Cyber Mimic Defense

Subjects: Transportation Science & Technology

Contributor: HandWiki Huang

From the inspiration of defensive guise behaviors based on mimic phenomenon in biology, Cyber Mimic Defense (CMD) introduces the mechanism of dynamic multi-dimensional reconfiguration into a dissimilar redundancy structure (DRS) which is widely used in the field of reliability. It addresses certain or uncertain threats in cyberspace by the principle of uncertain defense, and provides the strategic varieties and transformations of DRS elements inside objects in quantity or type, time or space dimension under the condition of unchanged visual functions. It provides a generally innovative defense theory and method to deal with the “known unknown risk” and “unknown unknown risk” which exist in related application levels of different areas of cyberspace and are based on unknown vulnerabilities, backdoors, viruses, Trojans, etc. This method can provide not only endogenous security gains which are independent of traditional security means and achieved via integrated structural technologies for critical infrastructures or key information equipment, but also resilient or restorable service ability with intensive attributes inherited from the architecture. Further it acquires super nonlinear effects combining mature defense technologies. It's aimed at creating a non-closed, self-controlled and sustainable-developed ecological environment which adapts to globalization technologies and industrial development models and integrates with win-win cooperation and open sources.

Keywords: dissimilar redundancy ; nonlinear effects ; ecological environment

1. Background

In the current cyberspace, there are "unknown unknown threats", namely uncertain threats. Usually, such threats are originated from human attacks, based on existing unknown design bugs referred as vulnerabilities in hardware and software of information systems, or induced from backdoor attacks, based on mounting malicious codes of software and hardware in the era of globalization which cannot ensure the credibility of the industry chain. Based on the existing scientific level and cognitive ability of human beings, it's impossible to make a scientific judgment neither from the theory nor from the practice that complex information systems have no vulnerabilities and backdoors. Moreover, it's impossible to completely avoid design bugs or backdoors in the engineering level. So it's a consensus in the field of security that the biggest threat in cyberspace comes from unknown vulnerabilities, backdoors, viruses or Trojans, etc.

The existing defense system is the concept of precise defense based on perceptual cognition, which requires a certain amount of clear and reliable prior knowledge as the support, such as sources, characteristics, processes and behavior of attack, working in the precondition of “known risks” or “known unknown risks”. So it's an acquired defense system with the "bottom line defense", often supported by encryption or authentication. It is a common fragility in the system and mechanism of defense against unknown vulnerabilities, backdoors, viruses or Trojans, etc. Especially in the ecological environment of system hardware and software components whose credibility cannot be ensured, main defense means based on it almost have no effective real-time defense capability in the face of uncertain threats except for repairing after damages have been done (“mending the fold after the sheep have been stolen”) without the security guarantee of steps in encryption and authentication or other defensive functions, which can bypass or make short circuits deliberately.

Additionally, existing information systems have static structures, similar functions, and certain operating mechanisms. These features can't provide attackers with the facilitation such as objective identification, defense behavior detection, attack techniques testing and refining, combat effectiveness evaluation and so on. Meanwhile, most of the information systems inherit the operating mechanisms of single processing space and resources sharing, so that invaders can achieve the desired operation through the operating mechanisms of resources sharing when they enter this space. This is also one of the important basic conditions in many network attack theories, including “the side channel attack” which is used to break through the “physical isolation network” nowadays. As a result, the largest black hole of cyber security consists of determinacy in the information system architecture and mechanism, fragility in passive defensive system, deficiency in active immune mechanisms and other key issues.

2. Basic Concepts

2.1. Foundation of the Axioms

> Axiom 1：“There are many algorithms to reach the goal under the condition of given functions and performance.”

These diversified heterogeneous algorithms are equivalent under the condition of given functions and performance. If it can be proven that union or intersection calculation results of feasible methods can still meet requirements of equivalent functions, no matter what scheduling strategies or dynamic combination of these heterogeneous algorithms are done, it will not change the given functions. Accordingly, the mapping relationship between the visual functions and the structure of the object is no longer unique or certain from the perspective of attackers, which can be used to achieve the active defense by the defenders.

> Axiom 2：“Everyone has diverse shortcomings while they rarely make the same mistakes on the same tasks in the same place at the same time.”

