Research and Design of Integrated Information Transmission System for Large Warships Formation

Nan Wang1, *, Yi Liu2

School of Computer Science, Wuhan Donghu University, Wuhan 430212, China

*Corresponding author’s e-mail: Wangnan9@tom.com

Abstract. The Navy is a comprehensive and highly integrated service consisting of submarines, surface ships, aviation forces, coastal defense forces and marines. The Navy is a systematic and technology-intensive military. Compared with other military services, the naval equipment requires higher system performance. The naval combat unit is mainly a fleet composed of several different fleets of warships and aircraft. Information warfare of naval fleet is divided into information level (network) attacks and defenses. In the future maritime information warfare, it is necessary to strengthen the defense capability of formation information warfare to ensure the security of communication and computer infrastructures. The integrated information transmission system of large naval fleet is designed to improve the information defense capability of naval operations. It has strong comprehensive defense capabilities of computer anti-reconnaissance, anti-jamming, anti-virus and anti-destruction. In the final analysis, it is to improve the security of computers.

1. Introduction

As the human society, the army has entered the information age, and the modern warfare has evolved into information warfare. Information warfare is an integrated warfare about land, sea, air, space and electricity, which takes the equipment platform of mechanized warfare as the main carrier. It uses the information weapon as the support, the information network as the center and the information advantage as the goal.

The goal of information warfare of naval fleet is to interconnect soldiers at tactical level; improve the security and reliability of the distributed database, and provide improved protection technology. Information systems may be attacked in many ways such as computer viruses, Trojan horse programs, Logic Bombs, Trap Doors and other methods.

Computers and their networks maintain national security, while most of the existing military general-purpose computers (including software) in China are imported, and a few self-designed vehicle-borne and ship-borne aircraft are basically copied (some use foreign block modules). The problems of that include: 1) Although the embedded computers of missile-borne, satellite-borne and airborne aircraft are self-designed, the main chips such as CPU and memory are imported; 2) Computer network products in many security systems are mainly purchased from the United States, and security technology falls behind them; 3) The information infrastructure of our army in construction lacks uniform security standards and norms, which is not reliable and perfect. Security design hardly considers countering information warfare attacks.

An effective method to solve the above problems is to build our army's reliable computing hardware platform on the basis of chips developed and manufactured by ourselves. Network node equipment in the army of that platform can be used and reliable computing network system of our
army can be constricted. Thus the reliable and safe operations of our army's operational command system can be ensured.

2. Functional Analysis of the Integrated Information Transmission System for Large Warships Formation

The integrated information transmission system of the large warships formation is a complete solution of the information security defense system of the naval fleet. For the navy, the network is a multimedia network. It can provide nearly continuous voice, video, data, text, graphics and image information to all naval vessels and command units at sea and coast. The security of information must be guaranteed. This system is designed for this purpose. Its specific functions are as follows:

- Ensure the user's unique identity, privileges, and integrity/availability of the workspace.
- Ensure confidentiality/integrity of storage, processing and transmission.
- Ensure the integrity of hardware environment configuration, operating system kernel, services and applications.

- Ensure the security of key operation and storage.
- Ensure that the system has immune capability and it can fundamentally prevent viruses and hackers.

3. Thoughts and Framework for the Implementation of Integrated Information Transmission System for Large Warship Formation

The integrated information transmission system of large naval fleet is based on the idea and standard of TCG. It has developed the trusted computing platform product independently, which takes the security control chip designed and developed by itself as the core, and develops the ESM module which is the trusted root of the platform. Its reliable computing platform is an independent system, which adapts to different platforms and operating systems. The reliable computing platform includes hardware and software.

3.1. Hardware system of the credible computer

The basic components of the hardware system of a credible computer include:

- ESM module with self-developed security control chip as the core;
- Dependable BIOS;
- Dependable transmission channel;
- Dependable Authentication Device (IC Card/Reader);
- Computer motherboard, etc.

ESM module can be integrated on the motherboard, and its security control chip is the core component of ESM. IC card is to identify users’ identities and store users’ identity information. Dependable BIOS is a code-level modification of ordinary BIOS and security enhancement.

As shown in Fig. 1 below, the hardware structure of the trusted computer platform of the integrated information transmission system for large naval formation is based on the computer motherboard, with the ESM module as the core and the external card reader as the core.
3.2. Credible computer software system

The software structure of credible computing platform is shown in Fig.2.

Among them, through the platform management center the central administrator will form the predefined security requirements and security policies into a security configuration file. Then the configuration is customized to a bare computer by the installation and maintenance program to make it a reliable computing platform. Security Enhanced Operating System/Secure Operating System provides users with a trusted operating environment. Through the collaboration of functions between the above components, a complete "reliable chain" and a "reliable environment" are established for trusted computing cryptography terminals.

4. Key Technologies of System Implementation

4.1. ESM Modular

ESM module is an embedded system, which consists of a hardware module and an embedded operating system with SOC chip as the core. As shown in Fig.3, the ESM module is the reliable root of the dependable computing cryptography platform, which provides trusted and secure support to the platform. ESM module is an independent operation system with CPU, with built-in cryptography algorithm. ESM module implements platform identity authentication, reliable authentication, reliable storage, I/O control, internal audit functions. The module provides data interface and logical channel of USB, GPIO, I2C and ISO.
4.2. CPK Technology

To solve the problem of large-scale key management and identity-based key distribution, the seed key algorithm and identity mapping algorithm which is a new key management algorithm must be constructed. The basic principle of seed key algorithm is to produce almost infinite key variables with a small number of seeds to meet the key management needs of almost infinite users. The following three seed key algorithms are introduced to meet the needs of different authentication environments. One is ECC combined public key algorithm (ECC CPK) based on ECC elliptic curve cryptography or LDC discrete logarithmic cryptography, the other one is LDC combined public key algorithm (LDC CPK) based on RSA, and the third one is CSK based on traditional symmetric key.

