

A Review of Endogenous Security Research

Xiaoyu Liu, Haizhou Wang and Cuixia Li *

School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450002, China;
lxiaoyu@gs.zzu.edu.cn (X.L.); hzw@gs.zzu.edu.cn (H.W.)

* Correspondence: lcxxcl@zzu.edu.cn

Abstract: The development of society has deepened the application of the Internet in production and daily life. At the same time, network security risks are becoming increasingly severe. For the security problems faced in cyberspace, most of the traditional defenses are currently focused on blocking the discovered vulnerabilities. However, these methods not only rely on prior knowledge of vulnerabilities but also fail to address the security issues brought about by the protection program itself. In view of this, endogenous security, which emphasizes the importance of not relying on a priori knowledge and not bringing in new security problems, has received increasing attention. This review provides a detailed introduction to endogenous security and its related issues, which is lacking in the field of network security. Firstly, this paper outlines the detrimental effects of vulnerabilities, identifies issues within moving target defense, and contrasts it with mimic defense. Additionally, the concepts, models, principles, and application scenarios of endogenous security are introduced. Finally, the challenges encountered by this technology are comprehensively summarized, and potential future development trends are further explored.

Keywords: endogenous security; mimic defense; dynamic heterogeneous redundancy



Citation: Liu, X.; Wang, H.; Li, C. A Review of Endogenous Security Research. *Electronics* **2024**, *13*, 2185. <https://doi.org/10.3390/electronics13112185>

Academic Editor: Andreas Mauthe

Received: 10 April 2024

Revised: 16 May 2024

Accepted: 23 May 2024

Published: 3 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cyberspace security is an important issue in the Internet era. In 2023, the H3C Cybersecurity Vulnerability Landscape Report recorded a total of 29,039 vulnerabilities, representing a 16.6% increase from 2022's tally of 24,892, making it the highest number in history [1]. Of these vulnerabilities, there are 4298 ultra-hazardous vulnerabilities and 10,741 high-risk vulnerabilities. The ratio of ultra-hazardous to high-risk vulnerabilities stands at 51.8%, and the number of vulnerabilities classified as high-risk or higher has increased by 7.1% compared with 2022. The number of publicly disclosed vulnerabilities has been steadily rising since 2017, with an annual increase of over 10%. Meanwhile, the risk of vulnerabilities in network security products is also increasing, making the network security situation more complex and severe [2]. Although existing defense mechanisms such as firewalls [3], intrusion detection systems (IDSs) [4], and vulnerability scanning technology [5] can detect and defend against known types of network security threats, they struggle to prevent unknown vulnerabilities and backdoors. This reliance on a priori knowledge renders defenders passive in the face of attack and defense confrontations.

In probability theory and statistics, a priori knowledge and posterior knowledge are the two basic concepts of Bayesian inference. Prior knowledge refers to our existing understanding or confidence in an uncertain parameter before observing any data, which may stem from past research, expert insights, or historical data accumulation. Conversely, posterior knowledge represents updated cognition or confidence after observing data, derived from the analysis of new data. In cybersecurity, prior knowledge can be seen as a general understanding of cyber attacks, while posterior knowledge may involve precise insights into an attacker's tactics gained from analyzing specific network traffic or attack events.

To address these challenges, mobile target defense (MTD) [6] transforms traditional static passive defense strategies into dynamic active defense strategies. By constantly changing the environment and resource allocation of the target system, MTD increases the difficulty for attackers to create and maintain attack chains. However, MTD still fundamentally fails to address security problems inherent in defense mechanisms as none of these defenses have endogenous security properties [7]. To tackle these issues, the literature [8] proposes a defense mechanism called cyberspace mimic defense (CMD). CMD constitutes a dynamic heterogeneous redundancy structure, adding a dynamic, random, and diversified mechanism based on negative feedback control to the dissimilar redundancy structure (DRS). This not only effectively defends against threats posed by unknown vulnerabilities and backdoors but also addresses endogenous security problems inherent in defense mechanisms.

Diversity-based intrusion tolerance technology enhances the robustness and survivability of information systems, ensuring the normal operation of security systems in harsh environments. However, due to its redundancy and voting mechanism, the application of this technology is more expensive and costly [9]. While its dynamic migration and reconfiguration characteristics can increase the difficulty of third-party attacks and the cost of hacking, the higher frequency of communication changes will directly affect the robustness and stability of the information system. Therefore, the core of this technique lies in balancing system performance and change frequency. In addition, in some cases, the information security system designed based on the MTD concept is essentially a single static system, which will increase the success rate of attackers and cannot effectively protect network security. Unlike MTD based on a stealth mechanism, DHR “neutralizes” or masks the output of the attacked target by voting the output, thereby reducing the success rate and impact of third-party attacks on the information security system. DHR has efficient and reliable defense capability at the router and web server level, making it widely used in various fields.

2. Endogenous Security in Cyberspace

2.1. Definition of Endogenous Security Issues

In network environments, to reduce system structure complexity and operational costs, people often choose to implement specific functions through a single protocol standard or a unified software and hardware scheme. However, this practice also introduces potential vulnerabilities in cyberspace. Therefore, diversity is regarded as one of the important means to enhance the service function of cyberspace and the anti-attack capability of network elements and terminals. Diversity is mainly reflected in two aspects: diversity of executors and diversity of execution space. Executor diversity involves heterogeneous CPUs, diversified operating systems, databases, and functional software. Execution space diversity refers to isolating the operating environment that hosts the executor, such as using different virtual environments or execution platforms.

Dynamics is a characteristic of a system that changes over time, sometimes referred to as “time-varying” in certain fields. Time-varying systems are distinctive because their outputs are influenced not only by the inputs but also by the timing of the input loads. This feature not only adds complexity to system analysis and research but also increases the cost and difficulty of attacks.

The first step to understanding the importance of dynamism is the proper allocation of redundant resources. Redundancy, in this context, is a method to mitigate the risk of system damage caused by unforeseen events by adding extra resources. In other words, the level of resource redundancy directly determines the extent of dynamic adjustment of the system, as well as its fault tolerance and resilience—its ability to withstand stress and remain robust in the face of errors or intrusions.

Ref. [10] proposes the principle of incomplete intersection. As illustrated in Figure 1, the three domains D, V, and R correspond to dynamism, diversity, and redundancy, respectively. If there is a lack of comprehensive intersection between these three domains, or only

partial intersections exist, they will not be able to effectively defend against cyberattacks launched based on unknown vulnerabilities and backdoors within the target object.

