Research on Mimic Defence Technology for Smart Unit Application Environment of Power Grid

Zesheng Xi\textsuperscript{12}, Bo Zhang\textsuperscript{12*}, Xin Sun\textsuperscript{3}, Xiaojuan Guan\textsuperscript{12}

\textsuperscript{1}Institute of Information and Communication, Global Energy Interconnection Research Institute, Nanjing Jiangsu, China
\textsuperscript{2}State Grid Key Laboratory of Information & Network Security, Nanjing Jiangsu, China
\textsuperscript{3}State Grid Zhejiang Electric Power Research Institute, Hangzhou, Zhejiang, China

E-mail:4317045xi@163.com

Abstract. Aiming at the problem that the new network attack cannot be effectively defended at present, this paper proposes a framework of application-level mimic defense technology for smart grid units to solve the active attack defense problem of smart terminal units in the source grid environment. In this paper, the application security mimic defense architecture and interactive instruction level heterogeneous redundancy technology for smart grid units are studied to achieve universal and self-immune active immunity against grid application-level attacks. Furthermore, the dynamic change and heterogeneous redundancy characteristics of application level are constructed by mimetic defense technology. The risk and vulnerability of terminal application security vulnerabilities are actively hidden to actively avoid attacks, so as to enhance the active defense capability of industrial control terminal side of power grid.

1. Introduction

With the deep integration of smart grid with Internet of Things, and the construction of Energy Internet, the grid company has established a two-way interactive service mode between grid side and user side. Users can understand power supply capacity, power quality, electricity price status and outage information in real time, and arrange power consumption reasonably. Meanwhile, the grid operation control is more flexible and economical, and can adapt to the access of a large number of distributed generators, micro-grid and charging and discharging facilities of electric vehicles. These larger number of heterogeneous intelligent interactive terminals expand network security protection boundaries and bring more flexible and diverse business security access requirements to the company's network security protection system\textsuperscript{[1]}. At the same time, the risks of information leakage, illegal forgery and being controlled in terminals themselves also pose higher challenges to the integrity protection and attack defense of heterogeneous terminals in power grid.

1.1. Static characteristics of vulnerability in smart grid units are easy to be detected by attackers.

Power grid application environment has the characteristics of complex and diverse embedded hardware environment, heterogeneous software environment, differentiated application and multi-type private communication protocols, which makes it difficult to obtain a unified and standardized "acquired immunity" when defending against network attacks. In addition, the static, similarity and certainty of the application also provide attackers with many conveniences, such as target recognition, defensive behavior detection, attack technology test improvement and attack effectiveness evaluation\textsuperscript{[2][3]}. 
1.2. Traditional protective measures cannot be applied on smart grid units because of limited computing environment.

The computing environment of smart terminals in power grids is heterogeneous and diverse, carrying a large number of industrial applications with heterogeneous enclosed and continuous operation. They are faced with the challenges of limited computing power, high reliability requirements, complex mechanism of malicious program destruction and complex protection technology[4]. Because of the complexity of implementation and high resource occupation, traditional terminal security protection products can hardly be applied to smart terminals.

1.3. Smart terminals of power grid bears core business, so active attack defense is urgently needed.

The terminal of power system is widely interconnected and carries the core business functions of power grid, and the environment of user side, site side and site side of the terminal is uncontrollable[5][6]. The high real-time requirement of power grid service and zero tolerance requirement of attack make the demand of active defense of power terminal attack urgent.

2. Mimic Defense Technology

Mimic defense technology is the frontier technology in the field of network security defense. It is mainly based on Bionics to construct the dynamic redundancy of defense objects. Mimic defense technology makes the vulnerabilities and flaws of smart units in power grids dynamic and makes it impossible for network attackers to find out the definite attack path, which realize active hiding of risk points and active avoidance of network attacks[7].

The key of mimic defense system consists of five mechanisms: dynamic heterogeneous redundancy, input-output proxy and policy scheduling, fragmentation, randomization and dynamics, iteration and superposition.

2.1. Dynamic Heterogeneous Redundancy Construction Mechanism

DHR is designed and developed by totally independent working groups using different development languages and tools. Mimic defense system runs these heterogeneous redundant executors with equivalent functions on different hardware platforms, which makes the vulnerabilities of each redundant executor independent, so as to avoid common vulnerabilities and backdoors.

2.2. Input-Output Agent and Policy Scheduling Mechanism

By introducing manageable I/O proxy mechanism and compound scheduling mechanism (e.g. combination of majority, weight, polling, randomness, etc.) between standardized or normalized interfaces, mimic can be presented in a more sophisticated and cunning manner, and it is easier to conceal the internal characteristics of the defense side (e.g., it can disrupt the attempt to derive system response functions from input-output relations), or shield from external excitation. Abnormal reactions triggered by excitation (such as significant increase in waiting time or incorrect output) or attempts to detect software version information through undefined fields of protocol packages are blocked.

2.3. Fragmentation mechanism

Fragmentation mechanism is introduced based on redundant backup designed according to reliability requirements. Information fragmentation is transmitted through multi-paths, fragmentation storage is realized by heterogeneous non-homologous devices, and logical expression of file catalogue and physical mapping are separated and managed by using "single-line connection" mechanism. It is expected that the security of file usage is based on the guarantee of the whole mechanism[9][10].

