Design of Smart Campus Security Management and Control Platform Based on Big Data Technology

Long Peng(✉)

Urban Vocational College of Sichuan, Chengdu, China
375417507@qq.com

Abstract. As the traditional campus network security defense means fail to cope with the smart campus security threats under the current background of big data, a design scheme of smart campus security management and control platform based on big data technology was proposed. In the scheme, the smart campus system was layered and classified for the design of security protection mechanism and the granular protection management of the smart campus security was realized. Big data technology was used to build a smart security brain, which solved the problem of disorder data and the difficulty in data association and succeeded in data fusion storage on the smart campus. The intelligent operation and management platform provided an all-around awareness of the security situation of the smart campus so that the risk prediction, security warning, security disposal, and intelligent linkage for protection and reinforcement were achieved. The simulated attack test and security risk assessment showed a significant boost in the smart campus security defense capability and an obvious drop in the security risk level after the deployment of the smart campus security platform. Besides, the smart campus security alert and self-disposal ability were also improved dramatically after the practical application analysis.

Keywords: Smart Campus · Smart Security Brain · Data Fusion · Security Management and Control Platform · Security Situation

1 Introduction

With the rise of cloud computing and big data, university informatization is changing from digitalization to intelligence, and the construction of smart campuses has driven universities to develop, offer comprehensive services, and be more competitive. Smart campus mainly uses cloud computing, big data, and other technologies to establish an overall awareness of the physical environment on campus and to identify, in an intelligent way, the characteristics, work settings, and behavior trace of the teachers and students. In doing so, businesses such as scientific research, office work, management, teaching, and living are deeply integrated; the frequent interaction of people-to-people, people-to-things, and things-to-things are interconnected. Therefore, there are great varieties of smart campus data that will grow exponentially to form big data and impact the

C. F. Peng et al. (Eds.): EIMT 2022, AHSSEH 3, pp. 586–595, 2023.
https://doi.org/10.2991/978-94-6463-012-1_65

cyberspace security of the university, but the traditional cyber security defense means find it hard to deal with such threats.

2 The Security Risk of Campus Network in the Context of Big Data

As the construction of smart campus advances, universities utilize cloud technology, artificial intelligence, and other new technologies to develop their management and service applications such as AI cameras for security campus, Internet of things for the green campus, facial recognition for the behavior management system, web-based teaching platform anytime and anywhere, and interconnected new media, etc. This shows that universities are becoming more and more dependent on the Internet, the correlation and complexity of people and things on campus are increasing, and the network, equipment, and data grow more centralized, leaving cyberspace security with more and more security risks. And that is a new challenge for the university.

3 The Design of Cyber Security System for Smart Campus

3.1 Analysis of Security Risk

At present, the construction system of smart campuses in universities consists of the infrastructure layer, supporting platform layer, intelligent application layer, and presentation layer. To protect the smart campus, it is necessary to analyze the possible security problems in each layer based on their application characteristics [3].

3.2 The Design Ideas for Security System

The overall design idea of the cyber security system for the smart campus is that we aim at the protection object in the smart campus construction system, follow the principles of safety and reliability, dynamic compatibility, integrated innovation, easy management, advancement and standard, and multiple protection, and focus on data security to build a cloud + end + boundary Internet security ecosystem, capable of risk identification, security defense, safety inspection, safety response, and security recovery. As a result, the safety goals of visible risk, proactive defense, and automatic operation are realized, and the safety of school business is guaranteed.

4 The Design of Security Management and Control Platform

4.1 The Overall Framework of the Management and Control Platform

The smart campus security platform was designed based on the smart campus system. According to the characteristics of each layer in the system, the safety protection design was set to deploy sensors at every layer and flow measuring probes in the key network ports. By the use of data collectors, the data was gathered timely and then sent to smart security brain after being preprocessed, providing data support for the smart operation management platform to have a full awareness of the security situation, timely analyze and deal with security threats, and predict the security risks [5].

