[1]Kexun He
[2,*]Qiang Zhang
[3]Baizheng Wang

Research and Application of Active Security Protection Methods for Automotive Cloud

Journal of Electrical Systems

Abstract: - With the gradual maturity of the Internet of vehicles and cloud computing industry and the continuous evolution of network attack forms, the demand for cloud security in the automotive industry will increase year by year. In the automobile cloud platform environment, because the traditional security scheme is still effective for the north-south traffic, the security problem of the automobile cloud platform mainly lies in the security protection of the east-west traffic of the platform and the division of the security boundary. The purpose of this project is to solve the security risk of east-west cross-subnet traffic of the automobile cloud platform, especially the traffic security problem between hosts, in order to provide the next generation firewall, intrusion prevention and other professional security protection functions for the virtual network environment without affecting the service virtual machine. In order to achieve the above purpose, it is necessary to solve the problem of virtual switch diversion and virtual machine drift on the cloud platform, study the service security requirements of the automotive cloud platform, the relationship between data transfer and processing on the cloud platform, and finally provide a prototype system of active security protection for the cloud platform risks. The system implements VM microisolation, network attack defense, malicious code defense, ip address-based secure access policies, application-type secure access policies, and VM migration security functions in cloud application scenarios.

Keywords: Cybersecurity, Automotive Cloud, Attack Traffic, Protection Method.

I. INTRODUCTION

With the acceleration of enterprise cloud steps, the gradual expansion of the mature application field of computing industry and the continuous evolution of network attack forms, China's political and business demand for cloud security will increase year by year. At present, cloud computing mainly covers the government, finance, transportation, telecommunications and other industries with a wide range of influence and high data confidentiality. These data are private and extensive, and once leaked, it will have a huge impact on the national economic and financial security and people's livelihood.

In 2017, Cloudflare was found to have leaked encrypted data from Https web sessions of cloud users for several months, affecting an estimated 2 million websites. In 2019, a well-known domestic cloud service provider code leak incident involved more than 200 projects from 40 enterprises, and even affected user privacy sensitive data. This matter also caused the "Internal debate", that is, the internal permissions are open within the company or open to the entire cloud effect platform, different enterprises have different understandings, but ultimately caused the source code leak. These security problems have brought huge losses to cloud computing users, cloud computing service providers, and even the country, and the importance of cloud computing security has also been rising [1].

Many enterprises have been on the cloud, cloud computing security needs are urgent, potential space is huge, is the birth of a new market blue ocean. According to the latest forecast released by Gartner, the growth rate of the cloud computing security services market will be higher than the overall growth rate of the information security market, and the global cloud computing security services will maintain a strong growth momentum. In 2021, China's cloud security market is expected to exceed 10 billion. By 2022, the market for cloud security services will reach $12 billion.

In the case of cloud becoming a trend, the attack pattern is more serious. With the continuous expansion of the cloud computing market, the security problems it faces are also increasing. In addition to traditional security issues, it also faces new security challenges brought about by cloud computing scenarios. In traditional home networks or enterprise networks, attackers enter layer by layer from the outside to the inside according to the assets and services exposed by the target, using a relatively fixed attack path [2]. However, on the cloud platform, security problems such as DDoS, intrusion and virus in the traditional network architecture are not only normal problems [3]. New security problems such as virtual machine escape, resource abuse and horizontal penetration for cloud platform architecture also emerge in an endless stream. Moreover, due to the characteristics of low cost, high convenience

[1] CATARC Automotive Test Center (Tianjin) Co., Ltd, Tianjin, China
[2] CATARC Automotive Test Center (Tianjin) Co., Ltd, Tianjin, China
[3] CATARC Automotive Test Center (Tianjin) Co., Ltd, Tianjin, China
*Corresponding author: Qiang Zhang

and good scalability of cloud services, using cloud to provide services or resources to attack other targets has become a new security problem [4].

