The framework study on mimic defense technology in power web service system

Yuxiang Cai1, Dan Pan1, Yiting Wang1
State Grid Fujian Information & Telecommunication Company, Fuzhou, China
150294189@qq.com

Abstract. Aimed at the features of the power grid web system for the State Grid Corporation of China (SGCC), the paper analyzes the confronting security risks. A mimic defense security protection system for the power grid web application has been designed by combining the features of network attack and introducing the mimic defense core technology. The defense framework with layered ideas and dynamic heterogeneous redundancy has implemented effective protection at multiple attack phase and expanded the defense range so as to provide the security protection capacity to the power grid web application.

1. Introduction
To reduce the dead weight of the floor, it can be replaced by ceramsite concrete instead of ordinary. The internet environment has changed a lot in recent years. According to the network security report released by the CNCERT/CC in 2016, the Web system vulnerability alone accounted for 16.5% of all of them. In 2016, about 178,000 fake pages against our domestic website were detected by CNCERT/CC and about 40,000 IP address were implanted in backdoor of more than 80,000 websites in China, which was a 9.3% increase compared to 2015.

With the popularity of power information system and increasing accumulation of data, more and more power generation, dispatch and marketing rely on the information system and more and more Web service system based on B/S framework have been established and come into service[1][2]. They are accompanied by the attack method against web service system in an explosive increase tendency and constantly upgrade, which have brought severe hidden danger of the security of the service system. The currently cyber security defense system, those are extensively applied or deployed to the power enterprises with technologies or devices, such as firewall, security gateway, intrusion detection system, virus killing, authentication of users and access control, actually, their essence is passive security protection system based on prior knowledge(including the features, behaviors and finger prints of known attacker)[3-6]. It has genetic deficiencies to tackle uncertain threats. It only has acquired immunity and can only keep searching for vulnerability and keep patching. It cannot defense the unknown vulnerability and the unknown attack of the unknown backdoor[7][8]. Under such circumstance, it is difficult to effectively deal with all kinds of increasingly complex and intelligent infiltration network intrusion for the power enterprises, which makes it difficult to guarantee the security of their key Web systems.

2. The overview of mimic defense technology
Mimic security was a network space security defense theory that formally proposed by Wu Jiangxing, the academician, in 2014. The theory was inspired by the behaviors of mimic octopus to avoid attacking from enemies by constantly shifting shapes, texture and colors. They can dynamically, pseudo-randomly
select to execute various hardware variants and the corresponding software variants under active and passive triggering condition so that the internal and external observers can observe the uncertainty of the hardware executive environment and software operating status[9]. Moreover, mimic defense technology makes the attack chain based on vulnerability or backdoor cannot or in a difficult way to be established, so as to improve the security level of the system[10].

![Diagram](Fig.1 The basic principle of mimic)

The core of the mimic defense technology mainly includes two parts, first one is the mimic defense heterogeneous redundancy executable framework technology and the second one is the multimode vote technology.

The mimic defense heterogeneous redundancy executors refers to the defense object program with equivalent function but different implementation model. Its framework method includes the multiple compiling of software intermediate language, the change of function structure, control code confusion, scripting language randomization. The structure change of key function, key program segment, key order and even the entire protective object program, can be achieved through the diversification of source - and compile-level programs. The heterogeneous redundancy executors and the dynamic dispatch, enable the change of the vulnerability in a dynamic way presented to the attackers, so that makes the attackers cannot attack successfully.

Multimode vote technology is mainly used to detect and find network attack. Its process is a comparison of the implementation results of the heterogeneous redundancy executable. It can rapidly identify the network abnormality if the enter is same but output is different so that to monitor and warn the network attack.

To summarize the working principle of mimic defense technology is a set of heterogeneous executables of equivalent function. It can randomly select multiple executables in the heterogeneous set in a certain time period and it can provide service with vote comparison mechanism. Obviously, mimic defense improves the attacking difficulty to three levels. The current static, single and certain object attacking difficulty has been upgraded to the level of coordinated attack with multiple objects in static and heterogeneous space and then further upgraded to the level of coordinated attack with dynamic heterogeneous space and multi-dimensional dynamic objects, which has been improved in a nonlinear trend.
3. **The mimic defense framework applies to power web service**

The mimic defensive technology designed in the paper, on the one hand, starts with the web resources to study its address detection and the dynamic replacement of its address to achieve the dynamic jump technology of web resources address. On the other hand, it begins with the execution environment and process of web application to study the heterogeneous executables and the redundancy of the web application to realize the defense technology based on heterogeneous redundancy.

The mimic defense technology designed in the paper has three main parts: the detection technology of web resource address, the mimic technology of web resource address, and the dynamic replacement technology of web resource address. These three parts work together to achieve the dynamic jump of web resource address and the realization of the defense technology based on heterogeneous redundancy.

The defense technology based on dynamic jump of web resource address is mainly used to solve the problem that the static URL will expose the Web application directory structure and change it to be an attack entrance [11][12]. The URL can be in a constantly changing status by combining the dynamic thought of mimic defense and adopting the dynamic jump technology of web resource address. In this way, the dynamic change of hidden and underlying attack entrance of the Web application directory structure can be realized so that to block the attacking and guarantee the security of the Web application.

