SCIENCE CHINA
Information Sciences

• PERSPECTIVE •

May 2022, Vol. 65 156301:1–156301:3
https://doi.org/10.1007/s11432-021-3379-2

Development paradigms of cyberspace endogenous safety and security

Jiangxing WU

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, *China*

Received 19 August 2021/Revised 19 October 2021/Accepted 3 December 2021/Published online 3 March 2022

Citation Wu J X. Development paradigms of cyberspace endogenous safety and security. Sci China Inf Sci, 2022, 65(5): 156301, https://doi.org/10.1007/s11432-021-3379-2

Scientific interpretation of paradigm. The concept and theory of paradigm were first proposed by Thomas Kuhn, a famous American science philosopher, and were systematically described in his book "The Structure of Scientific Revolutions" [1] published in 1962. He pointed out that a paradigm is an essential theoretical system and framework in which the theories, rules, and laws can be applied and regarded as coordinates, reference systems, and basic modes for scientific research, the establishment of scientific systems, and the application of scientific thoughts. Paradigms often remain unchanged until they are unable to solve the newly arising problems.

World outlook and methodologies for the conventional cyberspace security. Although the cyberspace community has not reached the consensus on whether there ever existed development paradigms so far, the author still tries applying the concept, method, and standpoint of paradigm to interpret the important development stage experienced by existing security technologies in cyberspace. Here, we might also use Paradigms 1–3.

Paradigm 1. The functional security development paradigm based on redundant configuration and voting. Its thinking perspective is to solve the problem of physical or logical failures of cyberspace terminals, nodes, and network system software and hardware. Its theoretical basis is on the reliability and robust control theory based on statistics. Its methodology is to introduce or import repeatedly processed time and space redundancies in the form of active backup or load sharing and homogeneous or heterogeneous redundancy based on voting/arbitration at key paths, nodes, network architecture, and other levels. Its processing principle is based on reliability design in conformity with redundant architecture. Due to the ceaseless penetration of the digital, network, and intelligent technologies, purely random failure assumptions are no longer valid, and uncertain or "unknown unknown" man-made attacks have become a new challenge to the functional security development paradigm.

Paradigm 2. The security development paradigm based on encryption, authentication, and authorization. Its thinking perspective is to use authorization management to safeguard legitimate users to get safe access to software and hardware facilities, information services, and data resources. Its code of practice is to authorize the use of network facilities, information services, and data resources based on cryptographic engineering theories and management methods. Its processing principle requires additional encryption authentication codes or special supporting facilities relative to the protected object. Its challenge lies in the difficulty in fundamentally eradicating security issues, such as loopholes and backdoors, in the host execution system subject to the encryption authentication algorithm.

Paradigm 3. The cybersecurity development paradigm based on detection and analysis. There have been three focus stages in history on (1) deletion and elimination of viruses and Trojans, (2) software and hardware flaw discovery and repair, and (3) attack behavior trait perception and blockage. It focuses on detecting and removing any malicious code inserted or implanted in cyberspace terminals, nodes, or system software and hardware, creating and iterating malicious code libraries. It also focuses on using patches to fix the security flaws in the target system's software and hardware code design, or introducing different levels of active/passive defense technology to avoid the injection of virus and Trojans or reduce the exploitability of the target object's vulnerabilities (backdoors). Additionally, it blocks the attack chain or reduces its reliability through the attack behavioral trait analysis and precise perception. Its corresponding code of practice is the deletion of malicious codes, alarm/quarantine/manual intervention, spread/proliferation prevention and control, establishment and iteration of virus and Trojan libraries to enrich the knowledge base of malicious behavioral characteristics, development of the vulnerability database, software and hardware code security design specifications, and vulnerability analysis technology to explore and discover vulnerabilities, reducing the accessibility of attack surfaces or the availability of attack resources, using built-in probes, honeypots, sandboxes, running logs, and other real-time or nonreal-time methods to collect data of suspected problem scenarios as much as possible, and using comprehensive technologies, such as black/white lists, big data, and artificial intelligence to detect, suppress, or prevent possible attack behavior. Its

Email: ndscwjx@126.com

common processing principle is that additional detection or protection facilities are required relative to the protected object. The common dilemma for the above three focus stages lies in how to deal with unknown security threats in cyberspace based on unknown vulnerabilities, backdoors, viruses, and Trojans for lack of prior knowledge.

