for the purpose of evaluating the effectiveness of *pag* in comparison with *aag*. A total of 83 participants were recruited and classified according to their respective backgrounds, with 37 belonging to the expert group (*exp*) and 46 comprising the non-expert group (*non-exp*). These participants were then randomly allocated to the two AMT groups, with 42 in the *aag* group and 41 in the *pag* group. Each participant was randomly assigned to either the *pag* or *aag* category to circumvent any inherent bias between the groups, thus ensuring that both groups attained an equivalent level of comprehension on a theoretical level pertaining to cyberattacks. To establish the significance of the findings, a two-way ANOVA with repeated measures was employed to scrutinise the experimental data by assessing the significance of the disparities in mean values. It is highly unusual for a process to be determined by only one factor [38]. Rather, there is usually a concomitant impact of multiple factors. The two-way ANOVA method enables the assessment of the simultaneous effects of two factors, as well as the interaction between them [39].

The empirical evaluation utilised three distinct independent variables *(background, AMT, test)*, as well as a dependent variable *(grade point average—gpa)*. The objective of this research was to evaluate whether any of the three independent variables *(background, AMT, test)* have an impact on the perceptions of cyberattacks. It is worth noting that the *test* constituted an autonomous variable in each participant, designed to address the three questions they must answer. The assessment of comprehension and evaluation of cyberattacks employed a multi-stage test, which necessitated the presence of cognitive skills of increasing complexity. Table 2 provides a summary of its features. Each test conducted aligned with one of the three lower levels (application, comprehension, and knowledge) of Bloom's Taxonomy of educational objectives [40]. A range of academic disciplines have adopted Bloom's Taxonomy to evaluate both higher- and lower-order cognitive skills.

Table 2. Description of the study scenarios and tests (adapted from Lallie et al. [1]).

Test	Lower-Order Cognitive Skill	Test Description	Scenario Reference	Sample Question
1	Knowledge Recall	Multiple Choice: select one answer	Scenario 1 4 questions	"What are the necessary exploits for an attacker to be able to achieve user access on host 2?"
2	Comprehension	Select correct scenario from a heatmap	Scenario 2 4 questions	"Study the image below and select the exploit(s) which result in the attacker gaining user access status on host 2?"
3	Application	Multiple Choice: read scenario and select one from three heat maps	Scenario 3 4 questions	Study the figure below and select the figure that most accurately describes the following scenario: "The stuxnet virus is installed when a new services.exe file and a new s7otdbxdx.dll file are installed. Before these can be installed, the following preconditions must be met. The target has to have the Remote Procedure Call (RPC) vulnerability, the target has to be running the Step7 application, and the target has to be a Stimatic Public limited company (PLC)"

The test outcome was determined by a grade point average (gpa)—the dependent variable. The gpa for each participant was calculated based on their performance in the multi-stage tests. Each test comprised multiple questions that were scored individually. The steps for calculating the gpa were as follows:

1. Scoring system: Each question within a test was assigned a score based on the correctness of the response. Correct answers received full points (1 point), partially correct

answers received partial points (0.5 points), and incorrect answers received no points (0 points).

2. Test scores: The scores for each question within a test were summed to obtain a total score for that test. For instance, if a test comprised 4 questions, the maximum possible score for that test was 4 points.
3. Normalisation: The total score for each test was then normalised to a scale of 0 to 1 by dividing the total score by the maximum possible score. This normalisation ensures that all tests are weighted equally, regardless of the number of questions they contain.
4. Overall gpa calculation: The normalised scores from all tests were averaged to calculate the overall gpa for each participant. This average was obtained by summing the normalised scores for all tests and dividing by the number of tests.

For example, if a participant scored 3 out of 4 on test 1, 2 out of 4 on test 2, and 4 out of 4 on test 3, their normalised scores would be 0.75, 0.5, and 1, respectively. The overall gpa would then be calculated as:

$$\text{GPA} = \frac{0.75 + 0.5 + 1}{3} = 0.75$$

This gpa reflects the participant's overall performance across the different tests, providing a comprehensive measure of their comprehension and evaluation of cyberattacks.

The interrogatives were carefully crafted and formulated with the intention of adhering to the guidelines on how to utilise keywords and structure questions to align with the various levels of the taxonomy. The test framework is highlighted in Table 2. The independent variable *background* has been divided into two categories: *exp* and *non-exp*. The *exp* group consists of participants who possess either a computer science degree or have acquired five or more years of experience in the computer industry. The *non-exp* group encompasses all other participants.

The two *AMT* groups, denoted as *pag* and *aag*, each correspond to either a proposed attack graph or an adapted attack graph scenario, respectively. The two hypotheses that have been determined are as follows:

H1. The choice of *AMT* has an influence on the response to gpa.
H2. The choice of *background* has an influence on the response to gpa.

