# 一、背景

安全加固后，推送给BI的数据中的敏感信息需要进行AES CBC加密

# 二、数据库表

## 1、routerecord表

当前推送语句：

select IMEI,MCC,MNC,PushserverIP,PushserverOutIP,PushserverPort,RecordTime,allocateBelongIdTime,agentVersion,info,retExtInfo,channel,mode from routerecord where RecordTime>=DATE\_SUB(curdate(), INTERVAL 1 DAY);

其中IMEI使用PUSH秘钥进行AES CBC方式加密，加密后样例：3opC5IvmFw9sePtdozM0dFoPxCAqNQlZWeQCTnhSQFWvRj0F41dWuYBNJKMyhrCp。BI接收到数据后，需要进行解密

## 2、mc\_msg表

当前推送语句：

select DeviceToken,receiveTime,Message from mc\_msg where (receiveTime > (now() - 60));

其中：

（1）     DeviceToken中的IMEI号（前16位）使用PUSH秘钥进行AES CBC方式进行加密，后16位没有加密，加密后样例：efjBaST44dagcm51K7peoX08wouUY/jVCJPJ89mjJgYBy+ns+VB3l0Gzh1EYkAfO0000000000000000。BI接收到数据后，要进行解密

（2）     Message使用PUSH秘钥进行AES CBC方式进行加密，加密后样例：。BI接收到数据后，需要进行解密

# 三、日志

## 1、auth\_dev\_LoginLogout.log

登录日志：

2016-02-26 09:34:24 992|2016-02-26 09:34:24 990|1|ngVFs/rTA6LIWvsnbxZJcER0/tjz5/0IRJGYWbA8qGR/Ry09KgNiVySoKOL5jrrM|1|0|10.45.12.36|1308672|323||||||||||||||||||||||||||||||||||||||||||||||||||||||FoS9cLOm6bi6K9LZSsgZa5mLEF2TNctlZ2oJi5dbMzU=

登出日志：

2016-02-26 09:34:44 200|2016-02-26 09:34:44|0|krO8ai/3CpqDx+76TU9Zp4enQea/IU+YmHAaXwHKs9OafP+6tQ6ls30An6phmVna|1|||1308672|323|FoS9cLOm6bi6K9LZSsgZa5mLEF2TNctlZ2oJi5dbMzU=

其中：

（1）     日志中的时间戳由原先的精确到秒，修改为精确到毫秒，绿底部分

（2）     登录登出日志中的第四位的IMEI使用之前跟BI协商的秘钥进行AES CBC加密，红底部分，BI接收到数据后，需要进行解密

（3）     登录登出日志的最后一位增加IMEI号SHA 256之后的值，黄底部分，根据最后一位+每一次登录的session标识（紫底部分）关联同一个设备的某一个登录登出记录

## 2、mc\_bilog.log

push request/push cancel/push timeout/rsd request/timeout delete/replace等：

2016-02-26 11:15:04 359|push request|0000001002000001|1|1|16ACF113DFC71473|||faEXy7zQa4t9T4FwPu8F0NENMH0wIRPwrYoEu5KsGV/hRAl93GDhjm77+sprPk0b0000001002000001|1|test123|10.93.200.148|||jrDm9cj2y3CFb1pIV2+yXDUZ53gBC0tXqu8YM6wBeFA=

响应日志：

2016-02-26 11:15:04 361|push response||||16ACF113DFC71473|||||||0||

其中：

（1）     push token红底部分，前16位使用之前跟BI协商的秘钥进行AES CBC加密，BI接收到数据后，需要进行解密

（2）     请求日志的最后一位增加了IMEI号SHA 256的值，黄底部分，BI可以不关注

## 3、auth\_dev\_token.log

token申请：

2016-02-26 15:02:48 167|register|cnb6P6s7owEoGoz+WM0UheLCBdnuvhFsMEZfm744J+E8NBr4xfTLTwbl5y6L62Xg|0000000002000001|com.huawei.android.push||FoS9cLOm6bi6K9LZSsgZa5mLEF2TNctlZ2oJi5dbMzU=

token注销：

2016-02-26 15:02:36 464|uninstall|H9PQT3wo09PWCduXkPNhlyARdPupNCzDfn979pcDr1075qwBNbgG8UFwhSNjpwz6|0000000002000001|||yIp0XVnxZOAwFMsLlx7/15UpGMNgLmLqG1zqBupEQDA=

其中：

（1）     token申请注销日志中，第三位的IMEI号（红底部分）使用之前跟BI协商的秘钥进行AES CBC加密，BI接收到数据后，需要进行解密

（2）     token申请注销日志的最后一位增加了IMEI号SHA 256的值，黄底部分，BI可以不关注

## 4、userLog.log

设备请求TRS：

2016-02-26 17:22:42 938|Req|kTGBFMXAZwQo0k12oqS1jDzvO/OUXvkWefvvShJ6r9HmA47wvMaSAfBOwOfqyndX|460|02|-1|2518|content123|com.huawei.android.pushagent|G510|1|10.45.1.132|NDO65hfAvBnDiFQbWbnAURCy7LETdyBMohxVqSZ8Z10=

TRS返回响应：

2016-02-26 17:22:42 949|Rsp|DZdaZMVAm/x8sBbudyjHa4dS/+IeibVUWobVOHIUIK29+bsOBF6/9ROQkj2CE+Tu|null|NDO65hfAvBnDiFQbWbnAURCy7LETdyBMohxVqSZ8Z10=

其中：

（1）     设备请求TRS和TRS给设备返回的日志中，IMEI使用之前跟BI协商的秘钥进行AES CBC加密（红底部分），BI接收到数据后，需要进行解密

（2）     设备请求TRS和TRS给设备返回的日志中，增加IMEI号SHA 256之后的值，黄底部分，BI可以不关注

## 5、statistic\_push.log

push request/push cancel/push timeout/rsd request/timeout rsd/timeout delete/replace：

2016-02-26 17:53:25 559|push request|7|0|1|21121a113519000c|||mkDnxwZm6CH0tWGxpJwvV2tDZl8urZnE1sJLbAFZ/tzrPfhQ3iSKV7OCT2FB3J6u0000000013000001|0||10.93.200.148|||FoS9cLOm6bi6K9LZSsgZa5mLEF2TNctlZ2oJi5dbMzU=

响应日志：

2016-02-26 17:53:25 560|push response||||21121a113519000c|||||||1||FoS9cLOm6bi6K9LZSsgZa5mLEF2TNctlZ2oJi5dbMzU=

其中：

（1）     push token红底部分，前16位使用之前跟BI协商的秘钥进行AES CBC加密，BI接收到数据后，需要进行解密

（2）     请求日志的最后一位增加了IMEI号SHA 256的值，黄底部分，BI可以不关注