**分析处置接口设计**

**一、分析系统与处置系统数据包格式定义**

数据以二进制+Json方式封装，封装格式如下。其中，Json作为数据包的数据域部分。



（1）版本号（1字节）：表示满足规范的协议版本，目前为1。

（2）安全模式（1字节）：目前只设置低4位（D3D2D1D0），分别表示是否加密（D3D2）、是否签名/MAC（D1D0）。具体取值如表1所示。

**表1 安全模式取值对应表**

|  |  |  |
| --- | --- | --- |
| **安全模式** | **取值** | **意义** |
| D1D0 | 00 | 未签名/MAC |
| 01 | SM2签名 |
| 10 | MAC（SM4 CBC） |
| D3D2 | 00 | 未加密 |
| 01 | SM2加密 |
| 10 | SM4 ECB加密 |

（3）保留字段（2字节）：暂时保留。

（4）报文序号（4字节）：用于防止遭受重放，通信双方各自维护自己的“报文序号”，依次递增。在密钥协商阶段，“报文序号”可以是任意值（如：全部置0），接收方对其不作处理。密钥协商后，发送报文通过“报文序号”来抵抗重放攻击。

（5）报文长度（4字节）：整个报文的总长度，包括头部、数据域、签名/MAC的长度之和。

（6）报文类型（4字节）：用于标识该报文的类型，可根据该字段区分不同的数据域格式。

|  |  |  |
| --- | --- | --- |
| 产品名称 | 指令类型编码的分类前缀 | 负责单位 |
| 异常行为感知组件15 种 | 0xA113 | **立思辰牵头下分（需尽快协调）** |
| 异常行为信息存储系统 | 0xA149 | 立思辰 |
| 异常行为信息汇聚系统 | 0xA150 | 信工所 |
| 异常行为融合分析系统 | 0xA151 | 上交大 |
| 安全态势分析系统 | 0xA152 | 上交大 |
| 安全事件追踪溯源系统 | 0xA153 | 上交大 |
| 应急联动处置系统 | 0xA154 | 信工所 |

|  |  |  |
| --- | --- | --- |
| 序号 | 编码 | 感知组件名称 |
| 0 | 0x00 | OS X PC 应用感知组件 |
| 1 | 0x01 | Linux PC 应用感知组件 |
| 2 | 0x02 | Windows 应用感知组件 |
| 3 | 0x03 | iOS 终端应用感知组件 |
| 4 | 0x04 | Android终端应用感知组件 |
| 5 | 0x05 | 企业应用感知组件 |
| 6 | 0x06 | 开具感知组件 |
| 7 | 0x07 | 查验感知组件 |
| 8 | 0x08 | 存储感知组件 |
| 9 | 0x09 | 认证服务感知组件 |
| 10 | 0x0A | 密码服务感知组件 |
| 11 | 0x0B | 核准感知组件 |
| 12 | 0x0C | 状态管理感知组件 |
| 13 | 0x0D | CA感知组件 |
| 14 | 0x0E | 道路客运感知组件 |

（7）发送方ID（16字节）：发送方的唯一性标识，该标识在注册时由管理中心统一颁发，通过该标识可以查询到实体的身份信息、公钥证书等。“发送方ID”出现两次：在头部中以明态出现，用于确定发送方的公钥证书；在数据域中以密态出现，用于解密后确认与头部中明态的“发送方ID”是否一致，防止被恶意篡改、伪造。

（8）接收方ID（16字节）：接收方的唯一性标识

（9）数据域（N字节）：该字段为可变长度，其组成格式可根据“报文类型”确定。如果安全模式表示数据域有加密，那么在密钥协商阶段，这里是公钥加密的中间参数；在密钥协商完成的数据传输阶段，这里是对称加密的载荷。

（10）签名/MAC（64/16字节）：对“头部”和“数据域”的签名值或MAC值。在密钥协商阶段，该字段为发送方的私钥签名值；在数据传输阶段，该字段为发送方使用会话密钥计算的MAC值。