4.2 The Security Design of Infrastructure Layer for Smart Campus

The infrastructure layer of smart campus mainly includes wired networks, wireless networks, Internet of Things, cloud storage, and cloud computing architecture. As the first and the bottom line of defense, its main security problems lie in the server virtualization, network perimeter, and others. In the face of security risks in the era of big data, it is far from enough to protect the infrastructure layer by local high-performance and multi-functional security products. Therefore, the traditional passive defense should be replaced by the active defense with a multi-layer security line. To take the initiative to defend against attacks, it is required to collect a large amount of network data before it is being analyzed and sensed dynamically by the smart security brain for security threats [2].

4.3 The Security Design of Platform Layer for Smart Campus

Being the core part of the smart campus system, the supporting platform layer works as the application engine motherboard by connecting various applications such as application engines, development platforms, data centers, certification platforms. The supporting platform is the core code of the smart campus system, whose major security risks exist in the code security vulnerabilities and undeclared functions (backdoors) of the platform software. Hence the key issues for the supporting platform are code security and defense capability.

It is far from enough to simply rely on the security protection of the infrastructure layer to solve its code security problems. Therefore, there is a need to design an intelligent code security management platform to manage the code security of the platform software. One is an automatic detection mechanism for code security. The intelligent code security management platform monitors the platform software and all kinds of interface application codes in real time. Once the source code changes, it will give an early warning [1], automatically analyze the code to match with the vulnerability database, and send a timely warning if there is a bug. The other is an automatic reinforcement mechanism for source code security. The intelligent code security management platform links with at least two mature third-party code security hardening software. If code changes or bugs are detected, it will invoke the software to repair the code and conduct code obfuscation and code reinforcement simultaneously.

4.4 The Security Design of Intelligent Application Layer

The intelligent application layer comprises portal websites and other business systems. The third level of information system protection requires the business system to have security functions such as "identity authentication, access control, security audit, communication integrity, communication confidentiality, software fault tolerance, and resource control [7]. Therefore, this layer mainly needs to consider the application system code security protected by intelligent code security management platform, and system application security which focuses on the security of user identity authentication and behavior.

4.5 The Security Design of Presentation Layer

The presentation layer is the entrance for users to experience various applications on the smart campus using various terminals. With various kinds of abundant Intranet terminal devices and users in universities, it imposes huge security risks to the smart campus network and mainly concentrates on security protection for terminal devices and WEB pages.

4.6 Intelligent Management Platform for Security Operation

All kinds of safety equipment were deployed at each layer of the smart campus to gather massive security logs and behavior data. For the linkage of their security protection and the unified management analysis of the logs and data, a security operation management platform was established based on the smart security brain, enabling administrators to be fully aware of the smart campus' security problems and deal with the security loopholes. The platform includes an awareness module, a data processing and analysis module, and a decision processing module [6].

Data acquisition module. The main function of this module is to collect various security data. Flow measuring probes were installed at network exits such as campus network exit, data center exit, and every convergence layer to monitor traffic, sense its changes in real time, and produce traffic logs. Data collectors were deployed at each layer of the smart-to-campus log data and behavior data of security equipment and software. The awareness module preprocessed the data collected by the collector and the flow measuring probe, converted them according to the unified normalized data format, and saved them in the big data platform of the smart security brain, providing data support for security event analysis, threat presentation, and source tracking.

Data processing and analysis module. The big data platform of the smart security brain stored and indexed the data collected at the perception layer and used the data relation rule engine, resource management engine, data search engine, and statistical analysis engine for data fusion and association analysis. Based on the analysis, deep learning, machine learning, reinforcement learning, and other technologies were adopted to identify and understand the behaviors and intentions of the attacks. In the end, analysis reports were generated in response to alerts in time.

Decision processing module. The main task of the decision processing module is to evaluate security risk levels and predict threat trends according to analysis reports. Based on the level of security risks, the linkage policies were generated and sent to cyber security devices, such as the firewalls, intrusion prevention system (IPS), and web application firewall (WAF), and corresponding policy interfaces were adopted. Based on security threat trend analysis, a set of commands were created to trigger related cyber security devices or software to update security defense policies and reinforce security defense. With the help of the technologies such as association rules analysis, homologous analysis, machine learning to mine traffic and log data, the associated metadata, behavior, traffic log data in different stages of the attack were analyzed to restore the entire attacking chain sent from the attacker. Once completed, it accurately reflected the attacked network resources, the information of the attacker and the victim, etc.

