Journal of Computer Science Review and Engineering | ***ISSN 1694-4488***
Published by AIR JOURNALS | *https://airjournal.org/jcsre*
16/18 Avenue des Longaniers, Quatre Bornes, Mauritius
airjournals@gmail.com; enquiry@airjournal.org

RESEARCH ARTICLE

Integrating Research Testbeds, Attack Mechanisms, and Defence Strategies into a Holistic Framework for Cybersecurity

Adeyemi Samuel Akintola
Western Governors University, Salt Lake City, UT

Citations - APA

Akintola, A. S. (2024). Integrating Research Testbeds, Attack Mechanisms, and Defence Strategies into a Holistic Framework for Cybersecurity. *Journal of Computer Science Review and Engineering, 8(2) 1-12. DOI: https://doi.org/10.5281/zenodo.14543273*

ABSTRACT

Integrating research testbeds, attack mechanisms, and defence strategies into a unified cybersecurity framework offers a pathway to addressing the growing complexity of cyber threats. This study explores the multifaceted roles of research testbeds in simulating and emulating real-world environments, enabling the assessment of vulnerabilities and testing defence mechanisms. It also examines the evolution of attack vectors, such as Advanced Persistent Threats (APTs), and the importance of adapting preventive, detective, and corrective measures in response to these threats. The research advocates for a spiral model of collaborative knowledge improvement, fostering iterative development and cross-sectoral collaboration by emphasizing the interdependencies between testbeds, attacks, and defences. This holistic approach underscores the necessity of aligning academic research, industry practices, and operational needs to create resilient cybersecurity solutions. The findings provide actionable insights for policymakers, researchers, and industry stakeholders aiming to enhance the security of critical infrastructure and digital ecosystems.

Keywords: *Cybersecurity Framework; Research Testbeds; Attack Mechanisms; Defence Strategies; Advanced Persistent Threats (APTs); Collaborative Knowledge Integration*

Introduction

Cybersecurity is a multifaceted problem that cannot be solved in isolation. As such, research testbeds have become crucial tools in the development of new attack mechanisms and countermeasures (Ukwandu, Farah, Hindy, & Brosset, 2020). However, we argue that research testbeds, new attack mechanisms, and defensive strategies must be considered to provide a holistic framework for advancing cyber security. The current use of research testbeds, attack mechanisms, and defence strategies to understand facets of cyber systems in isolation does not fully account for the complex interdependencies within such systems (Conti, Donadel, & Turrin, 2021). Therefore, understanding how research testbeds can be integrated with attack mechanisms and defensive strategies can offer solutions to complex cyber security challenges; the challenges are no longer based on the 'right' or 'true' model but on the systems view that has been adopted. Over the last few decades, the cyber security landscape has seen a steady increase in complexity, from the rise of the Internet of Things and cloud computing to the growing sophistication of cyber-attacks from legacy and emerging attack vectors (Ukwandu, Farah, Hindy, & Brosset, 2020). While many researchers have focused on attacking systems or designing defence against adversaries, less work caters to the complete understanding of research warfare. We advocate that the whole is more than the sum of its parts; research testbeds, attack mechanisms, and defence strategies can be seen as a sum of their parts (Shamsuzzaman & Mosleuzzaman, 2024). As such, we argue that a multidisciplinary approach is essential to 'raise the game' in the cyber security community. Effective defensive strategies must be formulated and adapted to accommodate real-time system attacks. These could incorporate software-defined networking-based firewalling and attacker intent recognition to develop proactive defence strategies aligned with the potential contextual threat landscape of the systems under attack (Conti, Donadel, & Turrin, 2021).

Research Testbeds in Cybersecurity

A research testbed is an environment where researchers can study phenomena that occur due to conditions intended to simulate the real world in a controlled manner (Ukwandu, Farah, Hindy, & Brosset, 2020). Testbeds in cybersecurity should facilitate scientific research and engineering and play a pivotal role in structuring relevant domains to further the field of cybersecurity. In cybersecurity, researchers use testbeds to carry out a wide variety of different studies. From the security point of view, testbeds do more than contribute to scientific work or advancements in technology; they play essential roles in validating new defence mechanisms, simulating results, and making practical suggestions and recommendations (Shamsuzzaman & Mosleuzzaman, 2024). Researchers who work in cybersecurity use several types of testbeds to carry out various studies. These include a) simulation environments, b) hardware-emulated systems, and c) live-network testbeds. Overall, a research testbed environment enables several groups, ranging from commercial organizations to different academic institutions, to study attack mechanisms using these designed testbeds to evaluate and develop better defence strategies (Huang, et al., 2023). Test environments can act as a stepping stone to simulate the effects of high-intensity attacks first-hand while analysing the real-world face of security by strengthening the theory for practical applications. Through analysing the functionality behind every type of artillery, this section provides an in-depth understanding of how attacks and practical defence mechanisms operate in a research testbed. These studies showcase the importance of knowledge of various physical effects and related mechanisms and forming a concrete foundation in policy-making and defence strategies (Ukwandu, Farah, Hindy, & Brosset, 2020).