**二、分析系统发送威胁报警Json格式**

表1 异常报警格式表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段** | **类型** | **示例** | **描述** |
| 异常报警ID | threatID | string | 00001 | 唯一且递增的异常报警ID |
| 报警时间 | timeStamp | string | 123456789 | 以秒为单位的时间戳 |
| 异常类型 | threatType | int | 0x0101 | 根据已经协商好的异常分类，将异常按照大类及小类进行划分，因此采用4位异常类型码描述具体的异常种类，高二位描述大类异常，低二位描述小类异常。  每个大类异常的低两位为00时，异常类型码作为大类异常标识码，不作为具体的异常类型码使用，该大类的具体小类异常从01开始编码。  将当前异常分类如下：  0x0100 服务器异常（大类标识）  0x0101 服务器仿冒  0x0102 假系统连接  0x0200 多次尝试口令（大类标识）  0x0201 用户多次尝试口令  0x0300 开票报销异常（大类标识）  0x0301 重复报销、作废/冲红凭据报销  0x0302 假发票报销  0x0303 同一企业短时间开具大量凭据  0x0304 同一企业短时间开具大量大额凭据  0x0305 同一企业异常时间开具大量凭据  0x0306 同一企业异常时间开具大额凭据  0x0307 同一用户跨企业异常时间开具大量凭据  0x0308 同一用户跨企业异常时间开具大量大额凭据  0x0309 同一用户短时间跨企业开具大量大额凭据  0x0400 查验异常（大类标识）  0x0401 同一用户/企业多次查验假发票  0x0500 同一凭据频繁变更状态（大类标识）  0x0501 同一凭据频繁变更状态  0x0600 同一用户频繁变更电子凭据状态（大类标识）  0x0601 同一用户频繁变更电子凭据状态  0x0700 用户/系统认证异常（大类标识）  0x0701 同一用户多次尝试认证失败  0x0702 同一系统多次尝试认证失败  0x0800 同一用户或同一企业发生多次异常行为（大类标识）  0x0801 受票企业发生多次异常行为/开票企业发生多次异常行为  0x0900 不同企业或不同用户异常行为关联（大类标识）  0x0901 不同企业或不同用户异常行为关联  0x0A00多次查询/下载（大类标识）  0x0A01多次查询/下载  0x0B00客票信息多次查验（大类标识）  0x0B01客票信息多次查验  0x0C00 核准异常（大类标识）  0x0C01同一用户同一电子凭据多次尝试核准失败  0x0C02同一用户不同电子凭据多次尝试核准失败 |
| 异常上报系统ID | uploadSysID | string | 123456789 | 将异常上报给分析系统的业务系统ID |
| 异常用户ID | threatUserID | string | 123456789 | 本次异常报警如果包含某一具体的异常用户，则本字段记录异常用户ID |
| 异常企业ID | threatEnterpriseID | string | 123456789 | 本次异常报警如果包含某一具体的异常企业，则本字段记录异常企业ID |
| 异常凭据ID | threatCredenID | string | 123456789 | 本次异常报警如果包含某一具体的异常凭据，则本字段记录异常凭据ID |
| 异常IP | threatIP | string | 192.168.0.1 | 本次异常报警如果包含某一具体的异常IP，则本字段记录异常IP |
| 异常IP段 | threatIPSegment | string | 192.168.0.1/24 | 本次异常报警如果包含某一具体的异常IP段，则本字段记录异常IP段 |
| 保留字段 | otherMsg | string |  | 为将来扩展异常类型进行保留  第八种威胁"同一用户或同一企业发生多次异常行为"和第六种威胁"同一企业频繁变更电子凭据状态"用到该字段，第八种威胁可以填充以下三个数据，第六种威胁只有"1"和"2"：  "1"： 受票企业发生异常行为  "2": 开票企业发生异常行为  "3"： 受票个人发生异常行为 |

**示例：**

**1）分析系统发送服务器仿冒类异常**

{

threatID:"10001",

timeStamp: "123456789",

threatType:0x0101,

uploadSysID: "123456789",

threatUserID: "",

threatEnterpriseID: "",

threatCredenID: "",

threatIP: "192.168.1.1",

threatIPSegment: "",

otherMsg: ""

}

**2）分析系统发送用户多次尝试口令异常**

{

threatID: "10002",

timeStamp: "123456789",

threatType:0x0201,

uploadSysID: "1112",

threatUserID: "12345678",,

threatEnterpriseID: "",

threatCredenID: "",

threatIP: "",

threatIPSegment: "",

otherMsg: ""

}

**三、处置系统回复分析系统Json格式**

表2 回复分析系统格式表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段** | **类型** | **示例** | **描述** |
| 异常报警ID | threatID | string | 00001 | 唯一且递增的异常报警ID |
| 时间戳 | timeStamp | string | 123456789 | 本条消息的回复时间 |
| 回复类型 | respondType | int | 0x01 | 本字段中，不同的回复类型码指定处置系统回复本条消息给分析系统时所处的处置阶段  0x01 处置系统接收威胁报警  0x02 处置系统下发处置指令  0x03 处置系统评估处置效果 |
| 结果 | respondResult | int | 0x01 | 处置系统接收威胁报警：  处置系统下发处置指令：  0x01 成功 0x02 失败 0x03 其他  处置系统评估处置效果（1-5）：  1无效果  2 轻微效果  3 中等效果  4 明显效果  5 显著效果 |
| 其他信息 | otherMsg | string |  | 处置系统具体返回给分析系统的信息，留作扩展 |

**示例：**

**1）处置系统接收威胁报警成功**

{

threatID: "10002",

timeStamp: "123456789",

respondType:0x01,

respondResult:0x01,

otherMsg: ""

}

**2）处置系统下发处置指令失败**

{

threatID: "10002",

timeStamp: "123456789",

respondType:0x02,

respondResult:0x02,

otherMsg: ""

}

**3）处置系统评估处置效果**

{

threatID: "10002",

timeStamp: "123456789",

respondType:0x03,

respondResult:4,

otherMsg: ""

}

**四、业务系统回复处置系统格式**

表3 业务系统回复处置系统格式表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段** | **类型** | **示例** | **描述** |
| 处置指令ID | instructID | string | 00001 | 递增唯一的处置指令ID |
| 时间戳 | timeStamp | string | 123456789 | 本条消息的回复时间 |
| 响应对象ID | receiverID | string | 123456789 | 接收处置指令执行并且回复本条消息响应对象的ID |
| 结果 | respondResult | int | 0x01 | 0x01 成功  0x02 失败  0x03 其他 |
| 其他信息 | otherMsg | string |  | 业务系统具体返回给处置系统的信息，留作扩展 |

**示例：**

**1）业务系统执行处置指令成功**

{

instructID: "10001",

timeStamp: "123456789",

receiverID: "11112",

respondResult:0x01,

otherMsg: ""

}

**2）业务系统执行处置指令失败**

{

instructID: "10002",

timeStamp: "123456789",

receiverID: "11112",

respondResult:0x02,

otherMsg: ""

}