Caltta

eChat PoC System Security White Paper

CONTENTS

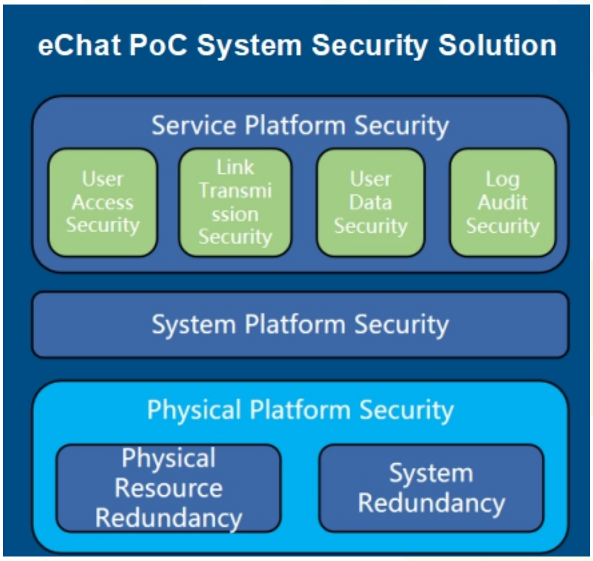
1 Security Overview

Private Mobile Radio (PMR) - sometimes also called Professional Mobile Radio - is a mobile communication system dedicated to users with sensitive requirements of safety, security and reliability (e.g. police, emergency services, private security, etc.). It is a dedicated wireless communication system developed to meet the needs of industry users for PTT command and dispatch, and is oriented to specific industry applications.

The traditional PMR systems, that is, "Push To Talk", have a long development history in the field of mobile communications. It is generally based on professional mobile communication technologies, such as narrow-band DMR system and broadband B-TrunC system. The characteristics of these systems are that users need to build and maintain dedicated wireless networks on their own to provide services such as voice calls and broadband/narrowband data services. With the rapid development of mobile Internet and the large-scale construction of global wireless cities, broadbandization has become the development trend of the entire wireless communications. Correspondingly, the PMR system is also developing in the direction of all-IP system, co-networking bearer, diversified services, broadband data, multi-mode terminals, and fully integrates the new and old communications systems to provide a wider coverage and deeper integration.

Therefore, Caltta's eChat PoC (Push-to-talk over Cellular) system came into being based on this command and dispatch scenario. More importantly, compared to traditional PMR networks, the eChat PoC system running on the public network poses a higher challenge to security.

Considering the public network features, the needs of users and the characteristics of our own products, Caltta puts security first in the entire system. eChat, Caltta's PoC communication system, provides the following security solution according to the bottom-up hierarchical architecture:


eChat PoC System Security Solution
Service Platform Security
User Access Security
Link Transmission Security
User Data Security
Log Audit Security
System Platform Security
Physical Platform Security
Physical Resource Redundancy
System Redundancy

2 Physical Platform Security

The security of physical equipment is the basis of the entire security system and the focus of customers' attention. Only the security of physical equipment is first guaranteed, then other security measures could be possible. The eChat system can be deployed flexibly, which can be deployed on both universal servers in the data center and various cloud platform servers. Different deployment methods use different physical security strategies, which can ensure the physical security of the entire system to a certain extent, eliminate single-point failure of equipment and provide service continuity.

2.1 Physical Resource Redundancy

For universal server deployment:

- The universal server system needs to provide redundant hardware that supports reliability guarantee. For example: dual power module access, RAID configuration of hard disk and other storage resources, network access via dual NIC, and so on;

- For the RAID configuration of storage resources such as hard disks, different redundancy capabilities need to be configured according to different service needs. For eChat service processing server, configure at least 2 hard disks as RAID1; for eChat storage server, configure multiple hard disks as RAID5 to provide data redundancy processing capability;

- Server network interface redundancy. For example: Aggregate configuration for server NIC to improve redundant processing capability. In special cases, specific network ports can be designated for specific services according to different processing services;
- Network communication equipment redundancy. For example, in order to provide reliable transmission of communication networks, routers, switches, firewalls and other equipment can be configured with redundant hardware according to specific project requirements to form a dual-network dual-plane network architecture to ensure network redundancy and smoothness;

For cloud platform server deployment:

- For the deployment of cloud servers, you need to deploy different cloud servers that have a backup or load sharing relationship in different physical available zones of the cloud platform to avoid deploying all cloud servers in the same physical available zone.
- The cloud service provider needs to be able to provide physical reliability guarantee for the cloud disks. During actual deployment, the cloud disks can be redundantly configured according to the requirement and the actual support of the cloud platform.
- For storage resources such as system disks and data disks of cloud servers, you need to create snapshot storage backups. You can use different scheduled backup strategies according to different needs.

