A security model based on intelligent decision

Shiping Xu, Ying Zhou*, Ronghua Guo, Jiawei Du, Zhe Liu
Luoyang Electronic Equipment Test Center of China, Luoyang, Henan, 471003, China
*Corresponding author’s e-mail: zy_jackson@sina.com

Abstract. This paper introduces intelligent decision-making into security model and proposes an adaptive network security model based on intelligent decision-making, based on the analysis of traditional security model. On this basis, the security capability of the model is preliminarily given, and the technical framework of the security protection system is constructed based on the model. Finally, an adaptive security protection process based on the model is given.

1. Introduction
With the rapid development of network and information technology, various security events such as Trojans, worms, DDoS attacks, botnets, and network intrusions have become more frequent, and the complexity and automation of cyber attacks have been increasing, all of which make the traditional security protection methods face a severe challenge. In order to utilize various existing security defense technologies and form a whole security protection system, research on various security models and related technologies has gradually become a hot research topic in the field of network security[1]. Based on the research status of existing PDR security model and its derivative model, this paper proposes a security model based on intelligent decision-making, and discusses the security capability, technical framework and security protection process of the model.

2. Research status of security model
As the foundation of the security protection system, the security model has always been the focus of information and network security research. The classic security models include the PDR model[2] proposed by the US Internet Security Systems Corporation, the P2DR model[3], the PPDRR model[4], and the PDRR model proposed by the US Department of Defense[5]. The dynamic defense model APPDRR model[6], the WPDRRC model proposed by China's 863 information security expert group[7], the adaptive security framework[8] proposed by Gartner for the next generation security system, and the P2OTPDR2 model[9]. The above models are supplemented and improved from the basic PDR model, taking into account the three elements of protection, detection and response, based on the theory of time-based security. The ability and security of different models are measured by time scales, which fully reflects the dynamic thinking of security. However, with the continuous development of cyber-attack technology and the security vulnerabilities that are constantly discovered by the network system itself, the security policy of the network protection system cannot be adjusted in real time according to the security status of the network, resulting in a longer "shutdown" time of the network system. The loss has become larger. Although the existing security model basically uses the security policy as the core to complete the model actions of early warning, protection, detection, response, etc., for the moment, the formulation, generation, delivery, and execution of security policies are based on human experience and When knowledge is implemented, it is often impossible to make security
decisions objectively and timely according to the current network security status and provide corresponding security policies to achieve real-time security protection.

3. Security model based on intelligent decision

3.1. Security model design based on intelligent decision

At present, the classical adaptive protection model PDR and its evolution model (such as P2DR, PDRR, P2DRR, etc.) propose a security capability consisting of "protection", "detection", "response", and "recovery" centered on "policy". And the stage is generally recognized. However, systems with the above security capabilities and phases are still passively protected, lacking sufficient ability to detect threats in advance and proactively protect them. With the development of technology, such as intelligent decision-making, it is possible to use it to predict and dispose of threats before they occur.

Combining the advantages and technical feasibility of the existing adaptive protection models, this paper proposes an adaptive security model for the network system—the ID-P3DR2 model, which will focus on the "security strategy" and include "predicting", "protection", "detection", The five core security capabilities and phases of "response" and "recovery" are shown in Figure 1.

![Figure 1 ID-P3DR2 model](image1)

**Intelligent Decision** It is the core of the operation of the entire safety technology system. In the adaptive protection system, the entire security system is constructed and operated by the security policy. As the security state changes, the security policy must be dynamically determined and adjusted to achieve security. In the earlier protection system, security decision-making and policy adjustment mainly relied on people to configure, resulting in inefficient security response. For highly dynamic and complex network systems, security decisions and policy adjustments have failed to meet security requirements[10]. With the development of artificial intelligence technology, intelligent decision making using artificial intelligence technology to achieve automation has become possible. The online model of the network system needs to be centered on intelligent decision-making. With the situational awareness and automated linkage response technology, the adaptive protection of security threats is realized, and the threat response speed is greatly improved.

**Security Policy** The security policy is a set of rules for guiding security activities based on the inherent security requirements, guidelines and principles of the network system, as well as external constraints such as laws, regulations, and regulatory requirements. It defines how to implement protection of the personnel, equipment, and software in the network system, how to deal with security incidents and other specific requirements. The entire network system security system operates under the guidance of security policies. The essence of adaptive security is that security policies can be adaptively adjusted with the security state of the system itself and the dynamic changes of external threats to guide the security system to effectively protect against threats.

**Prediction** The core of the forecasting phase/capability is to proactively predict the attack events and potential asset exposures that the network system may encounter by sensing changes in the internal and external environment, and feedback the prediction results to the protection and detection phases to form a closed loop. To avoid potential events, network systems must monitor hackers and other sources of intelligence to predict new attacks. Intranet systems must continuously track changes in assets and the environment and analyze new vulnerabilities.
Protection  The key goal of the protection phase/capability is to reduce the attack surface of the network system and prevent the attacker and its attack methods before the attack affects the network system. This phase typically includes a set of strategies, products, and processes designed to prevent the success of the attack, including the ability to strengthen and quarantine systems, vulnerability fixes, transfer attackers, and prevent unauthorized access and activity.

Detection  The protection system of the network system must assume that it has been compromised or that there is a possibility of being compromised, so the detection capability is crucial. The goal of detection is to reduce the time it takes to identify threats by identifying and identifying threats. This requires continuous and comprehensive monitoring of the system and the use of increasingly sophisticated analytical tools to provide detection capabilities.