The following problems are prominent in the cloud computing environment:

A. Dynamic Security Issues

One of the benefits of cloud computing to users is elastic expansion, for which the cloud platform will provide DRS (distributed resource allocation), HA (high availability) and other mechanisms. These mechanisms ensure that VMS can dynamically "drift" in the data center cluster at any time. For example, if the resources of a host are overloaded, the system can migrate some VMS to other hosts in real time under the deployment of the above mechanism, so as to alleviate the resource shortage problem of the overloaded host, and thus avoid the performance and even downtime of the virtual machine caused by insufficient resources. This mechanism of the cloud platform is obviously important to ensure the reliable operation of the business, but from a security perspective, this drift of the cloud environment has brought new challenges to security products such as firewalls. Take the firewall as an example. The firewall defines security policies based on security zones, which are statically configured on network interfaces. In this case, when a service VM is migrated from one host to another, the original security policies of the firewall may become invalid.

B. Visualization of Traffic and Threats

Because most of the traffic is in the data center or even in a host, traditional network audit and traffic analysis products are difficult to play a role. In the event of attacks and malicious traffic, the administrator cannot detect security events in the first place. As a result, the malware spreads horizontally to infect more networks, that is, nodes. Once an APT attack is caused, the loss of users is incalculable [5].

C. The Failure of Traditional Security Boundary Demarcation

With the rapid development and application of cloud computing technology, the traditional idea of dividing security zone boundaries around physical hosts and networks is no longer applicable, and traditional security vendors and cloud environments face great security protection challenges, mainly as follows:

a) The traditional security zone is enlarged: The application of computing and network virtualization technologies, as well as the construction of cloud computing centers, mostly follow the construction idea of microservices and large layer 2, so that dozens or even hundreds of virtual machines coexist on a layer 2 network, and the security zone boundary is magnified tens or hundreds of times. b) Difficult threat discovery and location: the traffic in the cloud is invisible, the threat detection in the security zone boundary is difficult, and the threat cannot be effectively located from the outside [6]. c) Blurred boundary and difficult to block: the migration of virtual machines from different physical hosts makes it difficult to divide traditional boundaries, and it is difficult for traditional technical means to effectively block attacks among virtual machines within the security zone. After a single virtual machine is captured, it is very easy to rapidly expand computing, resulting in "swarm death and swarm injury" [7].

In recent years, a number of domestic and foreign security vendors have launched virtual network security technologies and products [8]. In summary, most of them are still based on the traditional border defense idea, and the firewall is run in the cloud computing environment after virtualization, which cannot solve the security challenges faced by virtual machines [9]. However, cloud computing vendors have no responsibility and obligation to provide complete virtual network boundary protection measures for tenant applications, and tenants often take the initiative to seek security solutions after suffering network attacks. Existing solutions all require tenants to purchase related products and services from cloud computing vendors at a high cost [10].

Providing virtual boundary security protection technologies and solutions for tenant applications is still the most urgent need in the field of cloud computing security. To sum up, whether from the perspective of security requirements themselves or compliance, it is necessary to provide more perfect security solutions for cloud computing services.

From the above analysis, we can see that in the cloud computing environment, the traditional security solution is still effective for north-south traffic. Therefore, the cloud security problem mainly lies in the security protection of east-west traffic and the division of security boundaries. To this end, this paper is based on solving the following problems:

1) Solve the security risk of east-west cross-subnet traffic, especially the traffic security problem between hosts. This section describes how to provide professional security protection functions, such as next-generation firewalls and intrusion prevention, for virtual network environments without affecting service VMS. It mainly involves how

to divert traffic to the safety net element. Supports east-west traffic visualization, including traffic characteristics and threat display. Application traffic identification and statistics, threat analysis and display.

2) Learn and display asset information such as physical servers, VMS, and networks in the hypervisor to provide effective guidance for tenants to divide security domains. Set access control rules at the boundaries of network zones at different levels of virtual networks, and allow cloud service customers to set access control policies between different virtual machines. Controls all data communication between VMS and between VMS and physical machines. In addition, ensure that the access control policy is migrated with the VM.

The front-end data of X-ray energy spectrum is millivolt voltage pulse sequence, the pulse width of the sequence is microsecond level. But the amplitude and number of the pulse sequence contains the is sed system is FPGA as the control core. The data acquisition and processing system is composed of program control amplifier (PCA), A/D converter, FPGA unit, MCU unit and FIFO interface unit. The system block diagram is shown in Figure 1.