The defense technology based on heterogeneous redundancy firstly studies the attribute composition of the Web application system. The key points include the operation system, Web service software, Web application compiling language and etc. Based on that, construct a heterogeneous redundant execution environment covering multiple layers with functional equivalence and differentiation by combining the heterogeneity, dynamic nature and the redundancy thought of mimic defense, to break the stability of the environment that relied by the Web application attack, and protect the Web application.

![The Theoretical Basis of Mimic Defense Technology](image)

**Fig.2** Technical framework of mimic defense technology research
In order to establish the heterogeneous redundant execution environment of Web application, the heterogeneity of executables have been achieved in multiple layers including virtualization platform, virtual machine operation system, server software and web application in the mimic Web gateway. Each layer includes multiple practicable heterogeneous components to select from so as to build up the heterogeneous Web gateway executables. The message distribution and voter have been added to the entrance and exit as the proxy of enter and output. The message distributor will send the user request to multiple Web gateway executables separately and conduct a centralized vote of output through voting algorithm at the voter to get a uniform output result. The output result will be output after operated by the proxy of output.

The mimic defense of power web service system is deployed at the exit of the extranet internet. It can realize the active defense by forwarding the traffic to the power mimic Web gateway in a real-time and dynamic way. The detailed deployment framework is shown as figure 4[13][14]:

![Fig.3 The multi-layer mimic defense model](image-url)
Among others, the terminal will send request to master server through network and transfer the traffic of master server to the mimic protection area of the physical machine room through load traffic management. A part of attacking traffic can be filtered through the existing firewall protection devices and send the rest traffic to the mimic Web gateway. The load traffic management is mainly responsible for the traffic distribution between the Web gateway and the master server so that the optimal server can be selected for users intelligently according to the dispatch algorithm. Under normal circumstances, all traffic will be distributed to the mimic gateway through the load traffic management and safely defend the system in the mimic protection area. In case of excessive load or failure of mimic Web gateway, the traffic will be forwarded to the master server through load balancing server, so as to avoid the service unavailability caused by the failure at a single point and ensure the stable and smooth operation of the service.

In the synchronous process of service, the gateway can suffice the real-time synchronous requirements by the data crawling from the government service network periodically. The system will guarantee the real-time synchronization of the data service for gateway and real servo through incremental download. The actual operation validates that the system can suffice the need for customer information change synchronization among various service application system.

4. Conclusion
In order to solve the "Easy to attack but hard to defend" problem of power web system, this paper proposed a Mimic defense architecture of power web system, which integrates dynamic jump of web resource geology and heterogeneous redundant execution technology, without changing the existing application system. Through this method, the attacker can not master the real attack entrance on the web server, and enhance the attack difficulty.

Acknowledgments
This work is Supported by the science and technology project of State Grid Fujian Electric Power Company; " Research on proactive defense technology of power web service application based on mimic defense"

References
[1] Annarita Giani, Russell Bent’s Addressing Smart Grid Cyber Security.
[2] Tassos Dimitriou, Ghassan O’s KaramePrivacy-Friendly Planning of Energy Distribution in Smart Grids.
[3] P. McDaniel and S. McLaughlin, Security and Privacy Challenges in the Smart Grid, In IEEE Security and Privacy, Vol. 7, No. 3, 2009.
[4] S. Raj Rajagopalan, L. Sankar, S. Mohajer, H. Vincent Poor, Smart Meter Privacy: A Utility-Privacy Framework, In IEEE SmartGridComm, 2011.
[5] K. Kursawe, G. Danezis, and M. Kohlweiss, Privacy-Friendly Aggregation for the Smart-Grid, In Proceedings of PETS, 2011.
[6] Barbara Vieira, Erik Poll’s A Security Protocol for Information-Centric Networking in Smart Grids.
[7] C. Gentry and A. Silverberg. Hierarchical id-basedcryptography. In Proceedings of the 8th Internation Conference on the Theory and Application of Cryptology and information Security: Advances in Cryptology, ASIACRYPT 02, pages 548{566, London, UK, UK, 2002. Springer-Verlag).
[8] Y. Kim, V. Kolesnikov, H. Kim, and M. Thottan. SSTP: a scalable and secure transport protocol for smart grid data collection. In smart Grid Communications, pages 161{166. IEEE, 2011).
[9] D. Pointcheval. Provables security for public key schemes. In Contemporary Cryptology, Advanced Courses in Mathematics-CRM Barcelona, pages 133{190. Birkhauser Basel, 2005).
[10] Y.M. Cui, F.L. Li. Talking about Smart Grid and Smart Network [J]. Electric Power Information and Communication Technology.2008,6(11).
[11] B.X.Liu. Active defense against hacker intrusion [M].Beijing: Electronic Industry Press.2007.
[12] X.F.Song, F. Xue, W. Li. Summary of Smart Grid Frontier Technology [J]. Telecommunications for Electric Power System, 2010,31(7):1-4.
[13] L.J.Chen, S.W.Mei, Y. Chen. Smart grid information security and its influence on power system survivability [J]. Control Theory & Applications,2012(2):240-244.
[14] X.T.Xu, Z.H.Yang. Information security for Internet of Things[M].Beijing:Post & Telecom Press,2012.