Response  The response is to deal with discovered threats or attacks in a timely manner. It is necessary to combine comprehensive investigation and evidence collection and traceability analysis to determine the root cause and scope of the threat, and to develop appropriate strategies for rapid disposal. Changes to security policies and safeguards must then be designed, modeled, and implemented to avoid similar events in the future.

Recovery  The main purpose of the recovery phase/capability is to repair the damage caused by the attack in time to ensure the availability and continuity of the services of the network system. It usually includes two aspects of data recovery and business recovery.

The adaptive security protection process as a whole is a security decision based on the perceived security risk, and adjusts the closed loop process of the security policy implementation response. Through the continuous closed-loop operation of the protection process, the safety protection system can follow the dynamic changes of the internal and external security situation and continuously evolve itself.

3.2. Security model security capabilities based on intelligent decision
In order to ensure the security of all levels of the network system and realize the adaptive security protection of the network system, several key capabilities need to be realized in each stage of the model. Figure 2 lists the 14 core security capabilities that a network system's protection system must have and its correspondence with the capability phase of the intelligent decision-based security model.

The three core competencies of "threat knowledge extraction and continuous update", "risk identification and assessment" and "threat prediction" need to be realized in the forecasting stage.

Three major capabilities of "system reinforcement and isolation", "abnormal and attack event protection", and "protection system automatic construction and adjustment" are required in the protection phase.

The "system vulnerability detection", "abnormal and intrusion event detection", "risk confirmation and sequencing" capabilities are required during the detection phase.

Three major capabilities of "event investigation and forensics", "security policy adjustment", and "event linkage response and disposal" are required in the response phase.

The "data backup and recovery" and "business recovery" are required during the recovery phase.

3.3. Intelligent decision-based security model technical framework
The security technology framework of the network system is constructed based on the above security model, as shown in Figure 3. The entire technical framework consists of four parts: security mechanism, security resources, regulatory standards and security management. The security mechanism includes four levels: physical and environmental security, network and communication security, device and computing security, and application and data security. Security resources include security platform, security device and component, and threat knowledge. The basic support; at the same time, the implementation and operation of the technical framework also needs the support of the safety management system.

4. Adaptive security protection based on intelligent decision-making security model
Based on the model proposed in this paper, the security threat adaptive protection process shown in Figure 4 can be implemented.

Figure 3 Security Model Technical Framework  
Figure 4 Security adaptive protection process

**Situational awareness** Situational awareness continuously monitors and analyzes the massive data and analysis results of the network system's asset status, system vulnerability, security log, attack events and threat intelligence, knowledge base, etc., and analyzes the context, hazard, scope and development trend of each specific threat, in turn, comprehensively describe the current security situation of the entire network system, predict the next possible attack and its harm.

**Intelligent decision** Based on the security situation and threat development trend described by situational awareness, intelligent decision-making combines the security objectives, security policies, security capabilities and security knowledge of the network system to comprehensively determine the response strategy for security threats. Depending on the security threat, the response policy can include security policy adjustment, system hardening, defense system adjustment, event handling, backup, and recovery.

**Linkage response** The linkage response specifically implements the response strategy formulated by the security decision process, and according to the current situation of the security resources, jointly adopts different methods such as technology and management to deal with the security threat, track and verify the response result, and feedback the execution result to the situational awareness for situational awareness. Master the security status of the system in real time and initiate new security decisions and linkage response processes as necessary.

5. CONCLUSION

Based on the analysis of various existing classic security models, this paper introduces intelligent decision-making into the security protection system, and proposes a security model based on intelligent decision-making. Based on the model, the security model should be secure. The capabilities, technical framework and security protection process were initially discussed. How to extract the current network state feature factor, as the input of intelligent decision-making, takes the corresponding deep learning or reinforcement learning algorithm for decision-making, gives the optimal solution strategy to deal with the current network threat, and timely (or even real-time) network responding is the focus of the next step.

References

[1] Jiang Wei. Research on key technologies of active defense based on offensive and defensive game model [D]. Harbin: Harbin Institute of Technology, 2010.

[2] SCHWARTAU W. Time-based security explained: Provable security models and formulas for the practitioner and vendor [J]. Computers & Security, 1998, 17(8): 693-714.

[3] HAN R-S, XU K-Y, ZHAO B. Research and Design of Policy Deployment Model for P2DR Model [J]. Computer Engineering, 2008, 20(0): 69.
[4] Zhou Haigang, Qiu Zhenglun, Xiao Junmo. Network Active Defense Security Model and Architecture[J]. Journal of PLA University of Science and Technology: Natural Science Edition, 2005,6(1):40-3.

[5] Lin Shoumei, Zhang Jiandong, Hu Ruizhi. PDRR Network Security Model [J]. Computer CD Software and Applications, 2010(11):57.

[6] Pan Jie, Liu Aijie. Research on Network Security System Based on APPDRR Model [J]. Telecommunication Engineering Technology and Standardization, 2009(7):27-30.

[7] Yao Chuanjun. Application of WPDRRC Information Security Model in Security Level Protection[J]. Optical Communication Research, 2010(5):27-29.

[8] https://www.csdn.nearticle/2015-06-24/282503.Gartner: Using adaptive security architecture to deal with advanced directed attacks.

[9] Zuo Feng. Research on Information Security System Model[J]. Information Security & Communication Security, 2010(1): 70-72.

[10] HAN Ruisheng, ZHAO Bin, XU Kaiyong. Policy-based Integrated Network Security Management System[J]. Computer Engineering, 2009,35(8):201-204.