Research on Information Security Architecture of Aerospace Business Network for the Future

Hongyan Chen, Junwei Wan
Beijing Institute of Tracking and Telecommunications Technology, Beijing 100094, China
child_smile@163.com

Abstract. In view of the new network security situation, this paper analyses the present situation of the information security system of the aerospace business network, and puts forward the main problems that need to be improved and perfected. In view of these main problems, the overall consideration of the future-oriented information security system architecture design of aerospace business network is put forward. It includes building dynamic defense model, unified trust infrastructure, network-wide security situational awareness and early warning capabilities. A new generation of security architecture is designed. Measures and suggestion for follow-up construction are put forward.

1. Introduction
At present, information cyberspace has a high strategic value and has become a profit-seeking target for terrorist organizations, hostile countries and various malicious people. Unlike the single-soldier operations of hackers, network attacks, with the support of some governments and business groups, have shown the trend of weaponization, specialization and teamwork, and have the destructive ability of destroying lifelines, breaking channels and controlling systems, which poses a serious threat to the key infrastructure of information network space.

1) Information cyberspace has become a new area of the country. At present, more than 40 countries have promulgated national cyberspace security strategies, including the United States Cyberspace Security Framework, the European Data Protection Reform Program, Japan's Cybersecurity Strategy and India's National Cybersecurity Strategy. All countries in the world regard information cyberspace as a new field of their country.

2) The battle between attack and defense in information cyberspace is fierce. Information cyberspace concerns the social stability, economic operation, technological development and national defense security of a country. It has high strategic value and is the profit-seeking target of terrorist organizations, hostile countries and various malicious people. With the support of some government and business groups, various specialized, high-level and easily disseminated cyber-attack weapons emerge in endlessly, which not only affects the information system, but also poses a serious threat to weapon platforms and key facilities. The game against cyberspace is becoming increasingly fierce.

3) Weaponization of Network Attacks. At present, cyberspace attack is developing towards weaponization. Major countries vigorously develop cyberspace combat capability, and superconventional cyberspace combat weapons emerge in endlessly. The U.S. Army has developed more than 2000 kinds of network weapons, including computer viruses, computer hackers, electromagnetic pulses, electronic biology and so on. Network attack weapons usually lurk in the backdoor or preset code of computing components, storage components and operating systems. After
network start-up, they carry out organized and large-scale network security threats. Cyber attack weapons are cyber attacks aimed at the destruction of key national infrastructure. For example, the "seismic network" virus attacks the Iranian nuclear facilities, the "toxic zone" virus attacks the data of the Iranian industrial control system, and the "flame" virus attacks the commercial intelligence system of the Iranian petroleum sector. The destructive capability of these cyber-attack weapons seriously affects the military, political and economic security of the country.

2. Current Situation and Deficiencies of Safety System

Space business network is responsible for the organization and command of space missions, test launching and recovery tests, on-orbit management, test and processing and application of spacecraft information. The system mainly consists of spacecraft, Mission Center (command and control center, measurement and control center, operation and control center and application center), external networking system, measurement and control equipment and network infrastructure. Existing security protection measures are mainly deployed in different links such as aircraft, equipment, communication network and mission center. They provide encrypted space-ground information transmission, security isolation between uncontrolled networks, access control and detection of ground wide area network, user identity authentication and authorization, host input-output control, software system security, data storage security and so on. Functions, through the combination of technology and management, effectively guaranteed the previous test tasks.

With the promotion of new technologies such as cloud computing, Internet of Things, big data, and the increasing threat of network space such as information tampering, ATP attacks, covert channels, backdoor vulnerabilities, etc., the information security risk of aerospace business network is still severe due to various factors such as funds, management and so on. The main manifestations are as follows:

1) The phenomenon of safe islands is widespread. Although the security systems are deployed in the network, boundary and computing environment, they have different models, poor linkage of information sharing, self-management and no unified situational awareness and management capabilities.

2) The protective measures are incomplete. Restricted by funds, management departments and construction modes, some system security measures are not in place, which increases the security risk of system interconnection.

3) Static curing of protective capacity. Some of the protection strategies are too simple, and some fail to reset in time after the end of the mission. For fear of compatibility problems, some host protection systems are set to stop during the mission.

4) Insufficient integration with application system. The application of security protection at network and host level is good, but in identity authentication, application authorization and storage protection, the combination of application software and security protection system is not enough, and the fine-grained authorization, audit tracking and authority control are extensive.