New development paradigm of cyberspace endogenous safety and security. The goal of the cyberspace endogenous safety and security development paradigm is not to solve the personalized cyberspace endogenous security problems. However, it aims to construct a structure about paradigm to solve the ubiquitous cyberspace endogenous security problems to find a revolutionary security defense structure that does not rely on (but does not exclude) prior knowledge.

(1) Cyberspace endogenous security ubiquitous problems and paradigm revolution. In the article cyberspace endogenous safety and security [2], the author explains cyberspace endogenous security problem and indicates all natural or human functions with accompanied or derivative apparent side-effects or invisible functions, the so-called endogenous security problem. The endogenous security problem is the internal contradiction of metafunction or intrinsic function. Thus, it can only be avoided or suppressed and cannot be eliminated. The author believes that there are severe endogenous security ubiquitous problems in cyberspace for the following reasons. First, the defects or loopholes in software and hardware code design cannot be dodged completely. Second, the backdoor problem cannot be eliminated. Third, the current theoretical progress and scientific and technological capabilities cannot thoroughly investigate the loopholes in the software and hardware code. Finally, man-made attacks continue to penetrate the traditional functional security field. Besides, the functional security problem has evolved into a compound one featuring random failure and man-made attacks. It means that it has become a "generalized functional security problem".

How to quantify rather than "do our best" to deal with the uncertain (unknown and unknown) threats caused by endogenous security ubiquitous problems has become one of the most urgent and challenging tasks in cyberspace-related industries or application fields. Therefore, it is necessary to implement breakthrough changes to the existing security development paradigm. It is also crucial to change the thinking perspective and propose a new methodology and practice norms. The author calls it "cyberspace endogenous safety and security development paradigm".

(2) Cyberspace endogenous safety and security development paradigm. The goal of the cyberspace endogenous safety and security development paradigm is to deal with the deterministic risks or uncertain threats caused by the vulnerability/backdoor of the target object with the function of quantifiable security design. This is to end the current network attack theories and methods based on the design defects of software and hardware code in theory and practice. The core concept of cyberspace endogenous safety and security development paradigm is to propose a theoretical system and methodology independent of prior knowledge, such as vulnerability/backdoor detection and attack characteristic analysis, and establish a set of practice norms to effectively solve cyberspace endogenous security ubiquitous problems.

(i) New perspective and methodology. To solve the endogenous security ubiquitous problems, it is necessary to identify a new perspective: obtaining network security defense capabilities that do not rely on the attacker's prior knowledge; creating a new methodology: determining a universal method for transforming the "unknown unknown threat" to "known unknown threats" within the target system structure; implementing specifications and standards. It is also necessary to transform the "known unknown threats" into reliability events with a controllable probability to confine the common-mode escape probability within a set threshold; curb trial-and-error or blind attacks. Furthermore, it is necessary to develop a mechanism to suppress or eliminate such attack threats arising from the common structural endogenous security problems.

(ii) Theoretical system. Based on the goal of the endogenous security development paradigm, the following endogenous security theories have been formed.

• Analysis and generalization of the cyberspace endogenous ubiquitous problems;

• The relatively correct axiom and generalized robustness control theory based on the coding channels;

• Processing methods of uncertainty and random event normalization;

• Integrated functional security and network security architecture without relying on prior knowledge;

• Design and evaluation and measuring methods for the endogenous security structure.

The specific contents of relevant theories can be found in reference [3].