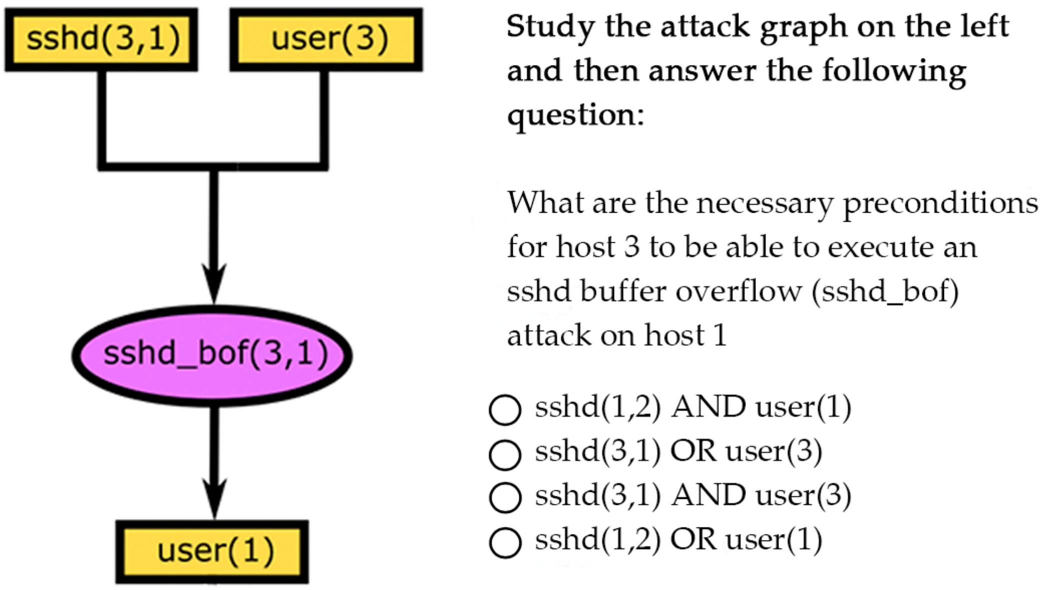
The participants were distinguished by two independent variables: *background* and *AMT*. The design can be presented as follows: *2 (background)* × *2 (AMT)* × *3 (test)*, which results in 12 unique conditions. To determine the significance of the results, a two-way ANOVA with repeated measures was employed. Identical assessments were administered, and each participant was presented with an identical sequence of queries. Moreover, these established the variables under control. In each individual trial, the relevant attack scenario was implemented, which was then adapted to both the *pag* and *aag* methodologies. Attack scenarios 1 (Figure 1), 2 (Figure 2), and 3 (Figure 3) were founded on the attack graphs formulated by [1,41,42], correspondingly.

5.1. Ethical Considerations

Ethical approval for the online survey was obtained. All participants were informed about the purpose of the study, and their consent was obtained before participation. The data collection process ensured the confidentiality and anonymity of the participants.

5.2. Data Collection

An online survey was employed to disseminate the online form to the targeted respondents. The research was segmented into three distinct phases: procuring the assent of the participants and other pertinent information; furnishing the participants with crucial background details germane to the AMT under investigation; and eliciting their opinions through a series of interrogations, as depicted in Figure 4.



Study the attack graph on the left and then answer the following question:

What are the necessary preconditions for host 3 to be able to execute an sshd buffer overflow (sshd_bof) attack on host 1

○ sshd(1,2) AND user(1)
○ sshd(3,1) OR user(3)
○ sshd(3,1) AND user(3)
○ sshd(1,2) OR user(1)

Figure 4. A sample from Qualtrics.

6. Results and Analysis

Due to the significant quantity of data gathered, the results have been partitioned into subsections. The grade point average (gpa_1, gpa_2, and gpa_3) attained for each evaluation are presented in Table 3.

Table 3. Grade point average—gpa.

Test			gpa_1			gpa_2			gpa_3	
		Mean	**SD**	**N**	**Mean**	**SD**	**N**	**Mean**	**SD**	**N**
exp	*aag*	0.5577	0.4102	13	0.1154	0.2193	13	0.6538	0.2982	13
	pag	0.4688	0.3709	24	0.1875	0.3062	24	0.5208	0.3529	24
	Total	0.5000	0.3819	37	0.1622	0.2777	37	0.5676	0.3367	37
non-exp	*aag*	0.3879	0.3509	29	0.1034	0.2546	29	0.3707	0.3034	29
	pag	0.5294	0.3172	17	0.0735	0.1470	17	0.6176	0.3437	17
	Total	0.4402	0.3423	46	0.0924	0.2196	46	0.4620	0.3373	46
Total	*aag*	0.4405	0.3737	42	0.1071	0.2416	42	0.4583	0.3263	42
	pag	0.4939	0.3468	41	0.1402	0.2565	41	0.5610	0.3481	41
	Total	0.4669	0.3595	83	0.1235	0.2481	83	0.5090	0.3391	83
	δ*aag*:*pag*	−0.0534			−0.0331			−0.1026		
	δ(*exp*:gpa)*aag*:*pag*	0.0889			−0.0721			0.1330		
	δ(*non-exp*:gpa)*aag*:*pag*	−0.1415			0.0299			−0.2470		

Table 3 highlights the mean deviation among all groups. The mean discrepancy is depicted by the delta (δ) symbol: δgpa(i)*aag*:*pag* = (gpa(i)*aag* − gpa(i)*pag*). It is worth mentioning that the average disparities for the three tests were in favour of the *pag* group (δgpa_1*aag*:*pag* = −0.0534, δgpa_2*aag*:*pag* = −0.0331, δgpa_3*aag*:*pag* = −0.1026). In terms of test 2, the average differences between experts favoured the *pag* group (δgpa_2(*exp*)*aag*:*pag* = −0.0721).

The average disparities between the groups of non-experts in tests 1 and 3 also endorsed the superiority of the *pag* group (δgpa_1(*non-exp*)*aag*:*pag* = −0.1415, δgpa_3(*non-exp*)*aag*:*pag* = −0.2470). However, the average disparities between experts in tests 1 and 3 favoured the *aag* group (δgpa_1(*exp*)*aag*:*pag* = 0.0889, δgpa_3(*exp*)*aag*:*pag* = 0.1330). Figure 5 portrays the relationship between the grade point average (gpa) and the *group*, as well as the gpa and *AMT*.