This axiom provides a theoretical basis for applications of multi-mode ruling mechanisms of the heterogeneous redundancy architecture in fault tolerance, handling random failures of hardware and software in the field of reliability. This means that cyber problems based on unknown vulnerabilities, backdoors, Trojans, viruses and certain or uncertain threats can be transformed into risk protection problems through heterogeneous and redundant mechanism defense. Unless the attackers have resources and capabilities to achieve the consistent error expression through a cooperative attack dilemma under the condition of non-cooperation in heterogeneous multi-target space, it is difficult for attackers to escape from the multi-mode arbitral mechanism.

2.2. Implementation Architecture

Dynamic Heterogeneous Redundancy Architecture，DHR

2.3. Operating Mechanism

Through the multi-mode policy ruling and multi-dimensional dynamic reconfiguration mechanism under the condition of “de-cooperation”, difficult and costly engineering problems of the attack surface of complex systems can be turned into reduced problems of the attack surface of soft and hard parts, which is space-independent, function-simple and within mimic bracket. Moreover, it's able to minimize the dominant or recessive correlation among heterogeneous redundant entities, which causes the heterogeneous multi-target dynamic cooperative attack dilemma for attackers under the condition of non-cooperation. This reduces the engineering difficulty to implement “self-control, secure and trustable” strategy in cyberspace from “no security short board of the whole chain” to the guarantee of the absolute security of individual procedures or key components.

2.4. Security Concept

With the idea of the Moving Attack Surface, (MAS), the CMD system can be regarded as a kind of proactive defense system which deploys the multi-dimensional attack surface in an unpredictable way under the condition of visually-unchanged functions. Due to multiple-heterogeneity of structures and environments from each executive entity, it enables resources exploited by attackers (including lurkers) to have uncertainty in temporal and spatial dimensions. At the macro level, it appears that the attack surface is always making irregular movements. Especially for those attack missions which need multiple steps to transmit data to achieve attack goals, the premise of achievability can hardly be guaranteed.

2.5. Security Gain

Mimic defense gains (MDG) purely acquire nonlinear security gains through endogenous mechanisms of the framework. MDG in the mimic defense framework is endogenous. In mechanisms, there is no dependence on existing security defense technologies, such as encryption authentication, firewall filtering, virus detection, intrusion detection (Trojan removal), prevention, isolation and removal measures while traditional incremental means (vulnerability patching, backdoor blocking or malicious code removal, etc.) can be seen as supplementary measures to stabilize the defense effect. Besides, it has no real-time requirements for above technologies. However, the heterogeneous property of the Mimic system can be significantly enhanced with combination of these traditional security technologies, and results in improving the defensive capability of the object in a super nonlinear way.

3. Technical Route

CMD has the following features. It integrates a variety of proactive defense elements technically as the concept. And the similarity and singularity of the target system are altered via heterogeneity and diversity while the static state and certainty of the target system are transformed through dynamic and stochastic means. Also it identifies and shields unknown defects and threats based on heterogeneous, redundant and multi-mode ruling mechanisms. Further, it enhances the flexibility or elasticity of the service function of the target system via high reliable architecture. Simultaneously, it defends or denies an uncertain threat to the target system depending on systems' uncertain attributes. The above objectives can be achieved by a DHR-based and integrated technological framework.

4. Mimic Defense Boundary

MDB (also abbreviated as Mimic Boundary) contains a number of service (operation) functions with normative definitions and strict agreements. Through consistency or conformance tests of these standardized protocols or specifications, we can determine the equivalence of multiple heterogeneous executive entities (complexity-unlimited) on given service (operation) functions or even performance. That is to say, the equivalence between functional executive entities, including the consistency of given exception handling functions or performance, can be judged via the consistency tests of the relationship between input and output through MDB. And the integrity, effectiveness and security of functions defined by MDB are a prerequisite for effective mimic defense, while functions (operations) not defined by MDB explicitly don't belong to the scope of mimic defense (but there may exist a derived protective effect). In other words, if attackers do not make the output vectors inconsistent on the Mimic Boundary, the mimic mechanism won't react. Therefore, it is essentially important to set, divide and choose MDB reasonably in engineering implementation. Specifically, security issues beyond MDB don't belong to the scope of mimic defense. For example, security threats are caused by means which are independent of unknown vulnerabilities, backdoors or other factors within MDB, like fishing, bundling malicious functions in service software, pushing virus codes in cross-platform interpreted executive files and carrying toxic software through downloading behaviors from users.