Definition and Purpose

Research testbeds are experimental platforms used in cybersecurity to investigate the latest research phenomena, theories, threats, and vulnerabilities in international standard services, protocols, arrangements, equipment, and systems (Domínguez, et al., 2022). The experimental objectives of these virtualised or emulated systems include assessing the system's ability to mitigate potential threats by performing attack scenarios. The purposes of research testbeds, beyond the experimental purposes of design verification, are: (i) to encourage the ecosystem of effective and deployable cybersecurity solutions by researchers; (ii) to help and support the standardisation of research results in cybersecurity; (iii) before large-scale deployment, to validate proposed defence strategies in a controlled and repeatable environment (Ukwandu, Farah, Hindy, & Brosset, 2020). At first, researchers and cybersecurity professionals use testbeds to evaluate the effectiveness of defence solutions and simulate cyber threat events. Hence, the testbed is a secure cyber range, a platform reserved for a particular research group or an organisation,

where one runs several attack campaigns to validate the system's vulnerability. The purpose of a testbed is to validate response strategies by sending attack traffic to a victim network. Designing a testbed that fulfils the earlier requirements is challenging (Yamin, Katt, & Gkioulos, 2020). Companies offer proof-of-concept facilities and tools to defend against specific threats. Tailoring these tools to the general public requires accepting advanced access to these tools to verify the strategies. Many researchers provide simulators to allow validation of the research results. Still, simulators often result in a “best-case condition” because they will not consider the overhead of attack data propagation to run an actual attack. In the best-case scenario, simulators and emulations should support real solutions for increased validation potential. Ultimately, testbeds instantiating a real-world use can be created by conducting realistic attacks. Moreover, the testbed will allow the assessment of a new concept or strategy. The work will not validate a publication if the idea or technique does not significantly improve. This limits deployment on premises in public domains to validate a new system. Before release, tool developers will not want to notify the tool vulnerabilities (Ukwandu, Farah, Hindy, & Brosset, 2020).

Types of Testbeds

Three types of research testbeds are used in cybersecurity studies. Each has strengths and limitations according to the research goal, as summarised in the following (de Santana & Schwarz, 2024).

Simulation environments. Cyberspace can be modelled using mathematics and exists in the minds of humans. A simulation environment is about recreating mathematical models to produce the same behaviour. They can be run in a virtual space, though they are used in almost the same capacity as paper and programs in human behaviour planning. This is a theoretical laboratory for 'what if' and hypothesis testing. Simulations do not rely on physical law; thus, true randomness is inherently difficult to model accurately. Using simulations allows breaking nature's hold on physics; of course, one still has to rely on the programmer to not 'inject' any spooky actions (Ukwandu, Farah, Hindy, & Brosset, 2020).

Emulated systems are testbeds that replicate actual interactions of hardware and software. Data is the main thing being manipulated. This is actual computer equipment in a simulated computer network. When one starts to experience data communications, the laboratory environment becomes more challenging and directly faces the chaotic nature of an actual computer network, i.e., unforeseen and unintended consequences (Conti, Donadel, & Turrin, 2021).

Live networks. These are actual operational military, government, and public and private networks where experiments can be conducted. The testbed used varies according to military research objectives, hypotheses, questions, assumptions, and target systems. The deterministic laws of physics, as instantiated by computer hardware, software, and networks, must be adapted to the research objective (Pospisil, et al., 2021). Suppose a person wishes to study the legal, ethical, and moral economics per computer node, IP address, network protocol, or even a single packet of information. In that case, one requires the real thing or an emulation to interchange data and learn more.

The right testbed must be selected. Some reasons that might apply are: Because simulations and emulations provide a controlled environment for repeated experiments, military analyses must be done using emulation/testbed systems since you cannot, nor should not, test live to gauge the system's impact on discovery (de Santana & Schwarz, 2024). There are questions to be addressed regarding who or what computer network attack failed. Research hypotheses exist that could not be true if the test was live. Challenges abound in model development, such as the lack of cyber range automation, the scalability of exercise conditions for large-scale experiments, effective resource allocation for major real-world models, major model difficulties associated with human behaviour, intent, and action, and needed advanced security capability (Pospisil, et al., 2021).

Attack Mechanisms in Cybersecurity

The capability for conducting these attacks is more complex than ever, mainly due to the growing commercialisation of malicious cyber actors and their reliance on social engineering techniques and host-level system exploitation (Perwej, et al., 2021). Organisations of all sizes and sectors can fall victim to cybersecurity attacks. This section provides critical attack mechanisms in cybersecurity, which can further solidify the need for a more holistic framework focusing on defence strategies.