2.2 System Redundancy

In addition to the redundancy of physical resources, redundancy at the entire system level is also a very important guarantee for the security of the eChat system. The eChat system supports local disaster recovery backup and geography disaster recovery backup functions.

- **Local disaster recovery backup**

When the eChat system is deployed on universal servers of a local data center, it can form a local disaster recovery system by using the system software deployed on multiple universal servers via Cluster software. The local disaster recovery system can realize automatic switching of the servers in the eChat system. Meanwhile, a unique set of eChat service system is presented externally, which can largely eliminate the hidden danger of single-point service failure of the universal servers.

- **Manual geography disaster recovery backup**

Whether the eChat system is deployed using universal servers of a local data center or servers of a cloud platform, it can support manual geography disaster recovery and backup functions.

Manual geography disaster recovery backup function needs to deploy a backup set of the same eChat system in a remote location. The backup system synchronizes the database of the main system regularly every day, and at the same time, the terminal uses the domain name to access the eChat system. When the main system fails, you can modify the domain name resolution to point to the backup system, so that the terminal can directly access the eChat backup system, which can ensure service continuity to a certain extent.

- **Automatic geography disaster recovery backup**

When the eChat system is deployed on cloud platform servers, it can also support automatic disaster recovery and backup based on the cloud platform SLB (Server Load Balancing) function.

When the cloud platform supports SLB function, by deploying the same eChat system in different physical available zones of the cloud platform, you can realize disaster recovery backup functions such as, automatic data synchronization, automatic service switch. The entire cloud platform presents a unique set of eChat system externally, which can largely eliminate the hidden danger of single-point service failure of cloud servers.

3 System Platform Security

In addition to the security of the physical platform, the security of the system platform software is also very important.

At present, the eChat system uses an open source operating system and some open source software and suites. During the development of eChat system, the eChat system will effectively detect, control and manage the used system platforms and open source components to ensure its security.

Some of the measures currently taken mainly include:

- Regularly conduct vulnerability scanning of open source software and update patches in time;
- The product can pass the scanning of security tools such as NSFOCUS, Nessus and WebInspect;
- In the delivered version of eChat, there is no high-risk security defect discovered and identified by code automation tools such as klocwork and Coverity, nor high-risk security vulnerability discovered and identified during security testing or independent security audit of NSFOCUS, Nessus, WebInspect;

- The system version has security reinforcement related deployment before release, including security reinforcement compliance configuration, security vulnerability patch processing, and service effectiveness verification after reinforcement implementation;
- The version files will be scanned by three or more mainstream anti-virus software before public release, to ensure that the version to be released is not infected by virus or accidentally killed;
- Version integrity protection will be carried out for all externally released versions;

At the same time, the open source protocol analysis of the used open source database will be separated from the service software in system design to avoid the infection of the service software.

The system can log all key system events and protect the log information.

The current eChat system uses operating system with version CentOS 7.7. CentOS 7.7 has been scanned by security tools such as NSFOCUS and Nessus. Meanwhile, corresponding patch packages are provided based on CentOS 7.7, and these packages have also been scanned by security tools such as NSFOCUS and Nessus, to provide a higher security guarantee for the system. During the development plan of the eChat system platform, the system version will be upgraded as the operating system and open source software versions evolve.

4 Service Platform Security

4.1 User Access Security

- User identity authentication: before a user accesses the system session, the system will authenticate the user identity. The password authentication mechanism should be provided during authentication at least, and is performed every time during system login.

The password is invisible and encrypted for protection during storage and transmission. In addition, when the logged-in user views the system configuration, the user password is also displayed in cipher text. The user is not allowed to perform any operation other than login before completing the identity authentication. When the number of user authentication failures reaches a certain number of times, the user account is locked. The maximum number of user authentication failures can be set, and user authentication information should be recorded in a log for traceability.

- Strong password: The system provides a strong password mechanism. The password verification mechanism includes: (1) The default length is not shorter than 8 bytes; (2) It is composed of numbers, letters, and symbols; (3) Support simple and weak passwords check function; (4) Store the password as cipher text in the system configuration file; (5) When the logged-in user is viewing the system configuration, the password is displayed in cipher text.
- Access session control: User online control is performed according to SIP standard. If there is no refresh message after timeout, the user will be changed to offline status. After the user logs in, no operation is performed within the timer set by the system, such as registration refresh, the system will automatically close the session, and the user needs to log in again to establish a new session.
- Account, terminal and SIM card binding: The eChat system supports user account binding with corresponding terminal and SIM card. When the user login, the login account is only allowed when the used terminal and SIM card are consistent with the bound terminal and SIM card, to prevent non-secure access from other users.
- Terminal white list: The eChat system supports the terminal white list feature. Only the terminal models in the white list can login to the server. The terminal models NOT in the white list will login failed.
- Remote stun/revive (planning): For some suspicious users, remote stun will make these

users temporarily unable to access the service; after passing the security and reliability testing of the stunned users, the remote revive can be performed in the background to resume the normal service of the user.