4.7 Network Security Assessment

The network security problem was regarded as a game with multiple stages between the defender and the attacker, each stage corresponding to a safe state. When the solution was worked out, the mixed strategy in the security state could be equalized, the optimal scheme of two-way confrontation in the network security state was obtained, and the network entropy was introduced for quantitative analysis. The specific assessment is as follows: set in as the indicator information of the active defense network driven by big data and the information of two-way confrontation behavior; set out as the prediction of aggressive behavior and the quantitative effect value of the confrontation. Let the initialization value vector be:

```
$H0 = (h_1^0, h_2^0, \ldots h_k^0) = (0, 0, 0\ldots0)$
Repeat
for each $Q_1 \in q$ do
for each $q_{ij}^l \in Q_1$ do
```

The entropy difference of each stage was calculated, the value vector was updated by combining the mathematical model, the mixed equilibrium was calculated to obtain (Q1/q1, Si1, Si2)Sl and state probability, and the security situation of the active defense network was analyzed to get the security assessment of the active defense network. The principle of active defense was analyzed, the mathematical model of assessment was constructed, and the network entropy countermeasures quantitative technique was introduced to weigh the benefits and reduce the influence of interference factors for higher accuracy of the assessment. The benefit of defenders was seen as the quantitative evaluation standard to carry out a security assessment of active defense networks.

5 Experimental Results and Analysis

5.1 Test Scene

To verify the effectiveness of each security layer in the design, the real scene of the smart campus from the author's school was selected for testing. Some key devices and applications, such as boundary zone (W), demilitarized zone (DMZ), data service zone (D), terminal device zone (H), and application service zone (B), were chosen as test objects. W1, F1, F2, F3, and F4 were all common firewalls before the deployment.

The DMZ was located between the internal network and the external network in which WEB (selected for the test), email, and domain name system (DNS) servers were deployed. Zone W is the network boundary zone, where firewall W1 (selected for the test), border router W2, core switch W3 and others were deployed. Zone D is a cloud data center, and a virtual data server D1 and a virtual application server D2 were selected for the test. H is the terminal equipment zone, and the terminal host H1, mobile terminal H2, and wireless access point (AP) device H3 were selected. The application server was placed in zone B, and educational administration system B1 and OA office system B2 were selected as test objects. Table 1 shows the network security environment of each test object before and after the deployment on the smart campus security platform.

Table 1. Network Security Environment of Each Test Object Before and After the Deployment on the Smart Campus Security Platform

Zone	Pre-deployment Scheme		Post-deployment Scheme
W Zone	Traditional firewall+Intrusion Prevention System+Intrusion Detection System		Border AI Firewall+Threat Intelligence Center
D Zone	Database Firewall+Database Audit System		Virtual Intelligent Firewall+Database Audit System+Security Code Guard
H Zone	H1	Anti-virus System+Security Guard	Anti-virus System+Trusted Browser+Terminal Environment Awareness System
	H2	Anti-virus System+Security Guard	Mobile Environment Awareness System+Mobile Application Self-protection System
	H3	Traditional Firewall+Wireless AP Policy	Wireless Intrusion Prevention System+Wireless AP Security Policy
B Zone	Traditional Firewall+Unified Identity Authentication System		Trusted Application Agent Platform+User Behavior Analysis System+Privacy Guard
DMZ Zone	Firewall+WAF+Email Threat Detection System+Webpage Tamper-proof System		WEB Firewall+Website Security Cloud Protection System+Email Threat Awareness System

5.2 Test Data

To test the security performance of the smart campus, four attack routes were designed, and different attack modes were adopted for the simulation test [4], as shown in Table 2.

5.3 The Test Results Analysis of Simulated Attack

Different times of cyclic attacks were adopted, and the attack data capture was completed through a security device management system to reach the condition of each node on the attack route. Take the attacker as the first node, and the test results of each route are shown in Fig. 1, 2, 3 and 4.

Before the deployment of the security platform, the Web server-side received attack information when the penetration was launched by 500 times, but after the deployment of the security platform, the attackers failed to pass the boundary AI firewall, though 1,500 cycles of penetration were launched, as shown in Fig. 1.