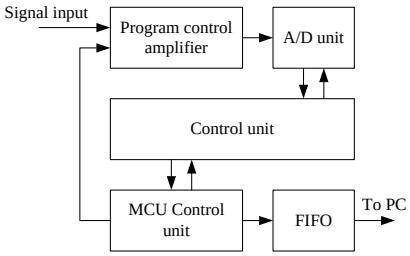

Figure 1: The System Block Diagram

II. SECURITY REQUIREMENTS ANALYSIS OF VEHICLE CLOUD PLATFORM

From the perspective of management mode, the traditional IT system usually has a unique operating unit, so that there is a clear division of security responsibilities between the system provider and the user, and once the system has a security risk or security incident, there will be a clear person responsible for handling. In this service-oriented mode of cloud computing, the entire IT system will face the relationship between cloud service providers, cloud tenants and cloud users. How to clarify their respective responsibilities is an important premise to ensure the security of cloud computing systems.

From a technical point of view, first of all, cloud computing uses resource pooling to provide services for users, and users' computing, storage, network and other resources can be dynamically expanded and contracted according to specific needs, so that the traditional way of centralized security investment is difficult to meet the on-demand expansion needs of cloud computing resources. Secondly, the cloud computing environment is a highly self-made ecosystem, and usually the IP address, gateway and other elements of the service virtual machine are automatically allocated by the cloud platform after the startup. Firewall and other gateway devices cannot provide security protection by acting as the gateway of the protected network node, which involves the problem of how to do traffic traction.

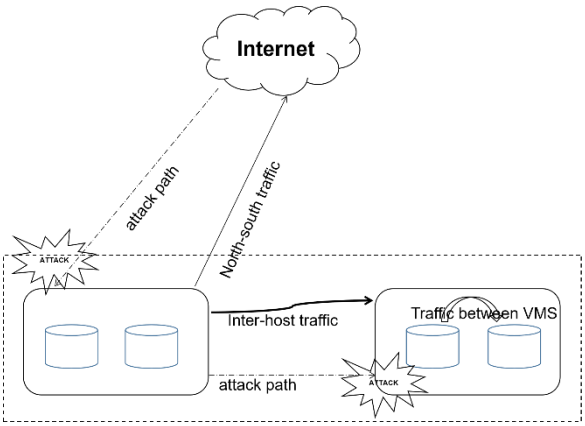

Figure 2: The principle block diagram of the Programmable amplifier

From the perspective of traditional data center security protection, usually security devices provide protection capabilities, including scanning (such as system leakage, Web leakage, configuration verification, etc.) security services and gateway (such as firewall, intrusion prevention, intrusion detection, etc.) security services. For the security protection of services in virtualized environments such as cloud computing, have the protection

requirements changed? What is the difference between the security protection of a virtualized environment and that of a traditional data center.

Through the actual testing and analysis of two cloud platforms, this study studied the security protection technology of traditional data centers and the virtualization security protection technology based on cloud computing, and analyzed the requirements of business for security protection. In the virtualization environment, service traffic is more complex and attack defense methods are more diversified and complex.

In Figure 2, the main three types of traffic and typical attack modes are shown:

a) North-South traffic: traffic accessing the public network, which is usually referred to as north-south traffic;

b) East-West traffic: access traffic between different hosts/subnets, and traffic between different VMS in the same subnet;

c) Malicious traffic: Attacks are usually launched from the Internet. Once a VM is compromised, the VM becomes a meat machine, and the threat spreads horizontally within the Layer 2 network to infect more machines.

For North-South traffic, security deployment is relatively simple. You can deploy security devices at the entrance of the data center to implement access control between the public network and Intranet. The security device can be a traditional hardware box or a virtual security device VM. As shown in Fig. 4, North-South Traffic Protection.

For east-west traffic, it is more challenging. In a cloud computing environment, computing resources (virtual machines) are highly centralized and dynamically migrated, and it is easy to cross established security boundaries, which makes the traditional physical environment based on network topology division of management areas no longer applicable. Moreover, once the boundary protection is breached, malicious code such as worms can easily spread from the infected machine to other machines in the area, so that the attacker can freely invade other machines, and then evolve into APT attacks, causing greater damage.

Traditional hardware box devices are difficult to deploy into the user's cloud platform, so its protection against east-west traffic is somewhat difficult.