4.1. Mimic Escape, ME

Mimic Escape refers to the process in which attackers make the heterogeneous redundant entities in MDB produce identical or mostly identical errors, thus breaking through the multi-mode arbitral mechanism and achieving the attack. Mimic Escape is an uncertain problem whose performance is not stable because of the DHR mechanism, and cannot be expressed by probability. More generally, “there is no second chance for a successful attack.”

4.2. Mimic Presentation, MP

Mimic Presentation refers to the visual relationship between the external service functions observed by attackers and the implementation structures of the object. The more complicated, less certainty and more diverse the relationship is, the more unpredictable the defensive behavior and environment of the object will be. Accordingly, the creation and maintenance of an attack chain will be more difficult, and the possibility of planning or deploying the attack will be lower. When the number and types of the heterogeneous redundant entities are determined, the levels of Mimic Presentation are strongly correlated to the scheduling and generation strategies for the set of executive entities.

5. Mimic Defense Levels

5.1. Utter-Shielding Level

If the given MDB is facing an external invasion or “insider” attacks, protected functions, services and information are not affected and attackers can't make any assessment on attack effectiveness, as if they fall into an “information black hole”, which is called the utter shielding level, the highest level of mimic defense.

5.2. Non-Sustainable Level

If the given MDB is facing an external invasion or “insider” attacks, protected functions or information may make corrections after error-making or be self-healing with uncertain probability or duration. For attackers, even if they make a breakthrough, they hardly maintain attacks' effects or can't provide any meaningful basis for subsequent attacks, which is called the non-sustainable level.

5.3. Hard-Reproducible Level

If the given MDB is facing an external invasion or “insider” attacks, protected functions or information may be out of control in a certain duration while it's hard to reproduce the same scene with repeating identical attacks. In other words, the attack scene or experience after a breakthrough can't be inherited and lacks in utilized value in time dimension, which is called the hard-reproduced level.

5.4. Principles of Grading

More defense levels can be defined to meet comprehensive demands for security and implementation cost in different application scenarios. Four factors have to be taken into account regarding the security. The core of mimic defense is different-degree uncertainty on attack actions. The non-perceptive trait makes it impossible for attackers to acquire effective information of the defender at all stages of the attack chain. The non-sustainable feature enables the attack chain to lose its utilized stability. And the non-reproducible character makes it difficult to exploit experience based on accumulative probes and attacks as priori knowledge in the following attack missions.

6. Applicable Field

Under the condition of the functional input-output relationship or meeting the IPO model, to solve the problem of service functions, performance and important information resources must be explicit and robust providing, insensitive to initial investment or product pricing, space or power consumption are acceptable and there are standard or standardized functional interfaces and protocol specifications and multiple or diverse processing conditions as well as occasions where the reliability and availability of the system or device are challenged by the traditional security and cyberspace non-traditional security. It should be pointed out that, under the above conditions, it is suitable to implement the mimic defense in any application where the target algorithm is determined and there are other equivalent algorithms. As the accuracy of results between different algorithms with function equivalence may be different (for example, the result is accurate to several decimal places.), or if the range of the control amount is a range, even if the problem is applied to a subject such as a scientific calculation or an application in an industrial control field, multi-mode decisions can also be made using a policy such as "precision mask" or "expected range".

7. Application Progress

Mimic Web Server[1]

Mimic Router[1]