Table 2. Security Performance Test Data of Smart Campus

No	Attack Target	Attack Rout	Number of Nodes	Simulated Attack Mode
1	WEB Server	Attacker - Internet - F1-web	4	WEB Penetration
2	B1Application System	Attacker - Internet -F1-W1-W2-W3-F3-B1	7	Distributed Denial of Service (DDOS) Attack
3	D1 Database	Attacker - Internet -W1-W2-W3-F2-D1	7	Vulnerability Scan
4	H1 Host	Attacker - Internet -W1-W2-W3-F2-H1	7	Virus Attack

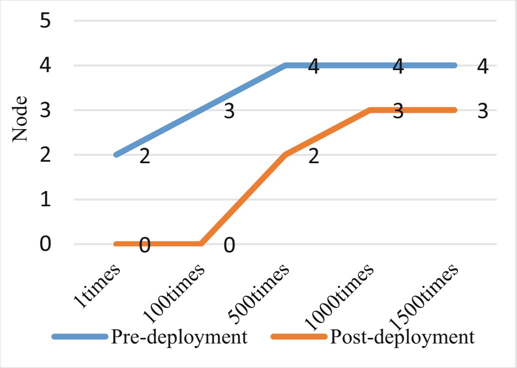

Fig. 1. Test Result of Route 1

Before the deployment of the security platform, the core switch W3 received attack information when the DDOS was attacked 100 times, and the target system B1 was breached when the number increased to 500. The target application system broke down under 100 attacks. But after the deployment of the security platform, the boundary AI firewall was not breached under 1,500 attacks, as shown in Fig. 2.

Before the deployment of the security platform, the firewall in zone D received attack information when the vulnerability scanning was launched by 100 times and was breached when the number reached 500 times. The D1 server received attack information and crushed the number rose to 1,000. However, after the deployment of the security platform, F3 did not receive the attack information until the Vulnerability Scanning was launched by 1,500 times, and it had been effectively defending against the attack, as shown in Fig. 3.

Before the deployment of the security platform, the firewall in zone H received the attack information when the virus attack was launched by 100 times and was breached under 500 attacks; the H1 host received the attack information and was infected under

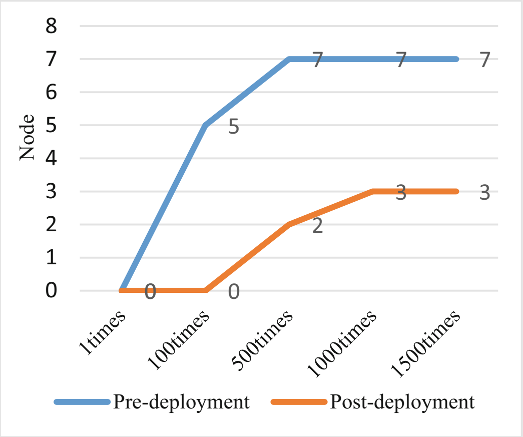

Fig. 2. Test Result of Route 2

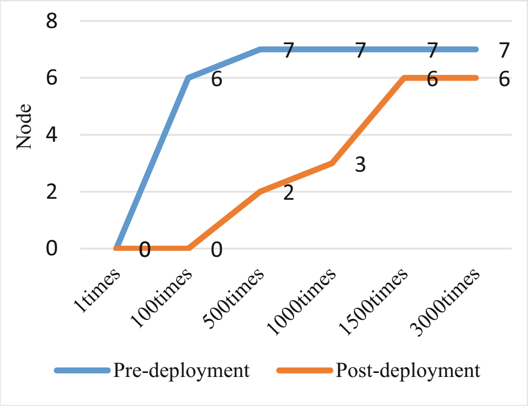

Fig. 3. Test Result of Route 3

1,000 attacks. However, after the deployment of the security platform, W1 only received attack information when it was under 1,000 attacks; F4 received attack information only after 1,500 attacks and had been effectively defensive; H1 was not infected, as shown in Fig. 4.

It can be seen that after the deployment of the smart campus security platform, key areas and critical devices' capability in security defense on the smart campus is significantly enhanced and tends to be stable after a cycling attack.