Attack Mechanisms

Financial and identity theft are two common vectors by which attackers compromise data and systems (Alawida, Omolara, & Abiodun, 2022). When attackers utilise these vectors, their technical challenges evolve into complex and intertwined social and technical aspects, illustrating the complex interrelationships between hostile players. These relationships between attackers and defenders demonstrate further skills, interchanged intelligence, economic trading, and the importance of mapping and monitoring these relationships, possibly through game-theoretical modelling and socio-political theory. Attackers can take multiple vectors to exploit vulnerabilities and launch attacks on information systems. Phishing, distributed denial of service, and malware are some of the most common.

Phishing, for example, is one of the most common ways to distribute malware (which focuses on compromising the confidentiality, integrity, or availability of information systems) (Li & Liu, 2021). Malware encompasses various forms, goes beyond viruses and worms, and targets outdated operating systems or web browsers, secretly installing itself and later replicating to other systems. Its primary purpose is usually to steal sensitive information. Similarly, DDoS floods an organisation's computer networks with illegitimate packets (Alawida, Omolara, & Abiodun, 2022). Finally, Advanced Persistent Threats patiently bypass an organisation's resources and pose as legitimate users to penetrate a network while considering the “persistence” layer to stay undetected. The growing crime market and computational power threaten information actively (Perwej, et al., 2021).

Common Attack Vectors

Attackers continuously probe an organisation's cyber defence mechanisms to identify the easiest attack vector that will gain access to sensitive systems (Aslaner, 2024). Once inside the network, attackers will look at further elevating privileges and moving laterally within the network, looking for sensitive data and servers. While many different types of attacks are detailed below, many are highly automated attacks where the attacker attempts, with a scattergun approach, to attack a wide range of assets, looking for the most vulnerable systems. Although the attack vectors are not likely to have high success based on any particular vulnerability, if the attacker successfully breaches the asset, the effect and loss to the organisation may be very significant (Yaseen, 2020). Organised crime, hacktivists, and state-sponsored capabilities will all have differing levels of preparedness and capabilities. Still, predominantly, the more sophisticated the attack, the higher the chance of being detected can be triggered. Some functions may also be significantly advanced, such as encrypting the data to protect storage. Phishing is also a standard attack that targets an individual user, where fraudulent communication is sent to deceive the target. An example of this would be an email that appears to be from an organisation and requests sensitive information (de Nobrega, Rutkowski, & Saunders, 2024). In most cases, the link goes to a fake website where the user is tricked into entering personal information and opening malicious documents.

SQL injection attacks occur when an attacker places code in a web form field, URL, or database query, ultimately enabling the attacker to gain access. An example of damage caused by SQL injection is through ransomware. Internal systems were encrypted, with the attackers gaining access to the data responsible for accounting, HR, and investor relations. The attacker informed the company that the data would become public if the ransom wasn’t paid (Yaseen, 2020). If an attack like this is successful, a company could face significant fines for not only having the data but also for being unable to protect it.

Ransomware is another type of malware that allows an attacker to encrypt an organisation’s data before requesting it pay a ransom to restore access. In some cases, the attacker will be paid but may leak crucial information on purpose to force the distressed organisation into spending more money to stop the leak. Some victims opt to pay the attacker,

but that doesn't guarantee the attackers will comply and send over the means to decrypt the files (de Nobrega, Rutkowski, & Saunders, 2024).

Advanced Persistent Threats

Advanced Persistent Threats (APTs) are sophisticated malware-based techniques invading enterprise networks (Hejase & Fayyad-Kazan, 2020). APTs are extremely hard for organisations to detect, and every year, cyber adversaries design and execute APT attacks to steal intellectual property, gather strategic intelligence, and perform corporate and government espionage, and carry out fraud, including corporate replication and investment trading skirmishes (Sharma, Gupta, & Singh, 2023). Advanced Persistent Threats (APTs) are a rising security issue. These threats are challenging to detect yet highly lucrative. The threat of an APT is pervasive and asymmetrical. Attempting to understand this persistent threat from the perspective of the various silos of cybersecurity is inherently tricky. APTs are extensive and strategic campaigns. Their phases typically include the initial compromise of an organisation's networks, establishing a foothold, intensive operational reconnaissance, escalating privileges, and subverting normal network defences. Finally, RuggedCom and Stuxnet are the most notorious APTs (Hejase & Fayyad-Kazan, 2020). The Stuxnet worm gained international attention in 2010 when it sabotaged Iran's nuclear centrifuge control systems and caused significant damage to uranium enrichment.

APTs have a wide range of implications. At the strategic level, it is evident that APTs constitute a significant category of cyber threats, which is a driving factor behind the United States and several international partners releasing major publications focused on APTs (Jabar & Singh, 2022). Finding and mitigating adversary actions are much more complex on the tactical side of an enterprise. When understanding APTs, organisations typically review the questions: "How am I currently performing against today's threats?" and "How can I do better against tomorrow's threats?" In other words, the focus of the tactical response to APTs moves from understanding (detecting APT actions) to preparation: what do we need to do or evolve in response to a determined and sophisticated adversary? The various studies highlight new tactics and techniques that adversaries use to break into organisations to steal information or perform other malicious activities (Sharma, Gupta, & Singh, 2023).