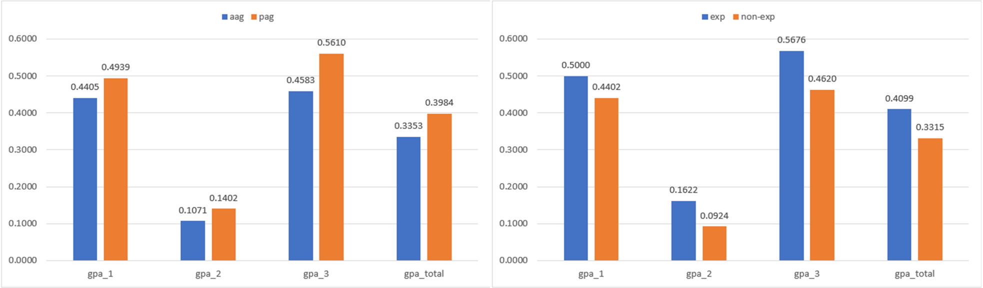


Figure 5. Total means of AMT vs test (**left**) and background vs test (**right**).

Table 4 presents a concise overview of the mean differences across all tests, yielding an overall δ(gpa)*aag*:*pag* value of −0.0630. These findings suggest that the *pag* and *aag* approaches offer distinct levels of support in detecting cyberattacks. Although the gpa and the average differences seem statistically insignificant (−0.0630), a more thorough examination is required to establish their significance.

Table 4. Average differences by background and ATM.

Delta	gpa_1		gpa_2		gpa_3		gpa_overall	
	Mean	n	Mean	n	Mean	n	Mean	n
δ*aag*:*pag*	−0.0534	83	−0.0331	83	−0.1026	83	−0.0630	83
δ(*exp*)*aag*:*pag*	0.0889	37	−0.0721	37	0.1330	37	0.0500	37
δ(*non-exp*)*aag*:*pag*	−0.1415	46	0.0299	46	−0.2470	46	−0.1195	46
δ(*aag*)*exp*:*non-exp*	0.1698	42	0.0119	42	0.2832	42	0.1549	42
δ(*pag*)*exp*:*non-exp*	−0.0607	41	0.1140	41	−0.0968	41	−0.0145	41

The mean discrepancies between experts with respect to the entire set of tests were in favour of the *aag* cohort (δgpa(*exp*)*aag*:*pag* = 0.0500), whereas the average differences between non-experts for the complete battery of tests were in favour of the *pag* group (δgpa(*non-exp*)*aag*:*pag* = −0.1195). The table underscores that skilled practitioners exhibit superior outcomes in the *aag* group, whereas novices demonstrate better outcomes in the *pag* cohort.

The mean differences among the *aag* cohort, pertaining to the entirety of the tests, favoured those with expertise (δgpa (*aag*)*exp*:*non-exp* = 0.1549); conversely, the mean differences among the *pag* cohort, also with regard to the full battery of tests, tend to favoured the non-experts (δgpa(*pag*)*exp*:*non-exp* = −0.0145). The table evidences that in the *aag* cohort, those with expertise exhibit superior performance when compared with their non-expert counterparts, whereas in the *pag* cohort, the reverse is true: non-experts tend to perform better than their expert counterparts.

6.1. Primary Effects

The primary effects of the *background* condition (*exp*/*non-exp*), *AMT* (*aag*/*pag*), and *test* were evaluated through a 2 (*background*) × 2 (*AMT*) × 3 (*test*) mixed-design factorial ANOVA for each of the 83 participants. The assumption of sphericity was not violated as per Mauchly's test of sphericity (Mauchly's test, χ2(2) = 0.565, p = 0.754), as shown in Table 5.

Table 5. Mauchly's test of sphericity.

Measure:							
Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon b		
					Greenhouse–Geisser	Huynh–Feldt	Lower Bound
M test	0.993	0.565	2	0.754	0.993	1.000	0.500

(1) *Primary effects of the test within the participants*:

The principal effect within participants for the test suggests that the participants' scores were only slightly different across the tests. The content of the three tests differs as the first two tests examine formal syntax, while the third one is a narrative representation. Therefore, it was hypothesised that non-experts would score higher on test 3 compared with tests 1 and 2. However, the findings indicate that there are no significant differences between the groups in their capacity to perceive attack descriptions in both formal syntactic and textual narrative formats. Table 6 unveils that all groups experienced a reduction in their gpa scores from the first to the second test, followed by an elevation from the second to the third test. Nonetheless, no significant disparities were found between the first and third tests, indicating that the perception of attack descriptions was not influenced by the form of presentation, whether it be formal syntactic or textual narrative in nature. The mean disparities among the tests reveal that all groups demonstrated lower scores in test 2. Table 6 presents paired comparisons between all three tests, which are further discussed in relation to the *AMT* and *background* groups.

Table 6. Paired comparisons between all three tests.

Group	(i) Test	(j) Test	Mean Difference (i-j)
all	1	2	0.3434
	2	3	−0.3855
	1	3	−0.0422
aag	1	2	0.3333
	2	3	−0.3512
	1	3	−0.0179
pag	1	2	0.3537
	2	3	−0.4207
	1	3	−0.0671
exp	1	2	0.3378
	2	3	−0.4054
	1	3	−0.0676
non-exp	1	2	0.3478
	2	3	−0.3696
	1	3	−0.0217

(2) *Primary effects of the AMT within the participants*:

Hypothesis 1 postulated that the choice of AMT has an impact on the response to gpa. However, upon investigation, the primary effects of the *AMT* within the participants did not support the hypothesis. The statistical analysis demonstrated that the choice of *AMT* was not significant (F (1,79) = 0.348, $p = 0.557$), indicating a negligible difference between the two AMTs. Table 3 and Figure 5 unveil minute differences in outcomes between the *pag*/*aag* groups that favour the *pag* group (δgpa_1*aag*:*pag* = −0.0534, δgpa_2*aag*:*pag* = −0.0331, δgpa_3*aag*:*pag* = −0.1026). The *aag* and *pag* groups demonstrated nearly identical outcomes for the total test: δgpa*aag*:*pag* = −0.0630. These findings are further examined in Section 6.2 with the goal of identifying any changes within the *pag* and *aag* groups.