In other words, without the need for prior knowledge as a foundation, if there is no complete intersection between D, V, and R, then the issue of unknown security threats in cyberspace will not be effectively addressed. When a defense system fails to achieve a complete intersection in terms of dynamism, diversity, and redundancy, the system lacks the ability to prevent and respond to unknown security threats and disruptions, indicating that the system does not possess endogenous security characteristics. The term “endogenous” is used to describe factors (or variables) within a system or model that are closely related and indivisible. Unlike factors that can be embedded or added, endogenous factors refer to core components that cannot be isolated from the system or model. The concept of endogenous security involves achieving quantifiable, designable, verifiable, and measurable security functions through the inherent architecture, functions, and operating mechanisms of the system itself. This security is not simply embedded in existing technology; rather, it is a natural part of the system and is designed to address both known and unknown security threats through a well-designed security architecture.

Endogenous security is a philosophical generalization and exposition of ref. [11] regarding the status of cyberspace security. It represents an emerging concept in the field of cybersecurity and technological development. Specifically, it encompasses two aspects: endogenous security issues and endogenous security institutional mechanisms.

Endogenous security in cyberspace can be categorized into two types of issues. One type is narrow endogenous safety and security (NESS), which pertains to software and hardware systems that, aside from their intended design functions, always contain explicitly or implicitly expressed non-expected functions, including side effects, vulnerabilities, and natural breakdowns. The other type of issue is general endogenous safety and security (GESS), which refers to systems specifically designed to be safe and secure in cyberspace. GESS encompasses the narrow endogenous security issues, including hidden functions not visible to end users or functions not explicitly declared or disclosed by hardware and software to the user, such as front doors, backdoors, trapdoors, and other “dark functions”.

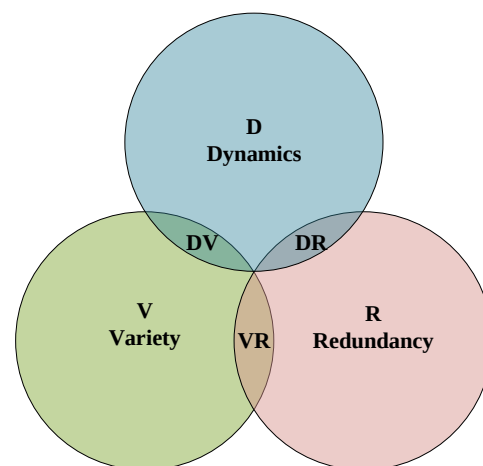


Figure 1. The principle of incomplete intersection.

At present, there is little that can be accomplished regarding defense against uncertainty threats based on endogenous security issues. The security design of information systems or control devices is unquantifiable, and verified metrics seem to have become the “Achilles’ heel” of cyberspace. Philosophically speaking, endogenous security problems are difficult to completely eliminate; only “conditional avoidance” can be implemented within the constraints of space and time. In theory and practice, researchers have been attempting to eradicate endogenous security problems for many years, but success remains elusive. A review of traditional cybersecurity thinking and technical approaches makes it clear why cyberspace security has fallen into its current predicament. However, it is worthwhile for

researchers to focus on and overcome the scientific and technological challenges of “conditionally avoiding or mitigating” uncertain threat impacts based on endogenous security issues. In the context of endogenous security, a domestic team, after extensive research and repeated practice, proposed a dynamic heterogeneous redundancy structure to address or mitigate the risks posed by “known unknowns” or “unknown unknowns” within the target object. This principle and method are named cyberspace mimic defense (CMD).

2.2. Approaches to Endogenous Security

According to the literature [12], the term “endogenous” refers to factors (or variables) within a system or model that are inherently interrelated and inseparable. Unlike factors that can be embedded or added externally, endogenous factors constitute core components that are integral to the system or model. On the other hand, the concept of endogenous security revolves around achieving quantifiable, designable, verifiable, and measurable security functions through the inherent characteristics of the system’s architecture, functionality, and operational mechanisms. This type of security does not merely rely on embedding into existing technologies; rather, it stems from the natural properties within the system, aiming to mitigate both known and unknown security threats through a well-designed security architecture. The application of endogenous security concepts is versatile, spanning numerous scenarios and technologies. For instance, the literature [13] combines AI with endogenous security principles to introduce a novel endogenous security defense mechanism called LSSM.

In biology, the phenomenon where an organism mimics its environment or another organism in terms of color, texture, and shape is called mimicry. According to defense behavior, it can be classified into the category of active defense-based on endogenous mechanisms, and the literature [14] on cyberspace mimicry defense refers to it as “mimic guise” (MG). Mimicry is very common in nature; for example, the *kallima inachis* butterfly can mimic the color of dead leaves, perfectly concealing its movements in the environment to avoid detection by natural enemies. Inspired by the defense effect demonstrated by mimicry in the biological world, the literature [14] proposed cyberspace mimicry defense (CMD) to address endogenous security problems. CMD is the first active defense theory pioneered by a domestic research team, and its core implementation is a dynamic heterogeneous redundancy construction (DHR) based on the endogenous security mechanism in cyberspace. The DHR provides innovative defense theories and methods of universal significance to deal with unknown threats in cyberspace, such as location vulnerabilities, backdoors, viruses, and Trojans.

Similar to mimic defense in biology, in the field of cyberspace defense, under the premise of maintaining the unchanged function and performance of a given service of the target object, various environmental factors such as its internal architecture, redundant resources, operation mechanism, core algorithms, and anomalous performance, as well as unknown vulnerabilities, backdoors, or Trojan horses that may be attached to it, can all be strategically altered in time and space. This creates a “plausible but not real” situation for the attacker. The attacker is presented with a scenario that seems “plausible but not true”, disrupting the construction and effectiveness of the attack chain and increasing the cost of a successful attack.

CMD aims to integrate multiple active defense elements. It achieves this by introducing heterogeneity, diversity, or plurality to change the similarity and singularity of the target system. CMD also introduces dynamism and randomness to alter the static and deterministic nature of the target system. CMD identifies and shields against unknown defects and unidentified threats using heterogeneous redundancy and multimode adjudication mechanisms. Additionally, it enhances the flexibility and elasticity of the target system’s service function with a high-reliability architecture. CMD defends against attackers by introducing uncertainty regarding the system’s apparent attributes.