Mimic File and Storage System

Mimic Industrial Control Processor

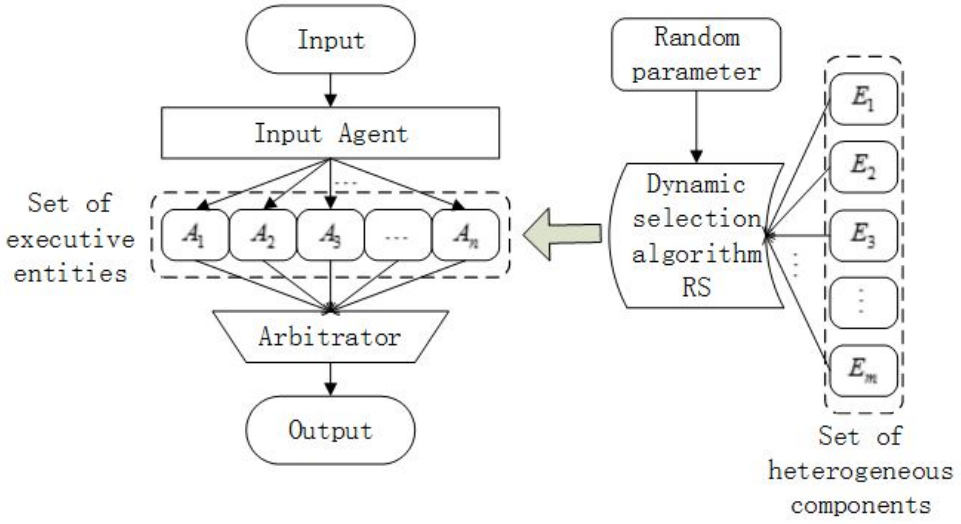
8. Mimic Phenomenon and Mimic Defense

The Mimic Phenomenon (MP) means that a creature simulates another creature or environment in color, texture, shape and other features so that one or both of the parties benefit from the ecological adaptation. From the perspective of the defender, it can be included in the category of active defense based on the endogenous mechanism, referred as Mimic Guise (MG). Besides the simulation in color, texture, shape and other features, we refer the simulation of behavior and state as Mimic Defense (MD). To be specific in cyberspace, under the premise of remaining unchanged in given functions and performance of an object, it can be transformed in space-time dimension strategically such as system architectures, operation processes, core algorithms, abnormal behavior and other environmental factors as well as unknown vulnerabilities, backdoors or Trojans, viruses which may exist in an attached mode . Accordingly, we refer this system and mechanism of defense as Cyber Mimic Defense (CMD).

9. Dynamic Heterogeneous Redundancy Architecture (DHR)

DHR is a theoretical method of achieving mimic defense. It's based on a dissimilar redundancy structure (DRS) in the field of reliability and introduces the mechanism of dynamically multi-dimensional reconfiguration, which enables it not only have high reliability of DRS but also high security of mimic defense. We refer this heterogeneous redundant structure as a dynamic heterogeneous redundancy (DHR) architecture.[2]

9.1. Composition and Operating Process of DHR



DHR architecture. https://handwiki.org/wiki/index.php?curid=1652569

The architecture of DHR is composed of the input agent, a set of heterogeneous components, dynamic selection algorithms, a set of executive entities and multi-mode arbitrators. In the diagram, the set of heterogeneous components and dynamic selection algorithms support the dynamic reconstruction in multi-dimension, which makes the set of executive entities dynamic. Multiple kinds of sets in which heterogeneous components are functionally equivalent can be combined by the software and hardware of standardization in module collection. The inputs are conveyed from the agent to n executive entities in set, represented as $A_1, A_2, \ldots, A_n$ selected from the collection E in Dynamic selection algorithm. Finally, system outputs are provided from the arbitrating between the output vectors through the multi-mode arbitrator.

9.2. Mimic Bracket

In the DHR architecture, system inputs are conveyed from the input agent to every executive entity in the current set, and system outputs are provided from the arbitrating between the output vectors through the multi-mode arbitrator. We refer both of the input agent and multi-mode arbitrator as the Mimic Bracket (MB).

9.3. Mimic Defense Boundary in DHR

Mimic Bracket, the combination of the input agent and multi-mode arbitrator, is operated in independent physical or logical space but coordinated functionally. The Mimic Defense Boundary (MDB), also abbreviated for Mimic Boundary, is defined by the Mimic Bracket as a range of protection. MDB is usually a heterogeneous redundant environment operated with “toxics and Bacteria”, which contains unknown vulnerabilities, backdoors and other bugs of hardware and software or viruses, Trojans, and malicious codes. In this environment, heterogeneous executive entities under the condition of a certain functional input sequence, can give a complete consistent output sequence essentially.