(3) *Primary effects of the background on the participants*:

Hypothesis 2 posited that the *choice of background would impact the response to* gpa. However, like Hypothesis 1, it was not upheld, as primary effects of the *background* on the participants were found to be statistically insignificant (F (1.79) = 1.418, $p = 0.237$), indicating a negligible difference between the two backgrounds. Table 4 and Figure 5 accentuate the grade point average among the *exp*/*non-exp* groups. The Table portrays that *δexp*(gpa)*aag*:*pag* = 0.0500 and *δnon-exp*(gpa) *aag*:*pag* = −0.1195. The statistics underline a disparity that appears to benefit *pag* for the *non-exp* group and *aag* for the *exp* group. This will be explored further in Section 6.2 to ascertain whether any statistically significant differences exist in the *exp* and *non-exp* groups.

6.2. Results for Background, AMT, and Test Groups

To investigate potential disparities between the *AMT* and *background* groups, an in-depth analysis of the primary effects was conducted.

(1) *AMT*: The primary outcome of the test was analysed using two 2 (*background*) × 3 (*test*) ANOVAs for *pag* (n = 41) and *aag* (n = 42) in order to investigate further effects.

(a) *aag*: The impact of the *AMT* on the participants did not reveal a statistically significant outcome that favoured the *exp* group (F(1.40) = 3.430, *p* = 0.071). Thus, indicating that the choice of *background* for participants in the *aag* group does not hold statistical significance. Paired comparisons were performed on all tests within the *aag* cohort. Table 6 highlights that the *aag* cohort witnessed a decrease of 0.3434 in gpa from tests 1 to 2, while an increase of 0.3855 between tests 2 and 3 was discerned.

(b) *pag*: The impact of the *AMT* on the participants did not yield a statistically significant outcome in favour of *non-exp* (F(1.39) = 0.031, *p* = 0.862). Hence, it can be inferred that the selection of *background* for individuals in the *pag* cohort is not statistically significant. Paired comparisons were conducted among all tests within the *pag* cohort. As depicted in Table 6, the *pag* group displayed a reduction in gpa by 0.3537 during the transition from tests 1 to 2, followed by an elevation of 0.4207 during the period between tests 2 and 3.

(2) *Background*: The underlying influence with regard to the test was further evaluated by conducting two 2 (*AMT*) × 3 (*test*) ANOVAs for the *exp* and *non-exp* groups to explore additional effects.

(a) *exp*: The impact of the *background* on participants did not suggest any statistically significant outcome for *AMT* (F(1.35) = 0.267, *p* = 0.609). This indicates that the selection of *AMT* for participants in the *exp* group is not statistically significant. Paired comparisons were conducted among all three tests within the *exp* group, as shown in Table 6. The results demonstrated a decline in gpa of 0.3378 between tests 1 and 2, followed by an increase of 0.4051 between tests 2 and 3.

(b) *non-exp*: The impact of the *background* on the participants did not elicit a statistically significant outcome for *AMT* (F(1.44) = 2.779, *p* = 0.103). This suggests that the selection of *AMT* for the *non-exp* group participants is not statistically significant. Paired comparisons of all three tests (Table 6) suggested that the *non-exp* group demonstrated a reduction in gpa by 0.3478 between the first and second tests, followed by a growth of 0.3696 between the second and third tests.

7. Discussion

Investigating the literature has revealed that the fault tree and arc were the most prevalent ways of signifying precondition logic, as shown in Figure 6. However, conjunctive/disjunctive relationships are distinct from other types of relationships as they do not define the properties of contributions themselves but rather their logical relationships [43]. As a result, it is crucial that they are represented not as visual properties of links (such as sufficiency and sign) but as relationships between links so as not to add complexity to the level of perception. One way to achieve this is by using joined lines to denote AND relationships and individual lines for OR relationships. This method allows for the clearer identification of one or multiple conditions, highlighting all possible routes of attack and weak points within a specific network. This is essential in a range of scenarios, particularly in the analysis of network problems [14].

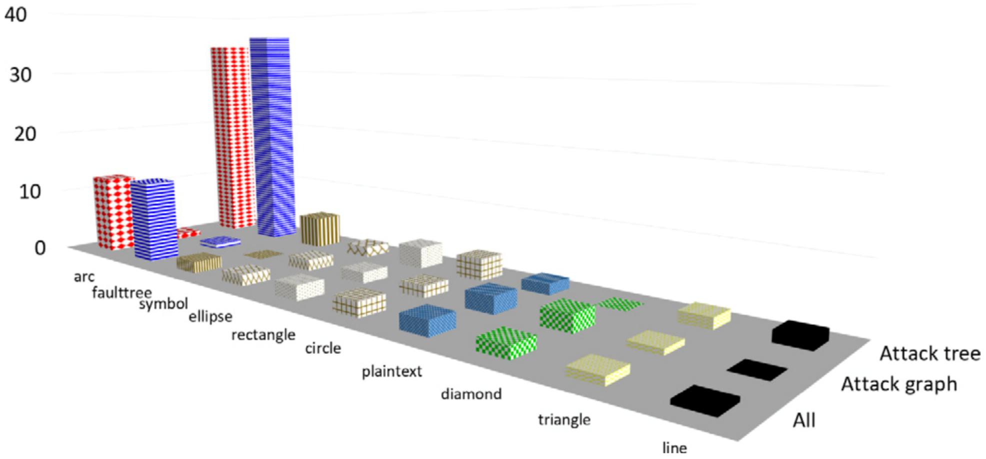


Figure 6. Shapes used to represent precondition logic [14].