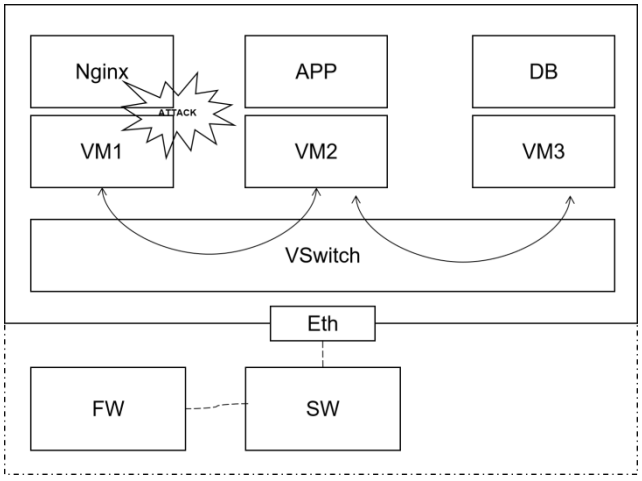

Figure 3: Intra-subnet Traffic

As Figure 3 shows, in a virtualized environment, existing physical security mechanisms may not detect malicious attacks at all. As shown in the following figure, VM1 and VM1 are two virtual hosts with the same tenant and subnet on the same physical host. Therefore, the communication between VM1, vSwitch, and VM1 exists only between VM1 and VM1, and the traffic does not go out to the host at all. Therefore, malicious traffic cannot be identified by external security devices.

Even if VM1 and VM2 are not on the same host, traffic flows through the external firewall device during communication. However, physical hosts are generally connected through tunnels. If the firewall is simply deployed on one side of the physical switch, it can only see packets from VM1 to VM2, but cannot remove the header of the tunnel to parse the real traffic from VM1 to VM2.

From the perspective of application business model, based on the existing mechanism of cloud service providers, the following access control Settings are studied through security groups, as shown in Figure 4.

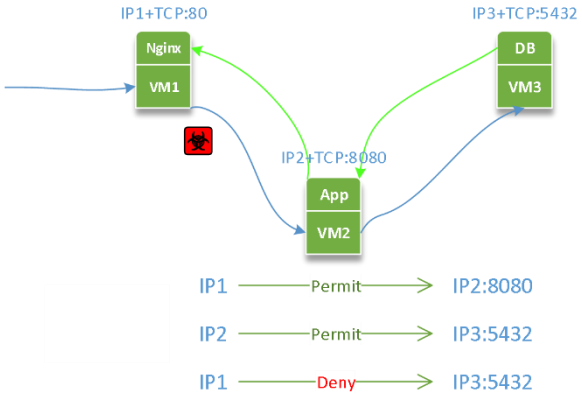

Figure 4: Intra-subnet Traffic

The configuration controls the access between the three nodes at the network level, but cannot filter out the malicious traffic. For example, after the attacker controls the Nginx node through malicious code, he discovers the open service interface of the App by scanning it, and then exploits the App node through system vulnerabilities or password cracking, etc., and then he can perform "delibrary" operation for the database, and then obtain the most core database data of the system.

Through the study of virtual cloud computing network, this study developed a risk probe to detect the traffic status of virtual machines in the original environment and see through the security risks in the interactive traffic of virtual machines.

III. Cloud Platform Risk Identification and Active Security Protection Methods

There are usually two ideas for east-west traffic protection: one is to put security equipment into the cloud platform for protection; The other is to export the service traffic inside the cloud platform, clean the security device, and then inject it back to the cloud platform. The latter method has a large network delay, and for the east-west traffic between VMS on the same subnet, the traffic between two nodes with a very close path is pulled to the outside in a "barbaric" way, which is particularly cumbersome.

This involves two key technologies: traffic diversion and security domain definition. Drainage is how to direct the flow to the safety device; The definition of a security domain refers to how to define a security domain based on the dynamic changes of assets in the cloud environment, so that you can set security policies for the security domain.