5) Autonomous and controllable applications need to be strengthened. Nowadays, domestic equipment and self-controlled software systems have been widely used in the newly built systems. In the transitional period, a considerable number of non-domestic and non-self-controlled equipment and software have been applied.

3. Architecture Overall Design

3.1. Establishment of Dynamic Defense Model Adapting to Risk Change

At present, the construction of information security protection system mainly adopts hierarchical model, corresponding to OSI open interconnection model, taking corresponding security measures in physical layer, link layer, network layer, host layer, application layer and data layer to ensure the safe and stable operation of the system. The security risks need to be preset in advance, and the equipment and strategy are relatively fixed. For changing security threats, means and measures are often in a
passive state. In order to deal with the changing security threats, it is necessary to perceive early warning in advance, carry out risk analysis according to the threat of early warning, formulate protective measures, detect and locate security incidents, take timely disposal measures, restore system capabilities, conduct audit tracking when necessary, and adopt counterattack means to build a defense system with dynamic empowerment, as shown in Figure 1.

![Security Dynamic Defense Model](image)

**Fig. 1 Security Dynamic Defense Model**

### 3.2. Establishment of Network-wide Unified Trust Infrastructure

Establish a unified and ubiquitous security trust system covering many elements such as "personnel, equipment, information system". It is compatible with various types of identity authentication systems (including passwords, certificates, tokens, fingerprints, etc.). It realizes cross-domain and cross-system joint authentication, and provides basic support for the realization of network personnel, equipment, system name authentication, service controlled access, and message tracking. Ability.

Construct trusted network space covering "terminal, network, application and management" to shield malicious users from threat implantation. Based on the network trust transfer mechanism, the trust relationship is transferred to WAN. By deploying terminal trusted protection system, network trusted access system and software trusted management system, network trusted space can be created.

### 3.3. Strengthen the Construction of Network-wide Security Situation Awareness and Early Warning Capability

To deal with the new threats of organization, scale, complexity and concealment in cyberspace, we should strengthen the integration and linkage of network system integration and security system, enhance the ability of security detection and vulnerability analysis through vulnerability mining and analysis and prediction of attack behavior, and realize the visualization of security threats such as illegal operation, ultra vires access, data leakage, network intrusion and virus spread. Now, and has the ability of the whole network early warning.

### 3.4. Establishing the Security Architecture of "Service Oriented, Dynamic Enabling and System Linkage"

The security protection system of the new generation Aerospace service network consists of security service layer, security function layer and security application layer. The security service layer constructs the remote backstage of the protection system by the security infrastructure support and security capability pool. According to the front-end requirements, security services are continuously pushed to various security components of "network, cloud and client", and the corresponding security defense functions are dynamically assembled; Security application layer realizes system integration based on the protection function of "network, cloud and end", and constructs a defense system which integrates "monitoring, operation, maintenance, traceability and evaluation", as shown in Figure 2.
The terminal system includes computer terminals, handheld terminals, combat units and information systems such as control centers, foreign bases, foreign stations, newly transferred networks, spacecraft, TT&C equipment and other mission units. Depending on the cloud security capability pool, security devices supporting dynamic loading of security payload are deployed in the terminal system to form a "cloud + client" joint defense mechanism. Through cloud service capabilities, the problems of ubiquitous terminal technology updating, security resource constraints and static defense functions are solved. The trusted mechanism is introduced into the unified trust infrastructure to construct an end system with endogenous immunity capability.

Deploy security devices to support dynamic loading of security loads in communication networks, support dynamic loading of security loads, and form a "cloud + client" joint defense mechanism. Through cloud service capabilities, problems such as technical updates of network security devices, security resource constraints, static defense functions are solved. Trusted network is constructed using unified trust infrastructure to provide network credible authentication.

Through the integrated design with resource center, the Security Cloud Service Center is built by means of module embedding and service invocation, relying on the cloud security capability pool,
supporting the dynamic loading of security load, forming a "cloud + client" joint defense mechanism, and adapting to the service migration and scale deployment mechanism of cloud platform by means of dynamic empowerment.

4. Main measures and suggestions

1) Complete shortcomings, pilot verification, step-by-step implementation, and gradually build capacity

Focusing on some newly built transfer systems, we will supplement and deploy terminal security protective equipment, communication network security protective equipment, information service security protective equipment and security operation and maintenance equipment, and complete information security protective board, so as to enable it to have basic defensive capabilities and prevent single-point invasion by the enemy.