3. Specific Implementations of Mimic Defenses

The cyberspace mimic defense system described in this section includes concepts, rules, and models.

1. The concepts of CMD include functionally equivalent heterogeneous executors, mimic defense boundaries, mimic brackets, and related core mechanisms.
2. The rules of CMD include that the external service request of the target object must be distributed to each executor according to the policy, the output vector of the multimodal executor must be adjudicated according to the policy, the multidimensional dynamic reconfiguration and policy scheduling must be composed of a closed-loop feedback control with the policy adjudication, and so on.
3. The model of CMD is a mimic IPO model, as shown in Figure 2. P represents a complex network element, hardware, software processing system or component, or module or building block. P connects to the left bracket (input agent) of input I with a policy distribution function. The functional mode can be static, dynamic, or random and can be one-to-one or broadcast. The brackets connected to P have multimodal adjudication functions and normalization functions for heterogeneous object input or output information.

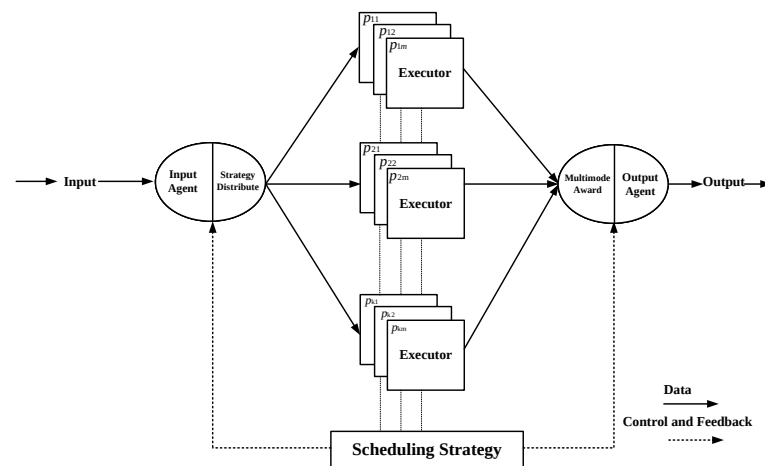


Figure 2. The CMD IPO model.

An abstract model of the mimic defense system is shown in Figure 3:

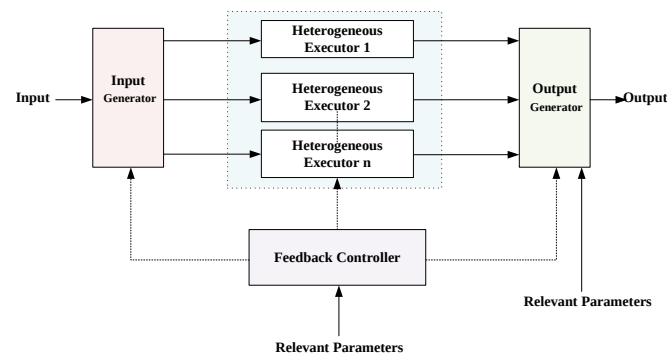


Figure 3. The CMD abstract model.

According to the literature [15], we can grasp the basic concept of CMD. When discussing the functional implementation of CMD, its function equal object (FEO) assumes a variety of forms. These FEOs can exist at various levels and granularities, including networks, platforms, systems, components, and modules, among others. They can be purely software-based, hardware-based, or a hybrid of both software and hardware solutions, or even the products of virtualization technology. In summary, while FEOs may differ in

structure, their core functions remain equivalent. The ideal FEO design aims for functional purity, meaning that there should be no functional overlap between them beyond the intended normal function. Consequently, regardless of the potential security risks contained within these heterogeneous entities, such as unknown vulnerabilities, backdoors, viruses, Trojans, and so forth, they should not generate the same unintended output response upon receiving identical inputs.

The mimic interfaces (MIs) and mimic brackets (MBs) introduced in CMD constitute a powerful mimic defense system. Mimic boundaries define specifications and protocols for service functions and determine the equivalence of heterogeneous executables for a given service function and performance through conformity testing. The mimic bracket then serves as the protection boundary, including input agents, feedback controllers, and output extractors, and achieves dynamic management and protection of multimodal actuators through core mechanisms such as mimic rulings, multidimensional dynamic reconfiguration, cleaning recovery, state synchronization, and feedback control.

One of the key mechanisms in this context is the mimic ruling (MR), which is instrumental in adjudicating multimode output vectors. This involves both multimode ruling and policy ruling. Multimodal adjudication allows for flexible selection of corresponding vectors through voting and policy adjudication, enabling the perception and determination of the operational status of heterogeneous actuators. To disrupt the synergy of attacks and negate the inheritability of phase results, multi-dimensional dynamic reconfiguration and policy scheduling are employed to alter the operating environment of the executives. In addition, cleaning recovery and state synchronization mechanisms are utilized to address anomalous output vectors from heterogeneous executables. This includes restarting anomalous executables, synchronizing their operating environments, and resolving restarted anomalies into standby states.

Feedback control is a key link where the output adjudicator sends adjudication state information to the feedback controller, which generates control instructions based on the algorithms and parameters of the control channel and realizes the operation instructions to the input agents and reconfigurable executables in order to dynamically select the heterogeneous executable elements to compose the current service set of the target object. This negative feedback mechanism is designed to evaluate the effectiveness of the defense scenario in a timely manner and decide whether to continue changing the defense scenario to avoid unnecessary system overhead.

Taken together, these key mechanisms and components in CMD collaborate with each other to build an efficient, flexible, and multi-layered mimic defense system that provides comprehensive and powerful protection for heterogeneous executables [15].

The basic process of mimic defense is shown in Figure 4:

The input information is connected to the heterogeneous executor via an input agent. The online executor compiles the input information across multiple levels of diversity. For the attack to be successful, the attacker must execute a multi-targeted attack within the mimetic environment and achieve the desired effect.

The mimetic adjudication process involves adjudicating the output information of the heterogeneous executor through combined or iterative methods, such as multi-selection, consistency comparison, and weight adjudication. It is then necessary to send the adjudication results to the feedback controller.

Based on these results, the feedback controller performs various tasks including scheduling, executor replacement, executor cleanup, and other processes until the system meets the established requirements. Finally, the output agent ensures normalized output for multi-modal output adjudication.