Among them, the construction of seed matrix is the extremely part of CPK technology. In general public key system, the public key of each user is published directly. If a user publishes a public key, an amount of users will publish an amount of keys. LDAP and other catalog stocks are usually used to store the public key for the relying party to invoke. When the number of users is large, the capacity of the catalog library is very large and the access speed is fast. Its design requires high quality which is highly difficult.

In the combined public key system (CPK), the public key of each user does not publish directly, but only publishes the seed matrix of the public key. The public key of each user is calculated by the seed matrix and the correlation mapping value. This is a new key management algorithm system in the basis of the original public key cryptography technology.

5. Solution of Integrated Information Transmission System for Large Warship Formation

The integrated information transmission system of large fleet of warships is a complete communication support platform for naval fleet, which is established by the trust chain of the whole trusted computer platform. As shown in Fig. 4, the main path of the trusted computer platform of this system is the original boot process of PC terminal. The reliable chain transfer process is composed of credible BIOS, ESM module, user card and the original boot process. After that the system is powered on, the credible BIOS and ESM modules on the motherboard start at the same time and the credible BIOS first gains the control of the CPU. The administrator card or user card is authenticated bidirectionally through the ESM module, while the credible BIOS and ESM modules also need to be authenticated bidirectionally. Then, credible BIOS performs trusted computation on master boot record, operating system loader and security enhancement operating system respectively, and gives the calculated summary value to ESM module for trusted verification. After the trusted verification is passed, CPU control will be transferred to the master boot record, the operating system loader and the security enhancement operating system in turn, thus a complete trusted chain is established.
Security Enhancement Operating System (SEOS) can authenticate the security configuration, system services and applications during operation, and establish a credible running environment for users. In the using process of users, the security enhancement operating system can control the system and user resources, network access, and the consistency verification and encryption and decryption protection of user data are also carried out. This ensures that the trusted environment will not be destroyed during the whole operation process.

6. Conclusion
In this paper, the design of integrated information transmission system for large-scale warships formation is proposed. The technology of dependable computer platform can provide the army with reliable hardware platforms, reliable operation systems and reliable applications. The trustworthiness of computing platform, the trustworthiness of operators and the trustworthiness of user behavior can be realized in a warship or a large-scale formation.

The core component of the reliable computing platform is that the security control chip can cooperate with various computer architectures to provide a trusted root and symmetric and asymmetric cryptography computing environment for computing devices. SOSCA architecture in security control chip can provide independent storage and instruction access control area, which is convenient for communication environment and computing environment to exchange different cryptography algorithms at different times. At the same time, cryptography algorithms in different areas of the chip can be upgraded and replaced in many methods, which can avoid the use of multiple encryption devices and strong binding between encryption devices and cryptography algorithms, thus less costs require for equipment management and maintenance.

When communicating in a warship or in a large formation, it is often necessary to confirm the identity of both sending and receiving parties. Using symmetric algorithm to confirm identity needs to store a lot of keys, and using asymmetric algorithm requires third party to provide identity certification. For the above reasons, the research and implementation of CPK cryptography management system need to be further studied in order to better solve problems about the key distribution and avoid the need for third party to participate in the authentication process. CPK technology can be used for communication transmission. Transport platform provides a more secure identity authentication solution.

References:
[1] Yong Yu, Changgeng Chen, Qiang Liu, Jiaxi Liu. Trust Guide Computer Network Collaborative Defense Model Based on Trust Type[J]. Netinfo Security. 2018(9).
[2] Beixiong Liu, Qiaoeling Xiao, Yi Zhang, Mengxiang Chen. Research on Network Password Security Transmission Based on Optimized Symmetric Encryption Algorithm[J]. China Computer & Communication. 2018(22).
[3] Hongchao Li. Research on cryptography Algorithm Recognition Based on cryptography Features[D]. Xidian University. 2018.
[4] Zheyu Qou, Ma Lianchuan. Research on the Test Method of Security Computer Communication Bus Based on Fault Injection[D]. Beijing Jiaotong University. 2018.

[5] Licheng Shi. Research on the Design Technology of Security IC Card Chip Based on Lightweight Password[D]. Strategic Support Force Information Engineering University. 2017.

[6] Qiaoping Liu, Bing Zhou, Wentao Wang. Research on Information Encryption and Network Identity Authentication Algorithm Based on Elliptic Curve[J]. Automation & Instrumentation 2016. (8)

[7] HaoXing Li, Fenghua Li, Chengeng Song, Yalong Yan. Data holding certification programme to support identification[J]. Journal on Communications. 2016(10)

[8] Janjun Guo. Design of Third Class Protection of Command and Control System of Ship Based on Credible Computing[J]. Command Information System and Technology. 2015(9)

[9] Mingdi Xu. A Review of Trust Chain Research in Trusted Systems[J]. Acta Electronica Sinica. 2014(17)

[10] Yu Sun. Introducing trusted chips to control risk structurally[J]. Information Security and Communications Privacy. 2014(9)

[11] Xiaoli Pei. Research on information security of shipborne information infrastructure[J]. Computer and Digital Engineering. 2014(8)

[12] Xiaolu Zhu, Qing Yang, Gefei Liu. Research and Design of an Encryption Algorithm Based on Identity Authentication Data[J]. Computer Engineering and Science. 2012(12).