5.4 Test Results and Analysis of Security Risk

To conduct the smart campus security risk assessment before and after the deployment of the smart campus security platform, the open vulnerability assessment system (OpenVAS) was used to scan the vulnerabilities of all servers and hosts on all routes for

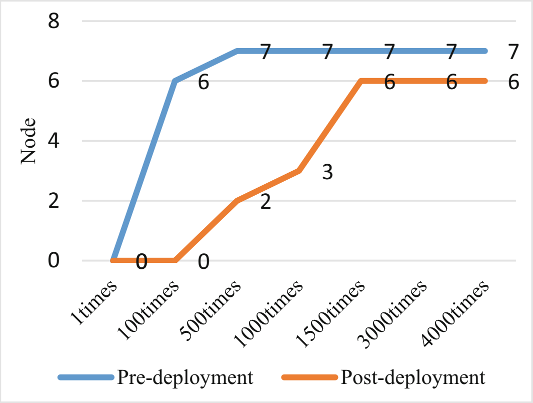

Fig. 4. Test Result of Route 4

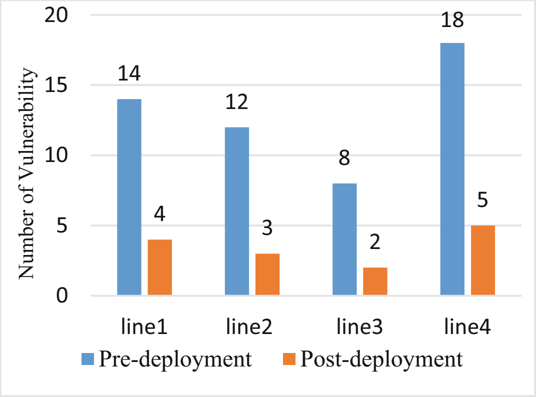

Fig. 5. Test Results and Analysis Diagram

vulnerability information of each key bug, as shown in Fig. 5. The assessment results illustrate that the overall number of vulnerabilities is significantly reduced after the deployment of the smart campus security platform, and the smart campus security level is greatly improved.

6 Conclusions

To meet the requirement of smart campus security applications, a design scheme of smart campus security management and control platform based on big data technology was proposed. According to the characteristics of each layer in the smart campus system, the security protection mechanism was set to deploy sensors at every layer and flow measuring probes in the key network ports to collect log data and behavioral data such as equipment, systems, attacker, network, and user. Big data technology was adopted to analyze data fusion, handle security threats timely, predict the security risks of smart campuses, and fully sense the security situation. After nearly one year's practical application data analysis of the intelligent operation and management platform, the timeliness of security risk alarms and the self-disposal ability have been significantly enhanced, promoting the further construction and application of the smart campus. In the later stage, the technologies of smart campus security data fusion and data association processing will be further studied and then combined with situational awareness technology to make the smart campus more effective in processing and analyzing all kinds of complex security data, thus truly realizing total awareness of the smart campus security situation in real time.

References

1. Franke, U., and J. Brynielsson. 2014. Cyber situational awareness: A systematic review of the literature. *Computers & Security* 46: 18–31.
2. Gong, J., X.D. Zang, Q. Su, et al. 2017. Review of network security situation awareness. *Journal of Software* 28 (4): 1010–1026.
3. Huang, L.F. 2020. Research on the cyber security management strategy of universities under the background of big data. *Research on Vocational Education* 5: 37–41.
4. Jin, Z.G., X.J. Wang, G. Li, et al. 2021. The generation method of network defense strategy integrated with attack graph and game model. *Information Network Security* 21 (1): 1–9.
5. Shelar, D., and S. Amin. 2017. Security assessment of electricity distribution networks under DER node compromises. *IEEE Transactions on Control of Network Systems* 4 (1): 23–36.
6. Wang, Z.G., Y. Lum, and X. Li. 2020. Active defense strategy selection of military information network based on incomplete information game. *ACTA Armamentarii* 41 (3): 608–617.
7. Zhang, B. 2019. *Design and Realization of Educational Administration Management System of Open University*. Changsha: Hunan University.