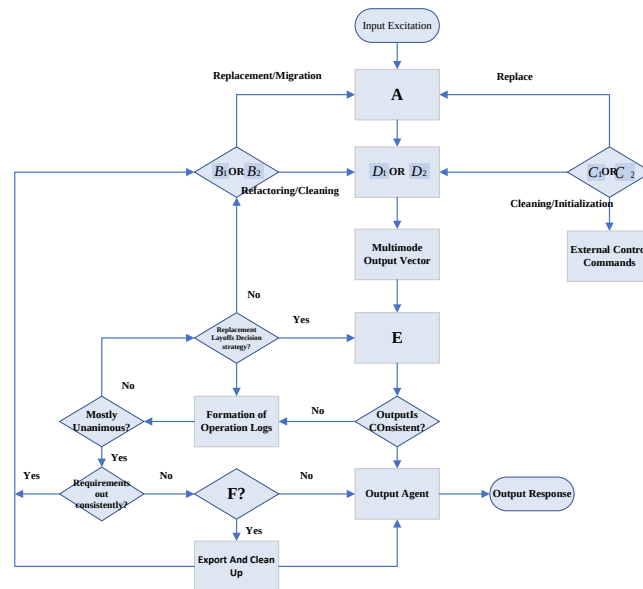


Figure 4. The basic process of MD.

3.1. Relative Correctness Axioms and Attack Chains

In human social activities, we often rely on the axiom that “everyone possesses certain shortcomings, yet it is exceptionally rare for the majority of individuals to commit precisely the same error in the same location and simultaneously when independently completing a shared task”. This concept, referred to as the “relative correctness axiom” in the literature [15], is depicted in its corresponding logical framework shown in Figure 5:

A_1 to A_i represent a population capable of independently completing task a . They can be logically understood as functionally equivalent heterogeneous redundancy relationships among them. When task a is simultaneously assigned to A_1 to A_i , it results in the outputs F_1 to F_i , where a significant number of voters select any output F_k with consensus properties.

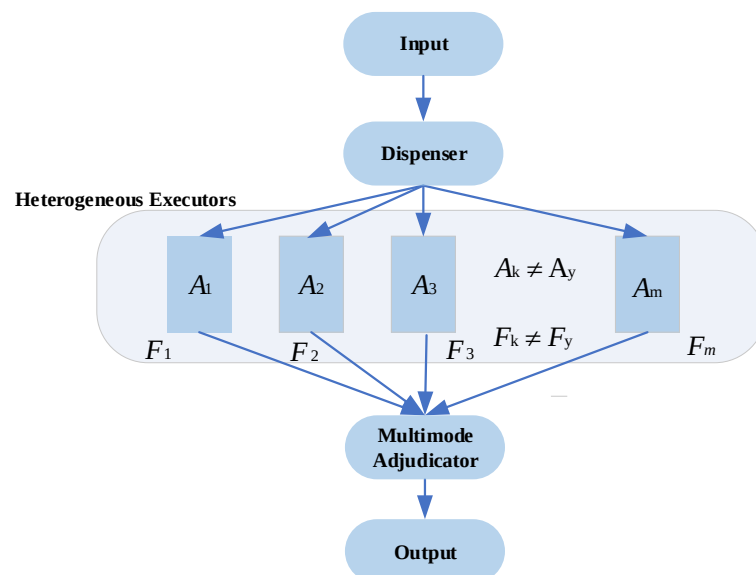


Figure 5. The corresponding logical construction.

Conducting a network attack typically involves several stages, including system scanning and detection, feature recognition, mapping and correlation, air coordination, vulnerability mining, attack execution, attack impact assessment, and information acquisition and dissemination. These stages are interconnected to form what is known as the

attack chain. Each link in this chain is intricately connected to the implementation structure, resource allocation, and operational mechanism of the target object. Given the disparate nature of two completely heterogeneous executives, their attack chains are likely to be fundamentally different. Therefore, attackers often exploit the static, deterministic, and homogeneous nature of the target object's operational environment in each step of the attack to ensure effectiveness and stability. However, introducing mimic camouflage or stealthy deception based on endogenous security mechanisms while maintaining the target object's performance, can create a cognitive dilemma for the attacker, ultimately disrupting the stability of the attack chain.

Building upon this concept and leveraging the axiom of relative correctness, the construct of "dynamic heterogeneous redundancy" was proposed in [14].

3.2. The Structure of Heterogeneous Actuators

The implementation policy of mimic defense is as follows: utilizing the DHR architecture to provide system service functions, thereby diversifying, randomizing, and dynamically mapping the structure and service functions of the target object. This creates cognitive dilemmas for attackers regarding the vulnerabilities, backdoors, and defense environments of the target system. The DHR's endogenous fusion of defense effects and the trinity of realization function characteristics make it the foundation for realizing the structure of target object service functions. Mimic ruling-based scheduling strategies and dynamic reconstruction, along with a negative feedback mechanism, aim to create non-cooperative conditions and ensure dynamic multi-objective synergistic attacks, with the ultimate goal of minimizing the probability of escape.

The DHR structure, illustrated in Figure 6, utilizes a collection of online executables as its runtime space (margin refers to the number of executables working in parallel). These executables, denoted as E_1 , E_2 , and E_3 , possess equivalent service functionality but differ in their compositional building blocks, such as hardware platforms, operating systems, runtime environments, and service programs. Input agents transparently replicate and distribute external requests, while output agents compare and validate the multiplexed results and return responses, forming the mimic guard boundaries (within left and right parentheses). Within these boundaries, E_1 , E_2 , and E_3 exhibit different vulnerabilities and backdoors due to their heterogeneous nature.

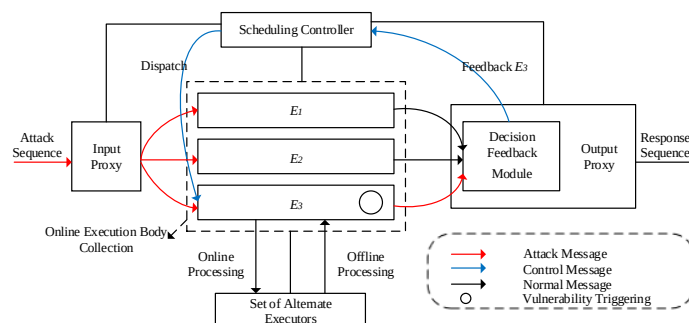


Figure 6. The DHR structure.