9.4. The Anti-Attack Feature of DHR

Firstly, the mechanisms of DHR can make the system show much uncertainty to the attacker within the controllable and cost acceptable range for the defender, which provides a powerful solution to security threats of the statically deterministic DRS. It can also force the inevitable human attack, different from the fault-error, into a risk control problem of minimum probability, which can normalize the threat of certainty or uncertainty into a reliability problem of stochastic failure according to the physical mechanism of DHR. Secondly, it is a big challenge to make precise cooperation between homogeneous redundant components according to the related researches. Hence the heterogeneous feature of DHR will make cooperation more difficult for attackers. Furthermore, dynamism and randomness can improve the uncertainty of multi-participatory actions with consistent or synergistic requirements. Last but not least, the multi-mode arbitrator significantly enhances the difficulty of cooperative attack under the condition of non-cooperation.

9.5. The Significance of DHR Construction

If the elements in the set of heterogeneous executive entities satisfying functional equivalence are scheduled in dynamic policies, or deploy the generalized dynamic technologies such as reconfiguration, recombination, reconstruction, redefinition, and virtualization themselves, we could simplify or weaken the harsh requirements of dissimilarity design accordingly in DRS. In the post-globalization era, this conclusion is of great engineering significance for the application of trustability-uncontrollable components, including open source software, hardware or middleware and so on, to build a safe and reliable system as well as to reduce the cost, in product life cycle over the open industrial chain and the supplying chain.

10. Mimic Computing and Mimic Defense

Mimic computing[3] can dynamically select the solution structure environment adaptively, according to different tasks, different time, different loads, different performance requirements, different resource conditions and parameters. Mimic computing can improve processing efficiency with the benefit of structure variable computing based on active cognition.

Mimic Defense fully mines the structure variable computing on the mechanism of endogenous anti-attack properties. As the external appearance is dynamic and random, the Mimic Computing system seems to be in active jumping or rapid migration irregularly in the vision of attackers in the time-space dimension among the diverse environments. It shows strongly dynamic, heterogeneous, random and other uncertain characteristics, disturbing the observation and the prediction, which will increase the difficulty and cost of constructing the attack chain based on vulnerability and backdoors.

In summary, mimic computing and mimic defense are based on a computing and processing architecture in essence, which is structure-variable under the condition of functionally equivalence. With the full use of structure variable computing, mimic computing can improve processing efficiency and mimic defense can provide the ability of active defense.

11. Differences from Moving Target Defense (MTD)

11.1. Different Technology Roadmaps

Mimic Defense is a kind of architectural technology derived from fault tolerance in the field of reliability. Its fundamental form evolved from static DRS served as fault tolerance to DHR applied in intrusion tolerance. However, MTD is inspired by the idea of Encryption and Scrambler, which typically makes the instruction, address, or data of systems dynamic, random and diverse in order to increase the level of efforts required to achieve a successful compromise.

11.2. Different Technical Systems

The technical implementation of Mimic Defense is based on DHR, which has the intensive property with functions, reliability and security trinity. It is not necessary to expose technical details of the functional equivalent components of heterogeneous redundant hardware and software. MTD is a purely defensive technique which belongs to the simple "stack" of the non-systematic discrete technique, and it is not transparent to the protective object.

11.3. Different Implementation Space

Mimic Defense emphasizes on the implementation of a DHR architecture, which is operated in independent physical or logical space and correlated weakly with the operating mechanism of shared resource. MTD depends on the operating mechanism of shared resources, usually coexisting in the same processing space with objects, which seriously affects the objective performance of services due to the cost of processing resources.

11.4. Different Implementation Approaches

In Mimic Defense, it is requested that the object has functionally equivalent implementation support from the diverse hardware and software components as redundant. That is, in the premise of not affecting the service performance, the way to improve the security is a trade of the software and hardware resources while MTD mainly uses software to realize dynamic changes, diversification and randomization in the case of certain resource, in exchange for security by consuming the resources of the objective system and reducing the performance of the services.

11.5. Different Degrees of Attack Difficulty

The classic method of Mimic Defense is intended to build the redundant working environment with multi-mode judging mechanisms, composed of multiple dynamic reconfigurable components in functionally equivalence. When the same input arrives at heterogeneous executive entities, the only consistent output is intuitively generated by the intersection of functions in these entities through the multi-mode judging process. Any attack based on the specific implementation of one entity, including the attacks to multiple entities simultaneously, is hard to bypass the mimic judging mechanism under the condition of non-cooperation and turns out to be a failure. So for the attackers, it is necessary to solve the problem including not only the accessibility of attack packets and the availability of vulnerabilities, but also to achieve the consistent error expression through the cooperative attack dilemma under the condition of non-cooperation in heterogeneous multi-target space. It can overcome the impact of so many uncertainties while MTD can not provide such degrees of difficulty for attackers.