In this paper, an effective attack graph was proposed to improve the perception of cyberattacks. The proposed approach *pag* is based on the attack graph visualisations in which shapes, such as circles, rectangles, and ellipses, are employed for portraying cyberattacks. The proposed approach *pag* employs rectangles and ellipses to designate preconditions/postconditions and exploits, respectively. There exists a potential for the diagrams to be reproduced in monochrome, as exemplified by Figure 7. The *pag* approach remains comprehensible, even when printed in greyscale. This study sought to determine the relative efficacy of two distinct AMTs in enhancing the perception of cyberattacks. Additionally, the investigation explored whether any discernible benefits to one approach over the other were observable under specific contextual conditions.

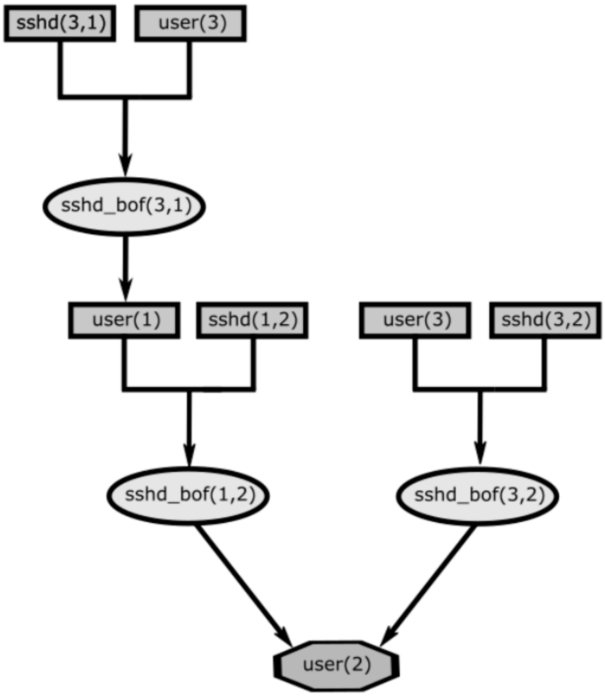
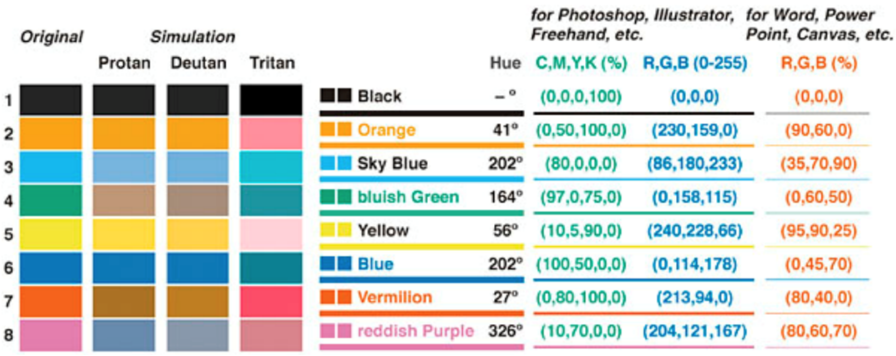


Figure 7. Cyberattack scenario 1 represented as the *pag* method in black and white print.

Although colour is widely acknowledged as an effective variable, it is imperative to consider a number of factors that may influence its effectiveness, such as colour blindness or colour vision deficiency, which affects approximately 1 in 12 men (8%) and 1 in 200 women globally. There are approximately 300 million individuals with colour blindness worldwide, which constitutes practically 4.5% of the total population, with the majority being men [44].

According to [45], the frequency of colour blindness is relatively high, with one in twenty-five African (4%), one in twenty Asian (5%), and one in twelve Caucasian (8%) males allegedly being "red-green" colour blind. The investigation carried out by [46] confirmed that colours can serve as a pivotal tool that brings harmony to various components, enhances the conveyance of information to the viewer, and furthermore has the potential to captivate and engage the viewer's attention. Additionally, Ref. [47]'s study utilised colour to provide greater distinction among identical constructs, as shown in Figure 8.



		Original	Simulation				for Photoshop, Illustrator, Freehand, etc.		for Word, Power Point, Canvas, etc.
			Protan	Deutan	Tritan	Hue	C,M,Y,K (%)	R,G,B (0-255)	R,G,B (%)
1	Black					– °	(0,0,0,100)	(0,0,0)	(0,0,0)
2	Orange					41°	(0,50,100,0)	(230,159,0)	(90,60,0)
3	Sky Blue					202°	(80,0,0,0)	(86,180,233)	(35,70,90)
4	bluish Green					164°	(97,0,75,0)	(0,158,115)	(0,60,50)
5	Yellow					56°	(10,5,90,0)	(240,228,66)	(95,90,25)
6	Blue					202°	(100,50,0,0)	(0,114,178)	(0,45,70)
7	Vermilion					27°	(0,80,100,0)	(213,94,0)	(80,40,0)
8	reddish Purple					326°	(10,70,0,0)	(204,121,167)	(80,60,70)

Figure 8. Colour blind barrier-free colour palette [45].