During an attack, as indicated by the red line in the figure, an x-attack message based on vulnerability, while valid for E_3 , will overlook vulnerabilities in the multiplexed results processed by the heterogeneous set of executables, leading to inconsistent outputs for E_1 and E_2 . When the adjudication feedback module of the output agent compares the results, it detects inconsistencies and generates an adjudication exception. Furthermore, the anomaly information from E_3 is reported back to the scheduling controller, serving as a basis for replacing and processing the corresponding executables in the online collection, thus implementing a targeted structural transformation [16].

3.3. Scheduling Algorithms for Heterogeneous Executables

Typical scheduling strategies span across various areas, including the SDN control layer, web servers, mimic switches, DNS servers, and other domains. The problems under investigation encompass three categories: scheduling timing, scheduling quantity, and scheduling objects. The system characteristics under consideration include three aspects: dynamics, negative feedback, and heterogeneous redundancy characteristics. In investigating the switching time problem of scheduling executives, the literature [16] introduced a scheduling sequence control method based on the sliding window model. This method dynamically adjusts the timing and size parameters of the scheduling window according to different attack scenarios, enhancing the security and robustness of the system. Another dynamic scheduling algorithm, proposed in the literature [17], utilizes temporal random thresholds for individual heterogeneous actuators, rendering the overall architecture dynamic. The optimal scheduling algorithm proposed in the literature [18] calculates the optimal scheduling time based on the scheduling cost, attack loss, and attack distribution function, which solves the problem of timing selection during scheduling to some extent.

In the problem of the number of working executives, the literature [19] proposes a feedback-based dynamic sensing scheduling algorithm, which decides the number of working executives in the next cycle according to the number of controller failures that the system can tolerate. This algorithm has some dynamics, but the complexity is high. The literature [20] proposes a utility-based dynamic elastic scheduling strategy, which determines the number of online executables in the next step according to the current external environment and has better dynamics.

The literature [21] proposes a scheduling quantity algorithm based on judgment feedback, which determines the number of online executables at the next moment based on the judgment feedback results. This algorithm considers the system load and increases the system dynamics and reliability while weighing the system cost and security, but it lacks the specific change conditions and research of follow-up work.

The longest dissimilarity distance component selection algorithm and software component selection algorithm with optimal average dissimilarity distance proposed in the literature [22] mainly discuss the dissimilarity from the spatial dimension to solve the problem of selecting software components in fault-tolerant design. The maximum dissimilarity system selection algorithm proposed in the literature [6] only gives common vulnerability indicators from the time dimension and does not consider vulnerability accumulation in the spatial dimension, and it also only selects the dissimilarity set with the largest executor, which is less dynamic. The literature [23] utilizes complexity and variability to describe heterogeneity metrics from the spatial dimension, and its scheduling algorithm is more stable but less dynamic. The literature [24] proposes the common vulnerability indicator (CVI, common vulnerability indicator) to quantify system similarity, and its indicator only considers similarity from the temporal dimension and lacks spatial dimension characteristics. The literature [25] proposes a heterogeneous functional equivalent scheduling model to measure the similarity from the spatial dimension and accordingly proposes the random seed and minimum similarity (RSMS, random seed and minimum similarity) method, which takes into account the dynamics and reliability of the algorithm.

4. Application of Mimic Defense

4.1. Ecological Development of Anthropomorphic Products

Mimic product development integrates wafer-scale micro-packaging technology and incorporates endogenous security design specifications, along with other advanced methods, into information systems, hardware and software components, control systems, and other common objects. These are used for research and development in mimic product environments with the ultimate goal of achieving a new generation of information systems with endogenous security as a fundamental feature [9]. Currently, representative products such as mimic routers [26] and anthropomorphic web servers [27] have been successfully developed, demonstrating the progress in this field.

4.1.1. Mimic Routers

The mimic router is a concrete practice of the mimic defense idea in the field of routers, which is realized in the architecture shown in Figure 7.

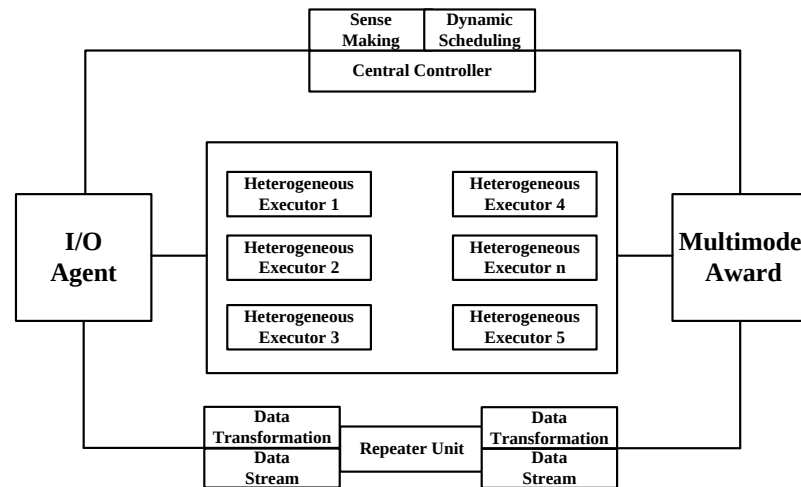


Figure 7. The mimic router construction.

The system consists of several components, including input/output agents, a central controller, a forwarding unit, multimode adjudication, and an executor pool. The central controller comprises sensing decision and dynamic scheduling modules, while the forwarding unit includes data transformation and data flow fingerprinting modules. The actuator pool consists of seven functionally equivalent heterogeneous actuators, which are scheduled online and offline by the central controller. The online executives can be categorized into two types: workers and inspectors. The worker is responsible for the external presentation of the entire router, with only one being active at any given time. The inspector supports multimodal adjudication, and the number of inspectors is determined by the system's preconfiguration and the size of the executor pool, typically comprising an even number of actuators. Mimic defense technology is configured through three aspects: data forwarding, router control, and management configuration, aiming to create a redundant, heterogeneous, and dynamic security defense system. Additionally, it supports typical parallel execution and voting output for OSPF and BGP [28].