Defence Strategies in Cybersecurity

Cybersecurity consists of various strategies to prevent, detect, and counteract the actions of would-be attackers and the damage they may wish to inflict. These strategies can be categorised into three general classes: preventive measures that stop attacks from happening, detective measures that identify ongoing attacks, and corrective measures that respond to incidents. Preventive measures seek to ensure that an attack does not occur. These measures, such as firewalls or deploying intrusion prevention systems, can be direct. Another defensive strategy is through the training of end-users, allowing them to spot a social engineering attack better. All the preventive measures have in common that they attempt to identify an attack before it breaches the network so that the threat can be contained or eradicated at the perimeter. Detective measures focus on identifying an attack that is in progress. The design principle behind detective measures is to slow the attackers down.

Corrective measures will stop or minimise the impact of an already ongoing attack. Corrective measures are placed after the fact, as in the example of having backup procedures. A deliberate and continuous effort must be made to understand the attacks better, and attack mechanisms become more accurate and up-to-date. A purposeful and constant effort must be made to understand the attacks better, and attack mechanisms become more precise and up-to-date. Investigative and policy-making bodies are showing a rapidly increasing interest in the field. Any organisation, large or small, must take sound measures to protect citizens' and employees' data. Defence strategies should be layered rather than relying on a single one to ensure multi-level security. Organisations should also attend to the strategic issue of when to spend money on defence and when to budget for attack recovery. As attacks themselves change, change is necessary regularly, but security needs should not be allowed to interfere unduly with an organisation's core purposes. In an ideal world, organisations should get together to present a unified front against would-be attackers by sharing attack prevention tips and technological information.

Preventive Measures

Implementing defensive strategies to prevent attacks refers to improving the system's security and increasing the difficulty level of designing new attack mechanisms or launching known attacks on possible targets (Ghiasi, et al., 2023). Suppose an attacker, understanding a specific attack mechanism and being able to aim it at one's victim, sees that the potential overall gain will likely be low. In that case, he or she will probably desist from the attack. On the other hand, an attacker may decide to stop the attack based on real-time monitoring of the likelihood estimation of the profitability of the attack. In other words, the effort likely to be spent would be much more than the gain if the attack is executed. Most of these are well-known risks managed daily by system administrators (El Kafhali, El Mir, & Hanini, 2022). This method is used in everyday responses to reduce the number of security incidents initiated by attackers and to improve the current intrusion detection systems. Information can be well protected through a layered approach, such as increased network security infrastructure and server protection mechanisms. Some attacks that attackers fail to predict require a high level of technical skill and security control to be effective. For example, phishing attacks could surprisingly work since they target many uneducated users. Still, an organisation can effectively use user awareness and software products as a multi-layered approach to its systems (Ghiasi, et al., 2023). Every time a potential client follows a link to an illegal website, the web browser will lock down and, in the process, alert the system administrators to possible attempts to execute unwanted content sent by the phishing attack. This indicates the point reached in the progress of the phishing attempt when the response was formulated (El Kafhali, El Mir, & Hanini, 2022).

Detective Measures

Detecting a threat or vulnerability before it becomes significant is essential and is known as a detective measure (Chakraborty, Krishna, & Ding, 2021). One must be aware of and consider the existing threats and vulnerabilities to utilise such measures. There are generally two main components in detection: 1) the subsystems that gather data and information about threats and vulnerabilities, such as intrusion detection systems and security information and event management solutions, and 2) the analytical model used to provide interpretation of threats and vulnerabilities to the system, such as regular audits, awareness, and event-based systems. For real-time detection, methods are used to collect data from the path of information like headers, packets, protocols, and systems that aid in categorising network threats and help in linking network actions of malicious activity with sensors deployed on the network (Ghelani, Hua, & Koduru, 2022). Continuous monitoring is mandatory to indicate when a security breach has happened, and this can be realised by using alerts and real-time detection systems. The efficiency of such a mechanism is the responsibility of one of the detective measures. However, if an incident occurs, the ability to respond is needed. The major drawback of detective measures is that an incident is generally reported and recognised as having happened after the fact. Therefore, there is a high probability that attackers will have the opportunity to cause damage before the threat is detected or the vulnerability exploited (Chakraborty, Krishna, & Ding, 2021). Producing a structured approach that will allow IT administrators to assess threats, define guidelines, and show them how to develop incident handling flow techniques is a valuable application for this research area.

In addition, the following situations can contribute to successful preventive practice based on the classified threats, as outlined in an incident response strategy based on the solutions formulated in the directive. Investigation and tracking of some intrusions, as well as discernment of planned attacks, are made possible by descriptive analytics (Ghelani, Hua, & Koduru, 2022). The problem, however, is that Pareto's Rule of 90/10 dictates that only a few of these warnings will raise the bar significantly and, therefore, require attention. Moreover, the software could deliver up to 1 TB of valuable analysis data daily, which may be presented to the analyst as events in real-time. For systems with this output type, the analyst's workload is more likely to be impractical (Chakraborty, Krishna, & Ding, 2021).