(iii) Practice norms. In 2013, based on the rediscovery of the "relatively correct axiom" (also known as the consensus mechanism), the author proposed to transform security problems into the "known unknown" from the "unknown unknown" using the principle of relative construction [4], with the following core ideas. The uncertainty (unknown unknown) at the individual level can be transformed into the "known unknown" probability at the group level in the form of differential/common-mode manifestation through the system construction, with the size of the differential mode probability controlled by a specific mechanism design, i.e., controlling the possible impact of the unknown problem. After several years of efforts made in this conjecture, the author proposes the practice codes for an endogenous safety and security development paradigm called the "dynamic heterogeneity redundancy (DHR)" architecture [4] (see Figure 1).

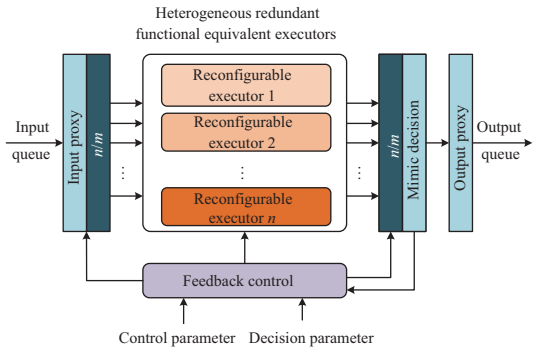

Figure 1 Abstract model of DHR architecture.

The multidimensional dynamic reconfigurative feedback operating environment of DHR based on the iterative rule can make any individuals trial-and-error or blind attacks shielded through the heterogeneous error-tolerance mechanisms. Feedback control loops can generate function equivalent difficult-to-measure effects within the heterogeneous

redundancy environment. This aims to undermine the supposed premise of trial-and-error attackers fixed background and conditions. Attackers are compelled to have the capability of launching concerted attacks within the dynamic heterogeneous redundancy environment in non-cooperative conditions. It means that we can deal with human attacks based on dark functions and failures caused by software and hardware random inefficiency only using such mechanisms as policy ruling, feedback control, and multidimensional dynamic reconfiguration without relying on (but it can absorb and integrate) external prior knowledge and additional defense measures. This is because of the difficult-to-detect and biological mimic phenomenon generated by random, diverse, and redundancy features within the DHR architecture. Thus, safety-security integrated and generalized robust control functions can be provided. It can also be called "generalized functional safety with quantifiable design and verifiable measurement".

(iv) Developmental dynamics. Currently, the theory system based on DHR has been constructed. The development of endogenous safety and security has formed an entire chain layout from hardware to software, components to systems, and technology to application in the network communication, laying a solid foundation for the innovation and development of the discipline direction. Several application technologies, such as supporting technology, generic foundation technology, network information infrastructure, industrial control, big data, chips, network service, and other fields, have also been developed. The technology development of endogenous safety and security baseline 1.0 has been completed in China, which is endogenous safety and security-based information systems or control devices set up with COTS-level parts, components, group sets, and subsystems. Since January 2018, the Ministry of Industry and Information Technology has conducted various deployment and application demonstrations of baseline 1.0 products in Henan Unicom and Jing'an Network Company, which has fully tested the universality, maturity, and economy of relevant technologies. Research on the practice specification of designing software and hardware systems using the endogenous security paradigm is being carried out, i.e., the work related to baseline 2.0. Therefore, to better verify the development route of endogenous safety and security in cyberspace and test the security of endogenous security-related equipment and products, the world's first permanently online and globally open network endogenous safety and security test bed was established in Zijinshan Laboratory in 2019 [5]. In 2020, Zhijiang Laboratory started developing China's largest industrial Internet endogenous security test bed.

Acknowledgements This work was supported by National Natural Science Foundation Innovation Group Project (Grant No. 61521003).

References

1 Kuhn T S. The Structure of Scientific Revolution. Chicago: University of Chicago Press, 1962
2 Wu J X. Cyberspace endogenous safety and security. Engineering, 2021. doi: 10.1016/j.eng.2021.05.015
3 Wu J X. Cyberspace Endogenous Safety and Security: Mimic Defense and General Robust Control (in Chinese). Beijing: Science Press, 2020
4 Wu J X. Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security. New York: Springer, 2020
5 Network endogenous security test bed. https://nest.ichunqiu.com