4.1.2. Mimic Web Server

The mimic web server incorporates the concept of mimic defense into web servers by utilizing multi-level mimic deployment to disrupt attack chains at multiple points, thus ensuring the security and stability of web services. Its key components include multi-level mimic heterogeneous executables, dynamic control modules, and mimic voters. The multi-level mimic heterogeneous executables of the mimic defense web server are primarily implemented at various layers, including the file layer, SQL script layer, server software layer, virtual machine operating system layer, and physical machine operating system layer, as depicted in Figure 8. At each layer, the mimic defense web server is composed of multiple heterogeneous executables, which achieve heterogeneity primarily through the reconfiguration of the server software stack and intentional diversity of data [29]. This multi-level heterogeneity complicates attackers' attempts to intercept information during the attack preparation phase and makes maintaining the stability of the attack chain more challenging, thereby significantly increasing the difficulty of attacks.

The dynamic control module oversees and manages the system as a whole, and it is primarily responsible for policy rotation and executor orchestration. The mimic web server incorporates two voters: the front-end voter evaluates user requests at the semantic level, while the back-end voter assesses the return data at the data level.

By effectively integrating mimic defense with web server functionality, the mimic web server significantly enhances server security and service resilience, albeit with a slight increase in latency costs.

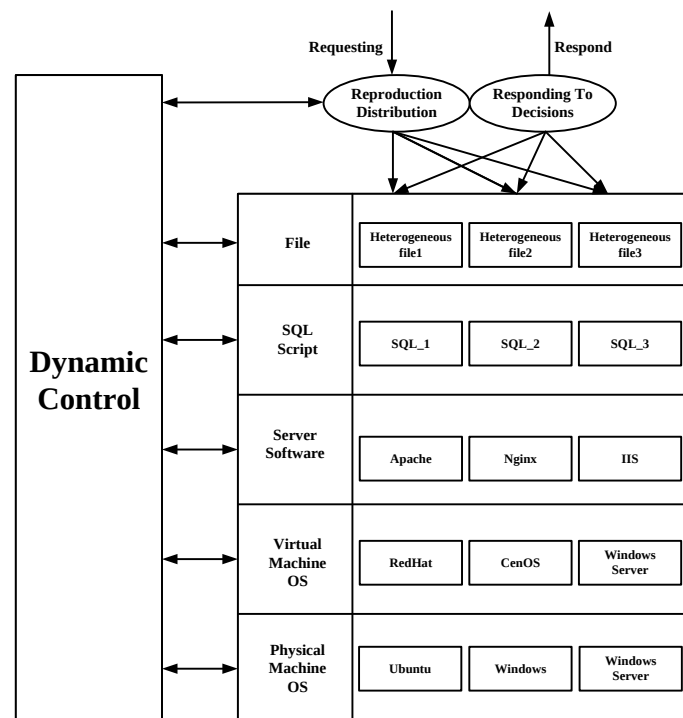


Figure 8. The architecture of the mimic web server.

4.2. Communication Techniques Based on Mimic Defense

The advancement of mimic defense technology in the communication field enables the cross-domain development of high-speed heterogeneous networks. Additionally, mimic technology offers new solutions to the security challenges faced by contemporary mobile platforms, such as cloud and mobile edge computing.

In contrast to 5G, the vision for 6G necessitates enhanced security performance and efficiency. Concerning security performance, there is a need to propose a quantifiable design and evaluate the metrics system. For security efficiency, it is crucial to simultaneously consider the inherent attributes of communication, service, and security to foster balanced development of the overall key performance indicators (KPIs) of 6G. This balanced development should promote synergy among these elements, realizing the “trinity” of communication, security, and service within an endogenous “root system” integration framework.

While 6G security encounters dual uncertainty and two opposing contradictions, it is evident that most of the security threats in the 6G network will stem from the endogenous security issues resulting from its inherent defects. These opposing contradictions arise from the failure to recognize and leverage the common inherent attributes of communication, security, and service. Often, traditional plug-in or add-on security solutions remain segregated from communication and service components. Following the philosophical principle that external factors act through internal factors and that internal factors play a decisive role, it becomes imperative to innovate security concepts and architectures and catalyze security technologies with “intergenerational effects” [30].

4.3. Mimic Cloud Services

The rapid growth of cloud services inevitably leads to an increase in the prominence of security issues facing these services. Similar to other fields, the primary threats to cloud security are unknown vulnerabilities and backdoors. This is primarily due to the

fact that cloud services are built upon existing technologies, leading to the transfer of vulnerabilities and backdoors from these existing technologies to the cloud service platform. The mimic cloud service (MCS) addresses these challenges by combining mimic defense and cloud service methodologies, thereby reducing the likelihood of continuous exposure to vulnerabilities [9].

MCS is an application of mimic defense in cyberspace, as depicted in Figure 9. The MCS architecture comprises four main components: the scheduling set, execution pool, service agent, and controller.

The scheduling set functions as a collection entity of multiple functionally equivalent heterogeneous executors, referred to as virtual nodes. The execution pool serves as the functional execution unit of MCS, with virtual nodes within the pool being mapped to corresponding nodes in the scheduling set. This logical mapping unit allows for different combinations of nodes to map to different execution pools.

The service agent is responsible for receiving and distributing user requests to the execution pool as well as performing multimodal adjudication on the returned responses.

Finally, the controller configures distribution and adjudication policies to direct the service agent's work while also managing the mapping relationship between execution pools and scheduling sets through scheduling policies [31].

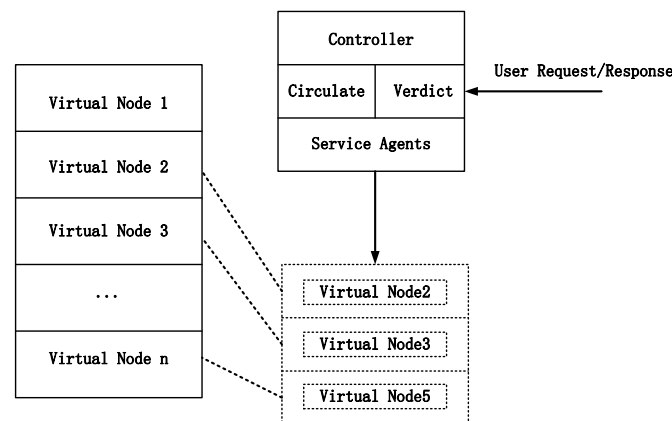


Figure 9. The architecture of mimic cloud services.