Hypothesis 1 scrutinised the impact of selecting *AMT* on the response to gpa. However, this hypothesis does not stand. Furthermore, it is noteworthy to mention that the primary effects of *AMT* on the participants indicated that the choice of *AMT* was not statistically significant (p = 0.557). This suggests that there existed only a marginal discrepancy between the two types of AMTs. Regarding Hypothesis 2, it was aimed at examining whether the selection of the background has an impact on the response to gpa. However, this hypothesis failed to hold. Moreover, the primary effects of the *background* on the participants were not statistically significant (p = 0.237), indicating a negligible difference between the two backgrounds.

A comparison of the gpa scores, as shown in Table 3, indicates a proclivity towards the *pag* method over the *aag* method among the non-expert group. Nevertheless, this result lacked statistical significance; therefore, caution is imperative when interpreting it. Given that all three tests assessed increasingly sophisticated cognitive levels instead of testing the exact same level every time, one might presume that a consistent performance across cognitive levels would be the minimum anticipated outcome. Nevertheless, discrepancies in performance (Table 6) were observed across tests. Specifically, participants exhibited a decline between tests 1 and 2, followed by an improvement between tests 2 and 3. These findings are subject to scientific limitations. Additionally, it was noted that modifications provided little enhancement to the overall understanding that people had. The outcomes demonstrate that substantially larger cohorts are imperative for achieving statistical significance. It is also plausible that the two graphs possess optimal visual syntax, thereby rendering further alterations to the graphs as inconsequential with respect to their perception.

As compared with recent studies from the literature, our findings expand upon recent advancements in cyberattack detection methodologies. While the research by [35] emphasized the attack graph model's effectiveness in illustrating the complex relationships between network vulnerabilities and information systems, our work not only corroborates these findings but also enhances the usability of the attack graph model through an improved visualization tool that caters to both experts and non-experts. This dual approach addresses the usability concerns highlighted by [35] and supports the argument that a well-designed visual syntax can significantly improve comprehension and navigation of cyber threats.

While [36] discussed attack graph visualizations, it lacks the depth of empirical evaluation and specific focus on visual syntax improvements that our work highlighted. The empirical evaluation and targeted visual syntax enhancements make it a more substantial and innovative cybersecurity visualization technique, particularly in addressing the needs of both experts and non-experts users. Furthermore, the empirical results gained from our work echo the conclusions of [36], who found that the attack graph model was favoured over the MITRE ATT&CK framework for its intuitive design and ease of use. Our work reinforces the superiority of the attack graph model in facilitating a deeper understanding of cyberattacks, as participants demonstrated increased confidence and ease in navigating the visual representations. In addition, our research diverges from [37]'s extensive review of cybersecurity visualization tools, which evaluates various techniques based on usability, cognitive load, and information conveyance. While [37] provided a broad overview, our study focuses specifically on attack graphs and their visual syntax, offering a more targeted improvement. By employing a sample size that includes a diverse range of 83 participants, our findings are robust and suggest that the improved visual syntax configurations can significantly enhance user understanding and operational effectiveness across different expertise levels. This contrasts with [35]'s narrower sample and approach, providing a broader validation of the proposed enhancements.

Limitations and Future Work

Given that effectiveness was assessed solely based on the ability to answer questions accurately in this study, it may be worthwhile to expand this assessment to encompass not only correctness but also the severity and timeliness of attacks. Although the time spent by participants in completing the tests was recorded, it was not analysed, as there was no time limit specified. Hence, it may be useful to consider the impact of time and severity of incorrect answers on the overall performance. Future research should aim to develop a methodology that takes into account all three variables of correctness, time, and severity for a more comprehensive evaluation of performance. Furthermore, more extensive investigations must be undertaken on the efficacy of the *aag* and the *pag* methodologies with larger-scale scenarios. The use of relatively small-scale attack scenarios in this study is not representative of complex cyberattacks, thus necessitating broader research.

An accessible online simulation would allow users to interact with the tool in real time, providing a deeper understanding of its capabilities and applications. Users receive instant feedback on their actions within the simulation. This immediate response helps them understand the impact of their decisions and actions on the configuration and functionality of the attack graph. Also, real-time interaction allows users to learn by doing. This hands-on approach helps users understand the capabilities and applications of the tool more effectively than passive learning methods. Implementing this simulation tool in real life involves several key steps to ensure its accessibility and effectiveness. First, the development of a user-friendly online platform is essential. This platform should be designed with intuitive navigation and clear instructions to guide users through the simulation process. It should also support a range of devices, including desktops, tablets, and smartphones, to maximize accessibility. Incorporating real-time feedback mechanisms is crucial as these will allow users to see the immediate effects of their actions within the simulation. Such feedback can be implemented through dynamic visualizations and instant notifications that reflect changes in the attack graph configuration and functionality. Furthermore, the platform should support interactive learning modules that enable users to engage in hands-on activities. These modules can include scenario-based exercises, where users can practice making decisions and see their outcomes in a controlled environment. To facilitate this, the simulation tool should have robust data processing capabilities to handle multiple users and provide personalized feedback based on individual user actions. In addition to the technical aspects, ensuring broad user engagement requires effective outreach and support. Providing comprehensive tutorials, user guides, and responsive customer support will help users understand and utilize the tool effectively. Hosting webinars, workshops, and interactive demos can also raise awareness and encourage adoption. Moreover, integrating analytics within the platform can provide valuable insights into user behaviour and engagement levels, helping developers continuously improve the tool based on user feedback. By focusing on these areas, the online simulation tool can become a powerful educational resource, enabling users to gain practical experience and a deeper understanding of its applications in cybersecurity. Hence, our future work will focus on developing such a simulation tool and online platform to facilitate broader user engagement.