2.4. Dynamic and randomization mechanism

Through the diversity, randomization and dynamics of instruction system, address space and system data, it is difficult for attackers or infiltrators to establish a sustained and reliable attack chain by making full use of the uncertainty brought by dynamics, diversity and randomness. Especially in the static
environment, the available conditions and attack effects that were originally determined should not be
determined and remain valid in the dynamic randomized construction environment[8].

2.5. *Iteration and superposition mechanism*

The complexity and uncertainty of the mimic protective device can be increased exponentially by using
the iteration and superposition mechanism. If the mimetic transformation is implemented at the system
level, the simulation-based intelligent redundancy scheduling of equivalent and multiple system-level
executives can make the external structure representation of the device appear non-linear cognitive
difficulty. The uncertainty of the whole device will be unprecedented if these system-level actuators
themselves are further mimetically upgraded or further mimetically implemented at their component,
module, component and device levels.

3. *Mimic Defense Technology for Smart Unit Application Environment in Power Grid*

Considering that the upper layer of the logical structure is often the most accessible to attackers and is
the key link to ensure external services, the design of the mimic defense architecture will focus on
protecting the security of the application layer. As shown in Figure 1, based on the analysis of mimetic
defense structure, DHR structure is implemented based on heterogeneous redundant variants.

![Diagram](image)

Figure 1 Implementation roadmap of mimic defense architecture

Heterogeneous redundancy variant implementation is the basis of mimic defense technology. It can
be achieved by means of diversified compilation and instruction heterogeneous redundancy[11].

The control design of heterogeneous redundant variants mainly includes input distribution design
and output redundant voting design.

3.1. *Input distribution design*

Input distribution is the real entry of parameters. According to the calling time and mode of application
program or program function and the structure of input parameters, the function of distributing input
parameters to multiple heterogeneous executors (according to the dynamic heterogeneous redundancy
architecture of mimic defense, the executor is a component of logic heterogeneous implementation) is
accomplished. It ensures diversity and heterogeneity to realize mimetic. The preconditions for defense are shown in Figure 2.

3.2. Output redundant voting design
Output redundant voting is the real export of output results. According to the calling time and mode of application or program functions, combined with the structure of output results, voting algorithm is used to cross-judge the response of multiple heterogeneous executives with the same request, ensuring the consistency and correctness of output results. It is an important part of mimic defense. The design circuit is shown in the Figure 3.

3.3. Heterogeneous Redundancy Technology of Data Query Instruction Code
Heterogeneous redundancy technology of data query instructions mainly makes the data query instructions have label information through the characteristic processing of data query instructions. The tagged statements are filtered by feature and identified by voting based on query requests from heterogeneous executors, thus blocking malicious injection attacks by attackers. Detailed design as shown in Figure 4.1
It includes instruction characterization processing module, label verification module, parsing execution module and voting identification module. The specific functions are as follows[12][13].

1) All data query instructions in the source code of the application are labelled by instruction characterization module, and the labels used are dynamically and randomly changed with sufficient complexity.

2) Through the label verification module, the received data query requests are labelled and the results are generated.

3) Voting authentication module is used to identify the results of label verification. If all executives verify the correct results, the data query request is considered legitimate. Otherwise, the system will be attacked by malicious injection, and the abnormal information will be pushed to the central dispatcher.

4) If the data query request is a legitimate request, it can be de-labelled by parsing execution module, and then parsed execution.

Heterogeneous redundancy design of data query instruction realizes mimic defense at source code instruction level. It reverses the current situation of passive defense, and realizes active defense against data query injection attack.

3.4. Characterization Label Method of Data Query Instruction Code

The core of heterogeneous redundancy design of data query instructions is instruction characterization processing module, which includes instruction traversal sub-module, tag generation sub-module and tag dynamic change sub-module as shown in the Figure 5[14].
Instruction traversal submodule traverses the key instructions of data query in source code according to the type of data query language. Here, we take the SQL language as an example, and traverse the SQL keywords related to data query such as SELECT, FROM, WHERE, AND, OR, etc.

Label generation submodule is based on the completion of instruction traversal sub-module, adding tags generated according to a certain algorithm to the special location of key instructions (instruction front-end, instruction back-end, etc.). As an example, we add the label "abc123" to the front-end of SQL keywords such as select, form, where, and or, as shown in Figure 6. When an attacker uses admin user and enters the password 'OR 1=1', the constructed statement is abc123SELECT COUNT (*) abc123FROM Login abc123WHERE UserName = 'admin'abc123 and Password='OR 1=' 1'. In the case of SQL injection attack, the retained word OR is checked to be illegal because it does not contain the label 'abc123'.

According to the time threshold, the label dynamic transformation submodule dynamically changes the label of data query instructions in the program code to ensure the confidentiality and complexity of the label.

4. Conclusion
Aiming at the application environment of smart grid, this paper proposes a security architecture based on mimic defense model, and constructs heterogeneous redundant components with typical characteristics. Moreover, a method of instruction heterogeneous redundancy based on tagging is
constructed to increase the attack difficulty of attackers. It provides a new idea to solve the malicious attack problem in the process of information exchange in power grid application environment. It is the first attempt of mimic defense technology in power grid environment, and provides strong guidance for the popularization and application of mimic technology in power grid environment.

**Acknowledge**
The paper is supported by the science and technology project of State Grid Corporation of China: "Research and application of Mimic Defense Gateway applied to web application for power grid" (Grand No. 52110118001F).

**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-based cryptography. 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.