- Access rights control: The system supports decentralization and separation of domains. Multiple roles can be configured with different levels and capabilities. The management scope and permission of each user can be limited by associating corresponding roles to prevent unauthorized operations. No user can be allowed to gain access to the system through back door.
- Management console supports HTTPS: The eChat management console supports HTTPS to make the access based on web more secure and reliable.

4.2 Link Transmission Security

In the PoC system, the information transmission between the platform and the terminal occurs on the public network, and the transmitted packets must have corresponding security protection mechanisms, usually using encryption and scrambling mechanisms. The eChat system is planning to adopt the following related link transmission security protection mechanisms:

- End-to-end encryption:

The eChat system provides the end-to-end encryption feature. When the user selects the encryption mode for communication, all the user control plane and media plane carried on the network will be processed through software encryption. The data packets such as key negotiation, terminal and dispatch console registration, voice session establishment, voice packet transmission and forwarding are all transmitted in encrypted mode in the IP link, ensuring that the user is safe enough when using eChat.

- Scrambling mechanism (planning):

The system uses a scrambling mechanism, which can effectively protect the information transmitted on the public network. Based on the original standard vocoder and video codec protocol, the eChat system introduces local transformation in the system design, adding interference in the frame structure, large message fragmentation, and framing. When the message is intercepted on the network, it is very difficult to analyze and restore effective information.

4.3 User Data Security

In order to ensure the security management of the user data, the data security design is carried out from the aspects of user data access, storage, integrity protection, privacy protection and so on.

- User data access: In order to control user access to user data, the system considers the following security attributes: operation privilege, operation object, user login address, user validity period and access method.
- User data confidentiality : When user-related data is transmitted on the network, the plaintext transmission is not adopted if there is no protocol requirement, instead the encrypted transmission is adopted to prevent user data leakage. At the same time, encrypted storage will be adopted during user data storage instead of plaintext storage.
- User data protection: After the user data is modified, the system supports rollback to at least the state before the most recent operation to maintain data integrity. Meanwhile, when the storage space for storing user information and other resources is released or reallocated for use of other users, the remaining information should not be reusable.
- Sensitive data protection: When using mobile terminal, management console, and dispatching console, user needs to confirm the terms and conditions of personal data information collection of the system. User can only perform normal service access after confirming that the terms and conditions are correct. At the same time, the system strictly complies with the “minimized” principle of data acquisition, prohibits the expansion of data

collection, and strictly prohibits the recording of personal data that is not necessary for service in the system. In addition, the system strengthens the data security protection for the storage, transmission and processing of personal data, and complies with the laws and regulations of applicable countries and regions.

- Sensitive data isolation: When the system stores information that can identify the user's identity, such as IMSI/ISDN/IMEI/IP address, etc., the system adopts anonymous storage. It can be stored as an identifier like ******, or 139xxxxxxxxx. Even if the data is transferred, the corresponding user cannot be identified.

4.4 Log Audit Security

The system supports the logging and preservation of all key system events and protects the log information.

- System operation log preservation: The key events for system operation mainly include: service startup, service shutdown, service interruption, service recovery, login time, account management, all operations performed by users, system time modification, and important system failure events. When preserving the logs of these key events, the log information includes the following key contents: date and time of the event, event type, event operator, event result, and related content of the event.
- Log information protection: The system saves the log information in the non-volatile storage media. For the stored log information, avoid unauthorized deletion and modification. When the log information storage is exhausted, meets failure, or encounters an attack, you should ensure that the most recent log information will not be destroyed within a certain period of time. At the same time, the system only allows authorized users to access the log information. The log information provided to the user should have a unique and clear definition and a format that is easy to read, and can be retrieved and viewed according to the corresponding keywords.

- Centralized log audit: With effective authorization, the system can provide a log collection interface for authorized devices to collect security logs for centralized auditing.

5 Appendix

Beijing Topsec Network Security Technology Co., Ltd. conducts a security penetration test on Caltta’s eChat PoC system.

The test report shows the overall safety status of eChat PoC system is in a good condition.

About Caltta

Caltta Technologies Co., Ltd (a subsidiary of ZTE) is a leading provider of integrated professional trunking communication solutions. Our company is committed to delivering value to customers by providing innovative solutions and Converging All to Talk. With more than 700 experienced professionals and over 300 trunking technology patents, Caltta is capable of providing DMR, CDMA GOTA, LTE and POC complete ranges of PTT end-to-end products and solutions, which have been accepted and deployed in more than 40 countries and regions globally, delivering satisfactory products and services to customers from various fields such as government affairs, public safety, transportation, energy, utilities, etc.

http://www.caltta.com/en/

caltta.sales@zte.com.cn