4.4. Mimic Blockchain

The blockchain domain faces various security challenges, including key loss, contract code vulnerabilities, and private mining, all of which can be addressed using mimic defense techniques [9]. Currently, most blockchains can be viewed as static isomorphic redundant systems, where each node stores the same data using the same algorithm. This redundancy ensures that the system can continue to function even if a single node is compromised. However, if critical components such as signature algorithms and consensus algorithms are targeted in an attack, the entire system remains vulnerable.

As early as 2019, a team from the People's Liberation Army Strategic Support Force Information Engineering University introduced the concept of the mimic blockchain, combining blockchain technology with mimic defense strategies [32]. To address potential security threats in blockchain systems, the team employed a dynamic heterogeneous redundancy architecture and cryptographic lottery principles. They proposed a security solution that reimagines blockchain consensus mechanisms and signature algorithms through a mimic lens. Through comprehensive security analysis and performance evaluations, the team demonstrated that the dynamic heterogeneous redundancy blockchain offers superior security compared with traditional blockchain architectures in several key aspects [9].

5. Challenges and Prospects

Cyberspace mimic defense, as a solution for uncertain threats such as unknown vulnerabilities and backdoors, has been extensively researched. Its core mechanism, the dynamic

heterogeneity redundancy (DHR) structure, is characterized by three attributes: heterogeneity, redundancy, and dynamics. These attributes make it challenging for threats to be successfully exploited, thereby realizing endogenous security within the information system's structure. This approach breaks through the limitations of traditional security defense, which focuses on network and system boundaries and can complement traditional network security technologies, with heterogeneity and redundancy being the most important aspects.

Heterogeneity primarily involves the diversity of system hardware and software. Greater disparities between hardware and software result in lower similarity, reducing the likelihood of symbiotic vulnerabilities and minimizing the impact of the same attack. However, challenges in realizing the DHR architecture are gradually emerging. These challenges include finding sufficient suitable heterogeneous executables to satisfy redundancy, balancing redundancy with system operation and maintenance costs, studying parallel processing of information in mimic executable constructs, and constructing high-capacity mimic executable constructs.

Areas requiring further research include scientifically proving and conceptually abstracting mimic construction, operation mechanisms, and effectiveness; formalizing the description of vulnerability exploitation mechanisms in a mimic environment and demonstrating the impact of a mimic system on an attacker's ability to exploit these vulnerabilities across domains; policy scheduling based on mimic verdicts and multi-dimensional dynamic reconfiguration of negative feedback mechanisms on the target system; and evaluating the inhibitory effect of mimic systems on the target system's "homologous" dark function. Additionally, there are still some limitations in the current research on endogenous security. For instance, when dealing with a global network adversary capable of monitoring the entire traffic exchanged by the network nodes, the literature [33] presents a privacy-preserving proximity-based solution that provides both symmetric and asymmetric proximity testing entirely within social networks. The literature [34] presents Loopix, a low-latency anonymous communication system that offers bidirectional "third-party" sender and receiver anonymity and unobservability. The literature [35] demonstrates that Tarzan imposes minimal overhead over a corresponding non-anonymous overlay route. In addressing the adversary in the local network, the literature [36] conducts a comprehensive and empirical measurement study to reveal insights into local communication within a smart home deployment and its threats. Moreover, in addressing the adaptive adversary, the literature [37] proposes AdaWFPA, an adaptive online website fingerprinting attack based on adaptive stream mining algorithms. However, the DHR architecture utilized in endogenous security aims to address issues such as message integrity and third-party malicious intrusions during transmission that traditional MTD architectures cannot resolve. As a means of network link defense, DHR cannot currently guarantee the confidentiality of content during information transmission. Therefore, how to integrate encryption techniques into specific implementations of the architecture is a direction worthy of further research in endogenous security. Additionally, there is a need for scientific descriptions of uncertainty within the mimic architecture.

It is evident that the development of mimic defense requires continued promotion of theoretical research and technical innovation.

Author Contributions: Conceptualization, X.L. and C.L.; investigation, X.L. and H.W.; writing—original draft preparation, X.L.; writing—review and editing, C.L. and H.W.; supervision, C.L., X.L. and H.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key Technologies Research and Development Program (2020YFB1712401), the Key Special Technologies Research and Development Program in Henan Province (231111211900), the project of Henan Provincial Science and Technology Research Project (242102221017, 232102210090), Key Scientific Research Project of Colleges and Universities in Henan Province (23A520015), the Key Scientific and Technology Project in Henan Province of China (221100210100, 221100211200-02), the Project of Joint Graduate-student Education Base in Henan Province (YJS2023JD04).

Data Availability Statement: Not applicable.