This study inserted a traffic diversion module through the interface provided by the cloud platform to study the security flow of traffic from the service virtual machine (VM1 in Fig. 4). The specific drainage process is as follows:

a) Service VM1 is connected to the virtual switch vSwitch, and then connected to the external hardware switch through the virtual NIC and physical NIC, as shown in mark 1 in Figure 4.

b) After the traffic diversion module is added, the traffic of VM1 is diverted to the secure virtual machine through the traffic diversion module under the control of the security management center by operating the API of the cloud platform. The security virtual machine filters the traffic according to the security policy issued by the security management center, as shown in tags (2) and (3).

c) After traffic filtering on secure VMS, malicious traffic entering and leaving service VMS is cleared to protect service VMS and virtual networks.

For security domain definition, microisolation technology is introduced. Microisolation abandons the traditional concept of security domains. Instead, security boundaries can be dynamically adjusted to meet the requirements of the service system. Security boundaries can even be focused on the single-machine level, and security policies can be deployed on a single virtual machine, greatly narrowing the scope of security protection areas. In this way, even if a VM (virtual machine) is infected with malicious code, because the virtual machine inside the network is in a protected state, it can effectively prevent the further spread of malicious code. In the micro-isolation architecture, a logical protection module is deployed for each service VM. When a VM is migrated to another physical host, the security policies related to the VM will be migrated synchronously.

On the secure virtual machine, you can enrich security function modules based on actual services to meet diversified security requirements. The security module is built-in on the virtual machine. The following is the security stack of the security module:

Intrusion prevention technology. By analyzing application-layer traffic anomalies, the intrusion prevention module can accurately detect and block all kinds of malicious network attacks, including overflow attacks, denial of service, Trojan horses, worms, and system vulnerabilities.

Apply control technology. Unlike traditional security devices that can only identify ports and IP addresses, the application control module supports fine-grained identification and control based on applications, users, and content through the industry-leading DPI intelligent identification technology. At present, more than 2,500 kinds of Internet applications have been identified, which can fully and accurately control various applications such as office, social, P2P, instant messaging, and entertainment. Combined with the filtering technology based on page content and URL, it can help users effectively implement online behavior management.

Malicious program detection technology. The network-level virus protection function can effectively detect and kill threats such as Trojan horses, botnets, and vulnerability attacks to prevent virus intrusion on virtualization platforms. If the host on the platform is infected with viruses or Trojan horses, the system detects the traffic when the viruses or Trojan horses attempt to communicate with the external network, blocks the traffic according to the policy, and logs the traffic. Cloud security protection software provides network virus protection function, from the way of virus transmission to HTTP, FTP, SMTP, POP3 and other protocol traffic to kill viruses, can also kill the virus in the compressed package (zip, rar, etc.), built-in massive level virus samples to ensure the killing effect.

Traffic visualization. The security management center collects and analyzes data communication between VMS, including traffic between different port groups. At the same time, it can also show users the new traffic in the cloud platform within a specified period of time, helping users to grasp the subtle changes in the cloud. By using the deep visualization technology, the security system can identify specific application types in VM traffic and provide traffic and application control functions to perform fine-grained permission control on service access between VMS to filter out unauthorized access and protect service security.

In the cloud internal visualization, the deep visualization feature of the security system can display fine-grained virtual machine visualization models, such as real-time traffic, application ranking statistics, IP address ranking, system logs, and IPS logs. Once a service VM is attacked, the system can respond immediately and take emergency measures to ensure high service availability.

IV. TEST AND VERIFICATION

A TCI/ IP-based network test environment with multiple network segments is composed of multiple VMware cloud computing platform devices running different application services and active security protection system running in the cloud computing platform.

The topology for the test validation is as follows in Figure 5: It consists of three host groups and a test machine.

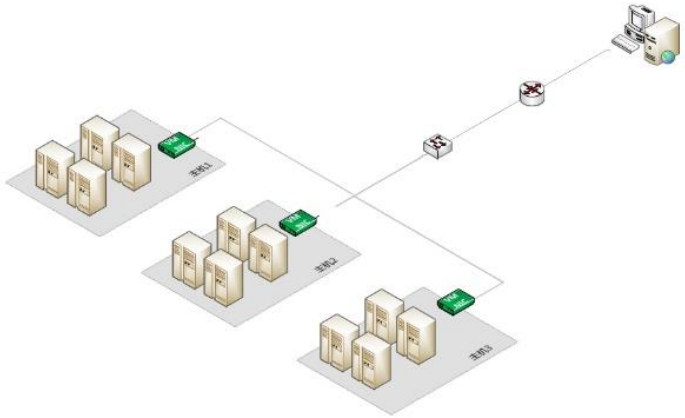

Figure 5: Basic Function Test Topology

In this study, simulation verification method was adopted to test and verify the host simulation attack events and attack traffic, which were respectively applied to hosts with and without the protection method in this study to check the response of hosts to the attack method. The test contents used in this study include Threat prevention, DOS attack defense, Malicious code protection, access policy and safety audit. After the test, the security

configuration and service impact of the two hosts are analyzed to determine whether the vehicle can withstand the attack of the North-South traffic.