Corrective Measures

In this case, we assume that something has already gone wrong: unauthorised access has happened, and we need to control it, prevent further damage, and recover (Mughal, 2022a). Everyone agrees that the more preventive measures you put into place, the better you can protect your network simply because the potential for success is reduced. We are also looking at the broader perspective of learning from network security and network security services. These findings can be used to reformulate and modify the policy that, directly or indirectly, guides security at different levels of an organisation (Mughal, 2021). Having incident response plans in place in an organisation is critical. An incident response plan helps to address the aftermath of an attack in an efficient manner. These plans are generally divided into four phases: 1. Preparation; 2. Detection; 3. Containment; and 4. Recovery. Following an incident, these four phases must sometimes be adapted, particularly for different parts of the organisation's infrastructure. To be most effective, post-incident plans and policies are ideally refined and improved over time by applying them in practice, in real situations (Shwedeh, Malaka, & Rwashdeh, 2023). Detection is also problematic in practice for various reasons, not all relating to technological capabilities. For example, real-time monitoring is typically expensive in terms of computing resources and staff time. It is also difficult to differentiate security threats from other system problems and to differentiate among security threats themselves.

It is unclear when one must be most concerned about ongoing threats or tactics. Many intrusion detection system logs may contain repeating signatures representing these concurrent ongoing attacks, but the rate of false alarms is much higher (Mughal, 2022a). Maintaining effective communications becomes increasingly difficult as the population at risk of participating in truly distributed attacks or similar coordinated efforts increases. Furthermore, what may work to foil an attack today may not be effective next week as attackers adapt their tactics. In the case of a security breach, organisations must engage with an entire support ecosystem in outreach and coordination communications, both for immediate response requirements and to maintain trust relationships and provide information to the community (Mughal, 2021). It is also important to show those involved that we take the incidents seriously and do all in our power to maintain excellence and integrity in our organisation. This results in a significant investment in time and financial resources. The final consideration is that an attack cannot bring down old systems or those that cannot be changed quickly. They must have their measures to survive an attack (Shwedeh, Malaka, & Rwashdeh, 2023).

Integrating Research Testbeds, Attack Mechanisms, and Defence Strategies

There is a recognised need for more integration and a spiral approach between research testbeds, attack mechanisms, and defence strategies (Chen, Tan, & Pi, 2021). The text outlines key challenges in integrating practical implementation and academic research and how this must be addressed to ensure we make balanced progress. Too often, there may not be any mechanisms through which research models and algorithms can be tested or verified, or the methods to prototype and implement solutions in a given sector may not yet have been addressed in the academic literature (Young & Bleakley, 2020). Either way, this can provide an unwanted barrier to innovation, making it more challenging to develop real-world prototypes, testbeds, and demonstrators that could potentially attract investment. In addition, some sectors (by their purpose) may need to understand attack mechanisms or potential security flaws in greater detail than is available from traditional business intelligence (Zhou, et al., 2021). Such regulators may also drive new operational controls and industry standards as best practices from emerging research and development. Moreover, if sectors are to defend against new, novel, or niche attacks, they must have a transparent model of how they might occur. This is a significant resource commitment, and as such, it is more the exclusive preserve of the larger engineering organisations.

Further, valuable measures of an attack's probability, impact, cost, or likelihood of going undetected can be inferred for particular systems of critical infrastructure, assets, safety systems, or control loops. In that case, they are better placed to decide whether to invest in additional countermeasures or protection (Chen, Tan, & Pi, 2021). Integrating testbeds, attacks, and strategies can provide a comprehensive and powerful tool. These outputs can assist an organisation in adhering to the new risk management standard and complying with other emerging IT security management standards. The high-level solutions can be used to develop operations concepts for a computer security incident response centre to manage cyber incidents locally with constituents (Young & Bleakley, 2020). By gaining these metrics, organisations can budget and invest according to their individual needs and make a more informed

judgment about the capacity and potency of their countermeasures and security technology portfolio. Best practices in research testbeds and integrating the technical-social aspects of cybersecurity are outlined (Zhou, et al., 2021). The ongoing communication and development initiated between known industry sector groups are considered particularly beneficial and essential in achieving the objectives of the national critical infrastructure protection research and technology strategy and ensuring a continual spiral approach to the innovation improvement cycle. Multi-sector use, inputs/outputs, and sub-projects between different groups are a valuable way of further improving and increasing the addressable audience of cross-cutting outputs from infrastructure research and technology. The valuable insights and networking opportunities relating to strategic consensus on forward research and technology priorities are particularly helpful in forging new collaborations, partnerships, and stakeholder relationships throughout this and other critical infrastructure protection research and technology solutions (Chen, Tan, & Pi, 2021). It also highlights to potential customers/constituents the variety of capabilities being addressed and developed and the potential range of security solutions that will emerge from the research and technology (Zhou, et al., 2021).