We will accelerate the development of pre-research, carry out safety pilot projects for some newly built systems, and verify the protective effectiveness of the new generation of security protection systems. Through upgrading and transformation, it is gradually extended to all information network areas.

2) Strengthen the Integration of Information Security Technology and Business Application

Business application function design and use mode should pay close attention to the relevant information security requirements, closely integrate their own needs to divide the security domain, and use various security services to customize fine-grained security defense strategies.

We will promote the independent and controllable construction and application of information systems, accelerate the migration of application systems to autonomous and controllable software and hardware platforms, and eliminate potential security risks caused by foreign-related equipment and software.

3) Strengthen the Linkage between Information Security Institutions and Business Application Departments

In the process of information system demonstration, design, construction and acceptance, business application design, use and management departments should strengthen their links with information security agencies, exchange information and avoid the lack of security design.

4) Strengthening the Construction of Information Security Specialty and Network Defense Force

Information security has the characteristics of strong professionalism and high requirement of technical reserve. The technical reserve and personnel allocation of the existing part-time information security operation and maintenance personnel in various units are difficult to support the existing security operation and peacekeeping security incident disposal, and can not meet the needs of network defense operations. It is necessary to strengthen the professional training of information security, cultivate and expand the network defense force formation.

5) Developing Civil-Military Integration to Support Security Operations and Peacekeeping Network Defense

Information security technology develops very fast. It is difficult to track the development of information attack and defense technology completely and effectively only relying on the professional forces of the army. Faced with the insufficiency of the ability to respond to the new network attack threat, it is suggested to introduce local professional forces in a feasible way to effectively enhance the ability of information security operation and peacekeeping and network defense.

5. Conclusion

At present, the reform of the compilation system has brought unprecedented opportunities for the development of space industry, and also puts forward higher requirements for the construction of information security system. Faced with the increasingly complex security situation, by building a security defense system that integrates "unified management, dynamic enabling, system compatibility, system linkage and security interconnection", we can eliminate the security isolated islands, realize the safety management objectives of early risk detection, early threat awareness, more timely protection
and more effective measures, and ensure the safety, controllable and efficient completion of various test tasks of the aerospace business network.

Acknowledgments
This work was financially supported by the Study on the Generation Mechanism of Multidimensional Information Scattering Field of Typical Ocean Targets of National Natural Science Foundation of China (61890965)

References
[1] Yuhong Jin. Research on Internet Financial Information Security Prevention and Guarantee System in Big Data Environment [J]. Information Science,2018,36(12):134-138.
[2] Xiaoheng Wang,Yongcang Yang. Construction and Application of Information Security and Secrecy Management System Documents in Military Enterprises [J].Information Security and Communications Privacy, 2018(11):44-50.
[3] Junwei WAN, Hongyan CHEN,Jing ZHAO. Application verification of cloud computing technology in real time space test mission area [J]. Netinfo Security,2017(05):63-68.
[4] Hui ZHAO, Junwei WAN etc.. Application Research of autonomous control technology in experimental task domain [J]. Journal of Spacecraft TT&C Technology,2015,34(02):109-114.
[5] Hongyan CHEN,Junwei WAN. Research on Application Model of Domestic Basic Software in High-Density Information Integrated Application System [J]. Modern Electronics Technique,2018,41(21):84-87+91.
[6] Hongyan Chen,Junwei Wan. Research and Application of Web-based Performance Optimization Scheme for Enterprise Websites [J]. Internet of Things Technologies,2018,8(02):67-69+73.
[7] Hongyan Chen,Junwei Wan,Qi Wang. Design and Implementation of High Performance Sorting Algorithms for Large Data [J]. Journal of Spacecraft TT&C Technology,2015,34(02):120-127.
[8] Junwei WAN,Hui ZHAO etc.. The development status and application analysis of autonomous controllable information technology [J]. Journal of Spacecraft TT&C Technology,2015,34(04):318-324
[9] Hongyan CHEN,Junwei WAN,Hongwei QI. Research on cloud smart office integrated management system solution based on Internet of things [J/OL]. Modern electronic technology,2018(10):85-89[2018-05-30].https://doi.org/10.16652/j.issn.1004-373x.2018.10.022.