The main test contents and results are shown in Table 1.

Table 1: Test Verification Results

Proof scheme	Main content	Result
Threat prevention	Vm microisolation protection and basic packet filtering protection	Add protection to VMS Access policies are configured for active and normal security protection
DOS attack defense	Test whether the active security protection system has alarms after adding protection	The DoS protection configuration is correct, the test script is executed between virtual machines, and the active security protection system has alarms
Malicious code protection	Antivirus FTP inbound, FTP Outbound, HTTP inbound, IPS inbound, IPS Outbound, and Application control	Malicious code protected VM application traffic is identified and protected
Access policy	Policy topology and traffic display	The security policy topology and traffic diagram are displayed
Safety audit	Test whether logging and log maintenance are available	The active security protection system supports multiple types of alarms and complete log information

According to the test, active security protection system is a distributed security gateway system for cloud computing platform. Professional traffic diversion technology pulls service VM traffic to the Virtual Security Protection module (vSPM), detects and blocks security threats to east-west traffic, prevents attacks from spreading across the cloud platform, and integrates multiple cutting-edge security technologies, such as DoS/DDoS attack defense, intrusion prevention, application protocol identification and control. At the same time, the virtual security management module (vSMC) realizes the visualization of the internal traffic and application of the cloud platform. The maximum number of VMS is 1000. Intrusion prevention throughput ≥1Gbps; Maximum number of concurrent connections ≥1 million; The number of new http connections per second is at least 50,000. The architecture design that separates the management plane from the service plane perfectly supports VM migration in the cloud to achieve dynamic and real-time security protection. Provides users with security solutions in virtualization and cloud computing environments.

V. Conclusion

This paper reveals the mechanism and law of vehicle cloud security, studies the dependency relationship of cloud platform services, analyzes the security risks of cloud platform, builds the threat model of cloud platform, and breakthroughs in solving key common technical problems such as service dependence and data interaction security of existing connected vehicles in cloud security. The project is expected to achieve key technological breakthroughs in the field of cloud security through the cross-integration of multi-disciplinary technologies. The application of basic theories and key technologies of this project will be widely used in the research and development and design of domestic vehicle networking cloud platform, improve product quality, promote industrial optimization and upgrading, and enhance industrial competitiveness, which has huge social and economic value.

References

[1] Abdullayeva F. Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization, 2023, 12: 100268.

[2] Younis Y A, Kifayat K. Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep, 2013: 599-610.

[3] Yang fei, Hong yun. Research on the construction of cloud computing network information security protection system. omniscient, 2022, 4(5): 74-76.

[4] Ke L. Network information security technology based on cloud computing environment. Journal of Electronics and Information Science, 2023, 8(2): 57-62.

[5] Wang qi. The application of total traffic analysis technology in network threat perception and security incident response. 2019 Proceedings of the China Network Security Hierarchical Protection and Critical Information Infrastructure Protection Conference, 2019.

[6] Yaoqi. Research and application of regional boundary protection model based on trusted computing. Information Security and Technology, 2010 (6): 71-75.

[7] Sheik S A, Muniyandi A P. Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. Cyber Security and Applications, 2023, 1: 100002.

[8] Burkacky O, Deichmann J, Doll G, et al. Rethinking car software and electronics architecture. McKinsey & Company, 2018: 11.

[9] Tan H, Choi D, Kim P, et al. Comments on “dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks”. IEEE Transactions on Intelligent Transportation Systems, 2017, 19(7): 2149-2151.

[10] Kaplan E. D., Hegarty C. J. Understanding GPS: Principles and Applications[M], 2nd ed.,Artech House, 2006.