11.6. Different Capabilities of Attack Tolerance

Based on the benefit from the DHR structure in functionally equivalence, Mimic Defense keeps the fault tolerance and intrusion tolerance property in MDB as long as consistent mistakes arise by falling from the majority of executive entities at the same time. MTD emphasizes the functional recovery after the compromise, which is called resilience and tenacity. Obviously, the protective effect of the former is much higher than that of the latter.

11.7. Different Defense Objects

Mimic Defense is effective not only in defending the external attacks based on unknown vulnerabilities, backdoors, front doors, trapdoors, etc., but also against the unknown viruses, Trojans and other penetration attacks. However, MTD only considers the impact of the unknown vulnerabilities.

11.8. Different Application Modes

Due to the differences between the two technical systems and implementation approaches, Mimic Defense can use both of open source products and COTS black-boxes whose credibility cannot be ensured, but MTD excessively depends on white-boxes on the contrary. So the former can avoid the most tremendous trouble from technology promotion, with more inclusiveness, openness and attractiveness, and turns out to have greater prospects for commercial promotion and researches.

12. Differences from Trustable Computing

12.1. Mimic Defense Doesn’t Belong to the Technology of Computational Complexity

Mimic defense can't distinguish between right and wrong from the results itself, which is computed or operated by components of hardware and software. It just refers to the situation of consistency, arbitrated between responsive outputs which are produced by heterogeneous redundant entities from the same input excitation, as a basis of recognition under the condition of functional equivalence. It is usually a big probability event that most of the expressions are consistent. This is considered as the law of identification with normal or abnormal states although it is easy to prove both in theory and practice that consistent error existing in most expressions is a minimal probability event. The key of breaking through the Mimic Defense system is the solution on how to obtain the consistent errors in most entities, achieving the escape stably, under the condition of non-cooperation and DHR environment at the same time. Trustable Computing, could be considered as a technique of encryption and belongs to the category of computational complexity technology which is not the same as Mimic defense in security principles.

12.2. Mimic Defense Doesn’t Have Credibility Problems of the Trusted Computing Base (TCB)

The Mimic defense ruling refers to the majority or minority of outputs judged by the arbitrator, by using the relativity results as identification rules without any absolutely credible outputs except the correctness of the arbitrator. However, the "absolute security" of the Trusted Computing Base（TPM or TCM）is the fundamental of Trusted Computing, and is still controversial because of the unsettled problem that "who guarantees the credibility of TCB".

12.3. Mimic Defense is Transparent to Components of Hardware and Software

For heterogeneous redundancy components of hardware and software which are functionally equivalent in MDB, Mimic Defense does not need to make any analysis or customization and has only to operate in accordance with the process of the "black box" to directly apply COTS-level products whose credibility cannot be ensured. It reduces the cost of the

engineering during the realization of defensive techniques. While the object of Trusted Computing must have a degree of transparency so that analysis and intervention are inevitable during the process of implementation (often facing the hard situation in which there are only program files of executable codes), which brings a big challenge to the engineering implementation.

12.4. Mimic Defense Architecture Have Integrated Functions

The Mimic defense architecture is intensive with functions. While providing active defense functions without priori knowledge, the system also gives service functions and the security function of high reliability. However, Trusted Computing only provides the security function and the function of fault detection in a certain level.

References

1. "现代快报多媒体数字报刊平台". http://dz.xdkb.net/html/2016-11/17/content_447329.htm.
2. Jiangxing, WU (2016). "Research on Cyber Mimic Defense". Journal of Cybersecurity. http://jcs.iie.ac.cn/ch/reader/create_pdf.aspx?file_no=20160401&flag=1&year_id=2016&quarter_id=4. Retrieved 2017-01-26.
3. "Meaning and Vision of Mimic Computing and Mimic Security Defense--《Telecommunications Science》2014年07期". http://en.cnki.com.cn/Article_en/CJFDTotal-DXKX201407002.htm.