8. Conclusions

The application of attack graphs in the domain of cybersecurity has gained widespread recognition. However, despite the provision of AMTs, users continue to face challenges in accurately understanding cyberattacks due to the absence of standardisation in the field. The comprehension of security and its associated risks has now become an indispensable requirement for both laypeople and experts. The proliferation of cyberattacks and the need for non-experts and experts to gain a deeper understanding of cyberattacks has necessitated the development of more effective techniques and methodologies to rapidly and accurately assess the means and strategies employed to launch cyberattacks, as well as the shortcomings in the systems that permit such threats to be successful. As a result, the level of perceptibility of cyberattacks has become an integral component in the utilisation and creation of attack graphs. This paper proposed an effective attack graph visual syntax method designed to enhance the understanding of cyberattacks for both experts and non-experts. The proposed approach focused on simplifying complexity and improving clarity by augmenting key visual elements like hue, chromaticity, and line parameters. The evaluation involved comparing the proposed attack graph (*pag*) with the adapted attack graph (*aag*). The empirical evaluation, which included 83 participants, utilised a 3 × 2 × 2 factorial design and two-way ANOVA test with repeated measures. The participants were divided into expert and non-expert groups, consisting of 37 experts and 46 non-experts. These groups were further divided into two subgroups, with 41 participants using the proposed attack graph (*pag*) and 42 participants using the adapted attack graph (*aag*). The empirical findings revealed that the proposed attack graph (*pag*) significantly improved the perception of cyberattacks, especially for non-experts and corporate executives. Variables such as colour, tone, and line width/density/structure played a crucial role in distinguishing objects within the graph, facilitating cyberattack perception among non-experts. However, despite implementing basic visual modifications like brighter hues, denser line structures, and varied shapes, the perception of cyberattacks did not show significant improvement.

Author Contributions: Conceptualization, A.S., H.F.A. and H.S.L.; Methodology, A.S. and H.F.A.; Validation, H.F.A. and M.A.A.; Formal analysis, A.S. and H.S.L.; Investigation, H.S.L.; Resources, M.A.A.; Writing—original draft, A.S.; Writing—review & editing, H.F.A., M.A.A. and H.S.L.; Supervision, H.F.A. and H.S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data can be shared up on request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lallie, H.S.; Debattista, K.; Bal, J. An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1110–1122. [CrossRef]
2. Conteh, N.Y.; Royer, M.D. The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *Int. J. Comput. (IJC)* **2016**, *20*, 1–12.
3. Morgan, S. *Why Ceos Are Failing Cybersecurity, and How to Help Them Get Passing Grades*; Forbes: Jersey City, NJ, USA, 2016.
4. Pfleeger, S.L.; Sasse, M.A.; Furnham, A. From weakest link to security hero: Transforming staff security behavior. *J. Homel. Secur. Emerg. Manag.* **2014**, 11, 489–510. [CrossRef]
5. Hughes-Lartey, K.; Li, M.; Botchey, F.E.; Qin, Z. Human factor, a critical weak point in the information security of an organization's internet of things. *Heliyon* **2021**, *7*, e06522. [CrossRef]
6. Coffey, J.W. Ameliorating sources of human error in cybersecurity: Technological and human-centered approaches. In Proceedings of the 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola, FL, USA, 21–24 March 2023; pp. 85–88.

7. Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-attack modeling analysis techniques: An overview. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 69–76.
8. Bryant, B.D.; Saiedian, H. A novel kill-chain framework for remote security log analysis with siem software. *Comput. Secur.* **2017**, *67*, 198–210. [CrossRef]
9. Wichers, D.; Williams, J. Owasp top-10 2017. *OWASP Found.* **2017**, *3*, 4.
10. Shin, Y.; Lim, C.; Park, M.; Cho, S.; Han, I.; Oh, H.; Lee, K. Alert correlation using diamond model for cyber threat intelligence. In Proceedings of the European Conference on Cyber Warfare and Security, Coimbra, Portugal, 4–5 July 2019; Academic Conferences International Limited: Oxfordshire, UK, 2019; pp. 444–450.
11. Wisniewski, R.; Grobelna, I.; Karatkevich, A. Determinism in cyber-physical systems specified by interpreted petri nets. *Sensors* **2020**, *20*, 5565. [CrossRef]
12. Geismann, J.; Gerking, C.; Bodden, E. Towards ensuring security by design in cyber-physical systems engineering processes. In Proceedings of the 2018 International Conference on Software and System Process, Gothenburg, Sweden, 26–27 May 2018; pp. 123–127.
13. Nagaraju, V.; Fiondella, L.; Wandji, T. A survey of fault and attack tree modeling and analysis for cyber risk management. in: In Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 25–26 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
14. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
15. Barroso, P.M. Visual literacy and visual rhetoric: Images of ideology between the seen and the unseen in advertising. In *New Media and Visual Communication in Social Networks*; IGI Global: Hershey, PA, USA, 2020; pp. 17–36.
16. Kress, G.R.; Van Leeuwen, T. *Reading Images: The Grammar of Visual Design*, 3rd ed.; Routledge: London, UK, 2020.
17. Lallie, H.S.; Debattista, K.; Bal, J. Evaluating practitioner cyber-security attack graph configuration preferences. *Comput. Secur.* **2018**, *79*, 117–131. [CrossRef]
18. Schneier, B. Attack trees. *Dr. Dobb's J.* **1999**, 24, 21–29.
19. Swiler, L.P.; Phillips, C.; Ellis, D.; Chakerian, S. Computer-attack Graph Generation Tool. In Proceedings of the DARPA Information Survivability Conference & Exposition II, 2001, Anaheim, CA, USA, 12–14 June 2001; Volume 2, pp. 307–321. [CrossRef]
20. Aboutorab, H.; Hussain, O.K.; Saberi, M.; Hussain, F.K.; Chang, E. A survey on the suitability of risk identification techniques in the current networked environment. *J. Netw. Comput. Appl.* **2021**, *178*, 102984. [CrossRef]
21. Calvi, A.; Viganò, L. An automated approach for testing the security of web applications against chained attacks. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; pp. 2095–2102.
22. Maloney, L.T.; Knoblauch, K. Measuring and modeling visual appearance. *Annu. Rev. Vis. Sci.* **2020**, *6*, 519–537. [CrossRef] [PubMed]
23. Granada, D.; Vara, J.M.; Brambilla, M.; Bollati, V.; Marcos, E. Analysing the cognitive effectiveness of the webml visual notation. *Softw. Syst. Model.* **2017**, *16*, 195–227. [CrossRef]
24. Polančič, G.; Brin, P.; Kuhar, S.; Jošt, G.; Huber, J. An empirical investigation of the cultural impacts on the business process concepts' representations. In Proceedings of the International Conference on Business Process Management, Vienna, Austria, 1–6 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 296–311.
25. Linden, D.v.d.; Hadar, I.; Zamansky, A. On the requirement from practice for meaningful variability in visual notation. In *Enterprise, Business-Process and Information Systems Modeling*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 189–203.
26. El-Attar, M. A comparative study of students and professionals in syntactical model comprehension experiments. *Softw. Syst. Model.* **2019**, *18*, 3283–3329. [CrossRef]
27. El-Attar, M. Evaluating and empirically improving the visual syntax of use case diagrams. *J. Syst. Softw.* **2019**, *156*, 136–163. [CrossRef]
28. El-Attar, M. Empirically evaluating the effect of the physics of notations on model construction. *IEEE Trans. Softw. Eng.* **2021**, *48*, 2455–2475. [CrossRef]
29. Moody, D. What makes a good diagram? improving the cognitive effectiveness of diagrams in is development. In *Advances in Information Systems Development*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 481–492.
30. Angelini, M.; Bonomi, S.; Lenti, S.; Santucci, G.; Taggi, S. Mad: A visual analytics solution for multi-step cyber attacks detection. *J. Comput. Lang.* **2019**, *52*, 10–24. [CrossRef]
31. Legg, P.A. Enhancing cyber situation awareness for non-expert users using visual analytics. In Proceedings of the 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), London, UK, 13–14 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–8.
32. Gutzwiller, R. *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment through 2015*; Technical Report; NIWC Pacific: San Diego, CA, USA, 2019.
33. Li, Y.; Huang, G.-q.; Wang, C.-z.; Li, Y.-c. Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 205. [CrossRef]