Figure 1 illustrates the interconnected relationships between **research testbeds**, **attack**, and **defence mechanisms**, offering a holistic framework for understanding how these components interact within cybersecurity. Each element plays a distinct yet interrelated role in developing and implementing strategies to counteract cyber threats.

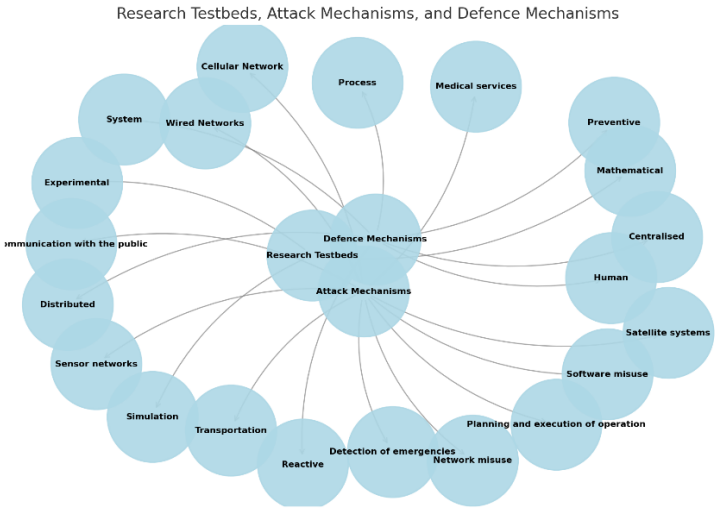

Figure 1: The relationships between research testbeds, attack, and defence mechanisms.

The figure underscores integrating research testbeds, attack, and defence mechanisms to create a comprehensive and adaptive cybersecurity framework. This integrated approach enables continuous improvement in understanding and defending against cyber threats, ultimately contributing to a safer and more secure digital environment.

1. Research Testbeds

Research testbeds provide controlled environments for testing and evaluating cybersecurity tools, techniques, and theories. The figure categorises testbeds into three primary types:

I. ***Mathematical* Testbeds**: Focus on theoretical models and simulations to predict system behaviour under various attack scenarios.

II. ***Simulation Testbeds****:* Virtual environments replicating real-world networks and systems to study the impact of cyberattacks and evaluate defensive measures.

III. ***Experimental Testbeds****:* Physical setups involving actual hardware and software that mimic operational systems, enabling high-fidelity testing.

Relationship*:* Research testbeds are foundational to the figure as they create environments where attack and defence mechanisms can be applied, tested, and evaluated. For example, an experimental testbed might simulate a hospital's network to assess its vulnerability to ransomware.

2. Attack Mechanisms

Attack mechanisms represent the various methods and strategies used by adversaries to exploit vulnerabilities in systems. These are further subdivided into:

I. ***Network-based attacks,*** Such as flooding, masquerading, and exploiting node vulnerabilities.
II. ***Software Misuse****:* Includes attacks executed locally or remotely, such as malware, SQL injection, and phishing.
III. ***Functional Disruptions****:* Attacks targeting specific system functions, such as emergency detection systems, transportation, or communication networks.

Relationship*:* Attack mechanisms link to research testbeds, as testbeds simulate or emulate these mechanisms. This allows researchers to understand how attacks propagate and impact systems, which is crucial for developing effective countermeasures. For example, a testbed might simulate a phishing campaign to study how it exploits user behaviour.

3. Defence Mechanisms

Defence mechanisms are strategies and tools designed to protect systems from cyber threats. The figure categorises these into:

I. ***Preventive Mechanisms****:* Include measures such as authentication, system resilience, and self-awareness to prevent attacks proactively.
II. ***Reactive Mechanisms****:* Focus on detection and response, including incident handling and system recovery after an attack.
III. ***Organisational Elements****:*
    a) ***System-Level Defences****:* Focus on technical solutions like firewalls and intrusion prevention systems.
    b) ***Process-Level Defences***: Encompass security policies, standards, and procedures.
    c) ***Human-Level Defences****:* Include user awareness training and behavioural monitoring.

Relationship*:* Defence mechanisms interact with both research testbeds and attack mechanisms:

With Testbeds: Defence mechanisms are tested within research testbeds to evaluate their effectiveness under simulated attack conditions. For example, intrusion detection systems might be assessed using experimental testbeds.

With Attack Mechanisms: Defence strategies are designed in direct response to identified attack mechanisms. For example, phishing attacks may be countered with enhanced user training and email filtering systems.

4. Interdependencies and Feedback Loops

The figure also highlights the dynamic interplay between the three elements:

I. ***Testbeds and Attack Mechanisms****:* Testbeds are used to replicate attack mechanisms, providing insights into how they function and enabling researchers to identify vulnerabilities.
II. ***Attack Mechanisms and Defence Mechanisms***: Attack mechanisms inform the design and refinement of defence strategies, while effective defences can influence the evolution of attack strategies.
III. ***Testbeds and Defence Mechanisms****:* Testbeds provide a controlled environment for testing and refining defence mechanisms, ensuring they are robust and effective against evolving threats.