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

References

1. H3C. Cybersecurity Vulnerability Landscape Report 2023. Report, 2023. [2024-02-29]. Available online: <https://download.h3c.com/app/cn/download.do?id=10684557> (accessed on 9 April 2024).
2. Wang, X.; Gui, C. Cybersecurity Vulnerability Landscape Observations for the First Half of 2022. Report, 2022. [2022-09]. Available online: <http://www.itsec.gov.cn/zxxw/202209/P020220902118368141314.pdf> (accessed on 9 April 2024).
3. Goncalves, M. *Firewall Technical Guide*; Machinery Industry Press: New York, NY, USA, 2000.
4. Tang, Z. *Introduction to Intrusion Detection Technology*; Tsinghua University Publishing House: Beijing, China, 2004.
5. Hong, H.; Zhang, Y.; Hu, Y.; Dai, Z. Research on Technology of Network Security Scan. *Comput. Eng.* **2004**, *30*, 3. [CrossRef]
6. Jajodia, S.; Liu, P.; Swarup, V.; Wang, C. *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 100. [CrossRef]
7. Cai, G.; Wang, B.; Wang, T.; Luo, Y.; Wang, X.; Cui, X. Research Progress on Mobile Target Defense Technology. *Comput. Res. Dev.* **2016**, *53*, 20. [CrossRef]
8. Wu, J. Cyberspace Endogenous Safety and Security. *Engineering* **2022**, *15*, 179–185. [CrossRef]
9. Hang, J.; Wu, Y.; Hu, X. New Equilibrium of Network Security—Review of Mimicry Defense Principles. *Ind. Inf. Secur.* **2022**, *5*, 25–34.
10. Wu, J. Endogenous Security Issues and Countermeasures for Intelligent Networked Vehicles. *J. Chongqing Univ. Posts Telecommun. Nat. Sci. Ed.* **2023**, *35*, 383–390. [CrossRef]
11. Wu, J. Endogenous security development paradigm in cyberspace. *Chin. Sci. Inf. Sci.* **2022**, *52*, 189–204. [CrossRef]
12. Ji, X.; Wu, J.; Jin, L.; Huang, K.; Chen, Y.; Sun, X.; You, W.; Huo, S.; Yang, J. Discussion on a new paradigm of endogenous security towards 6G networks. *Front. Inform. Technol. Electron. Eng.* **2022**, *23*, 1421–1450. [CrossRef]
13. Zhou, Z.; Kuang, X.; Sun, L.; Zhong, L.; Xu, C. Endogenous Security Defense against Deductive Attack: When Artificial Intelligence Meets Active Defense for Online Service. *IEEE Commun. Mag.* **2020**, *58*, 58–64. [CrossRef]
14. Wu, J. Research on Mimetic Defense in Cyberspace. *J. Inf. Secur.* **2016**, *1*, 1–10. [CrossRef]
15. Wu, J. *Introduction to Mimetic Defense in Cyberspace*; Science Press: Beijing, China, 2017.
16. Wei, G. Research on Mimic Architecture and Key Technologies of Distributed Storage System. Ph.D. Thesis, Information Engineering University, Zhengzhou, China, 2020. [CrossRef]
17. Sang, X. Computer Engineering and Design. Bachelor's Thesis, Nanjing University of Science and Technology, Nanjing, China, 2022. [CrossRef]
18. Lu, Z. Research on Proactive Defense of SDN Controller. Master's Thesis, Information Engineering University, Zhengzhou, China, 2019.
19. Qi, C.; Wu, J.; Hu, H.; Cheng, G. Dynamic-scheduling mechanism of controllers based on security policy in software-defined network. *Electron. Lett.* **2016**, *52*, 1918–1920. [CrossRef]
20. Li, J. Research on Key Technologies of Mimic Defense in Software-Defined Network. Ph.D. Thesis, Information Engineering University, Zhengzhou, China, 2019.
21. Gao, M.; Luo, J.; Zhou, H.; Jiao, H.; Ying, L. A Differentiated Feedback Scheduling Judgment Algorithm Based on Mimetic Defense. *Telecommun. Sci.* **2020**, *36*, 72–83.
22. Yao, W.; Yang, X. Design of selective algorithm for diverse software components. *J. Harbin Inst. Technol.* **2003**, *35*, 261–264. [CrossRef]
23. Zhang, J.; Pang, J.; Nie, G.; Tai, M.; Zhang, Z.; Zhang, H. Executors Scheduling Algorithm for Web Server with Mimic Structure. *Comput. Eng.* **2019**, *45*, 8. [CrossRef]
24. Garcia, M.; Bessani, A.; Gashi, I.; Neves, N.; Obelheiro, R. Analysis of operating system diversity for intrusion tolerance. *Softw. Pract. Exp.* **2014**, *44*, 735–770. [CrossRef]
25. Liu, Q.; Lin, S.; Gu, Z. Heterogeneous redundancies scheduling algorithm for mimic security defense. *J. Commun.* **2018**, *39*, 188–198. [CrossRef]
26. Jin, X.; Ge, Q.; Zhang, J.; Ding, J.; Jiang, Y.; Ma, H.; Yi, P. Design, Implementation and Formal Verification of TCP Proxy in Mimic Defense Router. *J. Inf. Secur.* **2023**, *8*, 1–13. [CrossRef]
27. Ma, H.; Wang, L.; Hu, T.; Jiang, Y.; Qu, Y. Survey on the development of mimic defense in cyberspace: From mimic concept to “mimic+” ecology. *Chin. J. Netw. Inf. Secur.* **2022**, *8*, 15–38. [CrossRef]
28. Ma, H.; Jiang, Y.; Bai, B.; Zhang, J. Tests and Analyses for Mimic Defense Ability of Routers. *J. Cyber Secur.* **2017**, *2*, 43–53. [CrossRef]
29. Tong, Q.; Zhang, Z.; Wu, J. The Active Defense Technology Based on the Software/Hardware Diversity. *J. Cyber Secur.* **2017**, *2*, 1–12. [CrossRef]
30. Jin, L.; Lou, Y.; Sun, X.; Zhong, Z.; Xu, X.; Yi, M.; Huang, K.; Ji, X.; Wu, J. Concept and vision of 6G wireless endogenous safety and security. *Sci. Sin. Informationis* **2023**, *53*, 21. [CrossRef]

31. Pu, L. Research on the Key Technologies of Mimetic Cloud Service Architecture. Ph.D. Thesis, Information Engineering University, Zhengzhou, China, 2022. [\[CrossRef\]](#)
32. Xu, M.; Yuan, C.; Wang, Y.; Fu, J.; Li, B. Mimetic Blockchain—Blockchain Security Solutions. *Softw. J.* **2019**, *30*, 1681–1691. [\[CrossRef\]](#)
33. Buccafurri, F.; De Angelis, V.; Idone, M.F.; Labrini, C. A protocol for anonymous short communications in social networks and its application to proximity-based services. *Online Soc. Netw. Media* **2022**, *31*, 2468–6964. [\[CrossRef\]](#)
34. Piotrowska, A.M.; Hayes, J.; Elahi, T.; Meiser, S.; Danezis, G. The loopix anonymity system. In Proceedings of the 26th USENIX Conference on Security Symposium, Vancouver, BC, Canada, 16–18 August 2017; pp. 1199–1216.
35. Freedman, M.J.; Morris, R. Tarzan: A peer-to-peer anonymizing network layer. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 193–206. [\[CrossRef\]](#)
36. Girish, A.; Hu, T.; Prakash, V.; Dubois, D.J.; Matic, S.; Huang, D.Y.; Egelman, S.; Reardon, J.; Tapiador, J.; Choffnes, D.; et al. In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes. In Proceedings of the 2023 ACM on Internet Measurement Conference, Montreal, QC, Canada, 24–26 October 2023; pp. 437–456. [\[CrossRef\]](#)
37. Attarian, R.; Abdi, L.; Hashemi, S. AdaWSPA: Adaptive Online Website Fingerprinting Attack for Tor Anonymous Network: A Stream-wise Paradigm. *Comput. Commun.* **2019**, *148*, 74–85. [\[CrossRef\]](#)

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.