34. Jošt, G.; Heričko, M.; Polančič, G. Theoretical foundations and implementation of business process diagrams' complexity management technique based on highlights. *Softw. Syst. Model.* **2019**, 18, 1079–1095. [CrossRef]
35. Jia, Y.; Gu, Z.; Du, L.; Long, Y.; Wang, Y.; Li, J.; Zhang, Y. Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the mdata model. *Knowl.-Based Syst.* **2023**, *276*, 110781. [CrossRef]
36. Pirca, A.M.; Lallie, H.S. An empirical evaluation of the effectiveness of attack graphs and mitre att&ck matrices in aiding cyber attack perception amongst decision-makers. *Comput. Secur.* **2023**, *130*, 103254.
37. Hankin, C.; Malacaria, P. Attack dynamics: An automatic attack graph generation framework based on system topology, capec, cwe, and cve databases. *Comput. Secur.* **2022**, *123*, 102938.
38. Bartasun, P.; Prandi, N.; Storch, M.; Aknin, Y.; Bennett, M.; Palma, A.; Baldwin, G.; Sakuragi, Y.; Jones, P.R.; Rowland, J. The effect of modulating the quantity of enzymes in a model ethanol pathway on metabolic flux in synechocystis sp. pcc 6803. *PeerJ* **2019**, *7*, e7529. [CrossRef] [PubMed]
39. Campbell, M.A. Underemployment and Job Satisfaction: A Comparison among Age Groups. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2018.
40. Bloom, B.S. *Handbook on Formative and Summative Evaluation of Student Learning*; McGraw-Hill Book Company: New York, NY, USA, 1971.
41. Barik, M.S.; Mazumdar, C. A graph data model for attack graph generation and analysis. In Proceedings of the International Conference on Security in Computer Networks and Distributed Systems, Trivandrum, India, 9–10 January 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 239–250.
42. Ghosh, N.; Ghosh, S.K. A planner-based approach to generate and analyze minimal attack graph. *Appl. Intell.* **2012**, *36*, 369–390. [CrossRef]
43. Lucassen, G.; Robeer, M.; Dalpiaz, F.; Van Der Werf, J.M.E.; Brinkkemper, S. Extracting conceptual models from user stories with visual narrator. *Requir. Eng.* **2017**, *22*, 339–358. [CrossRef]
44. Ohkubo, T.; Kobayashi, K. A color compensation vision system for color-blind people. In Proceedings of the 2008 SICE Annual Conference, Chofu, Japan, 20–22 August 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 1286–1289.
45. Okabe, M.; Ito, K. How to Make Figures and Presentations that Are Friendly to Color Blind People. 2002. Available online: https://jfly.uni-koeln.de/html/color_blind/ (accessed on 1 January 2024).
46. Zedda, M.; Piras, C.; Pinna, F. Road signs: Walking among shapes and colors. *Int. J. Res. Eng. Technol.* **2013**, *2*, 568–573.
47. Man, D.; Zhang, B.; Yang, W.; Jin, W.; Yang, Y. A method for global attack graph generation. In Proceedings of the 2008 IEEE International Conference on Networking, Sensing and Control, Sanya, China, 6–8 April 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 236–241.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.