5. Practical Applications

The relationships depicted in the figure have several practical implications:

I. ***Critical Infrastructure Protection****:* Testbeds can simulate attacks on power grids or healthcare systems, allowing for the development of targeted defence strategies.
II. ***Cyber Threat Intelligence****:* Organisations can develop more effective threat detection and mitigation techniques by simulating and studying attack mechanisms.
III. ***Policy Development****:* Insights from testbeds can inform organisational policies and industry standards, improving overall cybersecurity resilience.

Challenges and Opportunities

The cybersecurity community often lacks the necessary solutions and strategies to address increasing threats (Ghelani, 2022). In part, such capabilities may be developed by having tight integration between research and operational practices and environments. However, pressing challenges must be addressed to ensure effective exchange and collaboration. There is a lack of scalability between the operational environments and the narrow and targeted domains in which research testbeds operate (Aslan, et al., 2023). This is challenged by the scalability of the wide variety of cyber aspects that such research could apply to and the narrow approach most research takes. Additionally, the stress testing process inherently has a broad definition of necessary scope and expensive development processes. Generally, it requires organised attacks over timescales that are often impractical for research purposes (Ghelani, Hua, & Koduru, 2022). Each of these challenges will likely reduce the potential funding and collaborative opportunities to a clear standardisation of integration of tools and approaches to foster precise evaluation and compare and contrast collaborative effects. Political and confidential concerns pose the most significant practical challenges for integrating research approaches with operational contexts. Cybersecurity is dynamic and evolving, and attackers use various strategies to break into computational systems (Ghelani, 2022).

Despite the challenges above, tight research practice integration can create ample opportunities. Some good case studies show the opportunities for value-added utilisation. Additionally, successful collaborative efforts are positively advancing security systems (Aslan, et al., 2023). The research community and industry possess different expertise, insight, and specialised work areas. Individually, these areas develop strategic opportunities to support, in theory, a well-rounded operational view of operational relevance and reality. Multiple research agendas can provide the necessary specialisations to foster an operationally viable, deployable, and defendable concept of whole system security. Ongoing research can ensure that strategic work and thoughts are at the cutting edge and address evolving thoughts, strategies, and technological defences (Ghelani, Hua, & Koduru, 2022). Evidence, not just concept, supports deploying a cybersecurity framework with some value.

Best Practices

We aim to define a best practices guideline to integrate testbeds, attack, and defence strategies to achieve a safer internet (Chygryn, Bilan, & Kwilinski, 2020). This can be achieved by improved cooperation between researchers and other stakeholders that use these operationally. Technical solutions are often seen as the only way to improve future cyber defences. Still, without extensive cooperation between the different stakeholders, this development will increasingly be unable to adapt to the requirements. A framework focusing on cooperation could show the stakeholders what they could gain (Bridoux & Stoelhorst, 2022). A range of best practices were found. Working iteratively is essential to constantly improving testbeds, attack mechanisms, and defence strategies. Developing testbeds, attack, and defence mechanisms often requires adjustments that could be defined as prototypes. With continuous feedback, aspects of the system should be improved. In the different sectors (testbed, attack, or defence), the development might be better realised by other experts; however, it is essential to have good communication between the sectors (Chygryn, Bilan, & Kwilinski, 2020).

In conclusion, one should adjust the interdisciplinary scientific approach across the pipeline. To ensure a high level of cooperation between all stakeholders, it is essential to use a standard process for attack and defence strategy exchange. Work on standardising the process among researchers could potentially lead to a more widely available database that improves the collective goals for securing cyberspace. Research in a testbed focuses on attacking and defending against a single system. The opportunity to share a system for development is essential as it will allow collaborative working (Bridoux & Stoelhorst, 2022). Often, staff in operational environments are not familiar with the advances in testbed or academic research. Developing training provisions across the industry would be a successful interim measuring tool. Providing standard drafting to multiple stakeholders would offer an iterative approach and make technology development accurate. Functions can also be used as a starting point for new areas where data isn't successful. It is essential to have a system that promotes both success and failure, as it encourages inter-stakeholder response (Chygryn, Bilan, & Kwilinski, 2020).

Conclusion

Organisations and individuals must collaborate and share information and experiences to design and build an in-depth defence. They must extend their first line of defence and protect their resources and assets more effectively. This conclusion identifies what needs to be done in cybersecurity to improve the defence against automated and complex cascading cyber-related events. Constructing a cybersecurity regime consisting of cybersecurity research testbeds, a scientific program that develops new attack mechanisms, and high-quality test data is central to our message. In contrast, increased operational resilience and continuous monitoring are just as critical. The new vision to strengthen cybersecurity assumes that defensive tools must be developed based on current and future attacks, attackers, and attack patterns. A proactive stance by operational managers is, however, of equal importance. They need to integrate cybersecurity into their current and future risk management framework to continue uninterrupted core business functions, even in the face of a high-probability, high-risk cyber event. Consequently, security professionals must know where their systems are vulnerable and accept this. They must appreciate evolving threats and operational environments and realise that they need to be adaptable, not simply to use the best defensive options but also to operate continuously within acceptable risk boundaries. Significantly, the work of the science strand of our vision influences the broader operational environment. It connects research and practice in a way that is rarely seen in today's cybersecurity efforts in the public or private domain. Practice informs science, and through new scientific knowledge and insights, practice is stretched and extended to new capabilities.

References

Alawida, M., Omolara, A. E., & Abiodun, O. I. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud*. sciencedirect.com

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., & Yilmaz, A. A., et al. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*. mdpi.com

Aslaner, M. (2024). Cybersecurity strategies and best practices: A comprehensive guide to mastering enterprise cyber defense tactics and techniques. HTML

Bridoux, F., & Stoelhorst, J. W. (2022). Stakeholder governance: Solving the collective action problems in joint value creation. *Academy of Management Review*. researchgate.net

Chakraborty, S., Krishna, R., & Ding, Y. (2021). Deep learning-based vulnerability detection: Are we there yet? *IEEE Transactions on ...*. PDF

Chen, W., Tan, J. S. H., & Pi, Z. (2021). The spiral model of collaborative knowledge improvement: An exploratory study of a networked collaborative classroom. *International Journal of Computer-Supported*. researchgate.net

Chygryn, O. Y., Bilan, Y. V., & Kwilinski, A. (2020). Stakeholders of green competitiveness: Innovative approaches for creating communicative system. .... sumdu.edu.ua

Conti, M., Donadel, D., & Turrin, F. (2021). A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*. PDF

de Nobrega, K. M., Rutkowski, A. F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *The Journal of Strategic*. sciencedirect.com

de Santana, K. G. Q., & Schwarz, M. (2024). Cybersecurity testbeds for IoT: A systematic literature review and taxonomy. *Journal of Internet*. sbc.org.br

Domínguez, M., Fuertes, J. J., Prada, M. A., & Alonso, S. (2022). Design of platforms for experimentation in industrial cybersecurity. *Applied Sciences*. mdpi.com

El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering, Springer*. researchgate.net

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A review. *Authorea Preprints*. techrxiv.org

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints*. authorea.com

Ghiasi, M., Niknam, T., Wang, Z., & Mehrandezh, M. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems*. HTML

Hejase, H. J., & Fayyad-Kazan, H. F. (2020). Advanced persistent threats (APT): An awareness review. *Journal of Economics*. researchgate.net

Huang, H., Wlazlo, P., Sahu, A., & Walker, A. (2023). Validating an emulation-based cybersecurity model with a physical testbed. *... on Dependable and ...*. HTML

Jabar, T., & Singh, M. M. (2022). Exploration of mobile device behavior for mitigating advanced persistent threats (APT): A systematic literature review and conceptual framework. *Sensors*. mdpi.com

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. sciencedirect.com

Mughal, A. A. (2021). Cybersecurity architecture for the cloud: Protecting network in a virtual environment. *International Journal of Intelligent Automation*. tensorgate.org

Mughal, A. A. (2022). Building and securing the modern security operations center (SOC). *Journal of Business Intelligence and Big Data*. tensorgate.org

Perwej, Y., Abbas, S. Q., Dixit, J. P., & Akhtar, N. (2021). A systematic literature review on the cyber security. *International Journal of ...*. hal.science

Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R., et al. (2021). Application perspective on cybersecurity testbed for industrial control systems. *Sensors*. mdpi.com

Shamsuzzaman, H. M., & Mosleuzzaman, M. D. (2024). Cybersecurity risk mitigation in industrial control systems analyzing physical hybrid and virtual test bed applications. *Academic Journal on ...*. researchgate.net

Sharma, A., Gupta, B. B., & Singh, A. K. (2023). Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures. *Journal of Ambient*. HTML

Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The moderation effect of artificial intelligent hackers on the relationship between cyber security conducts and the sustainability of software protection: A .... *Migration Letters*. researchgate.net

Ukwandu, E., Farah, M. A. B., Hindy, H., & Brosset, D. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*. mdpi.com

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*. ntnu.no

Yaseen, A. (2020). Uncovering evidence of attacker behavior on the network. *ResearchBerg Review of Science and Technology*. researchberg.com

Young, D. G., & Bleakley, A. (2020). Ideological health spirals: An integrated political and health communication approach to COVID interventions. *International Journal of Communication*. ijoc.org

Zhou, Y. C., Tan, S. R., Tan, C. G. H., Ng, M. S. P., & Lim, K. H. (2021). A systematic scoping review of approaches to teaching and assessing empathy in medicine. *BMC Medical*. springer.com