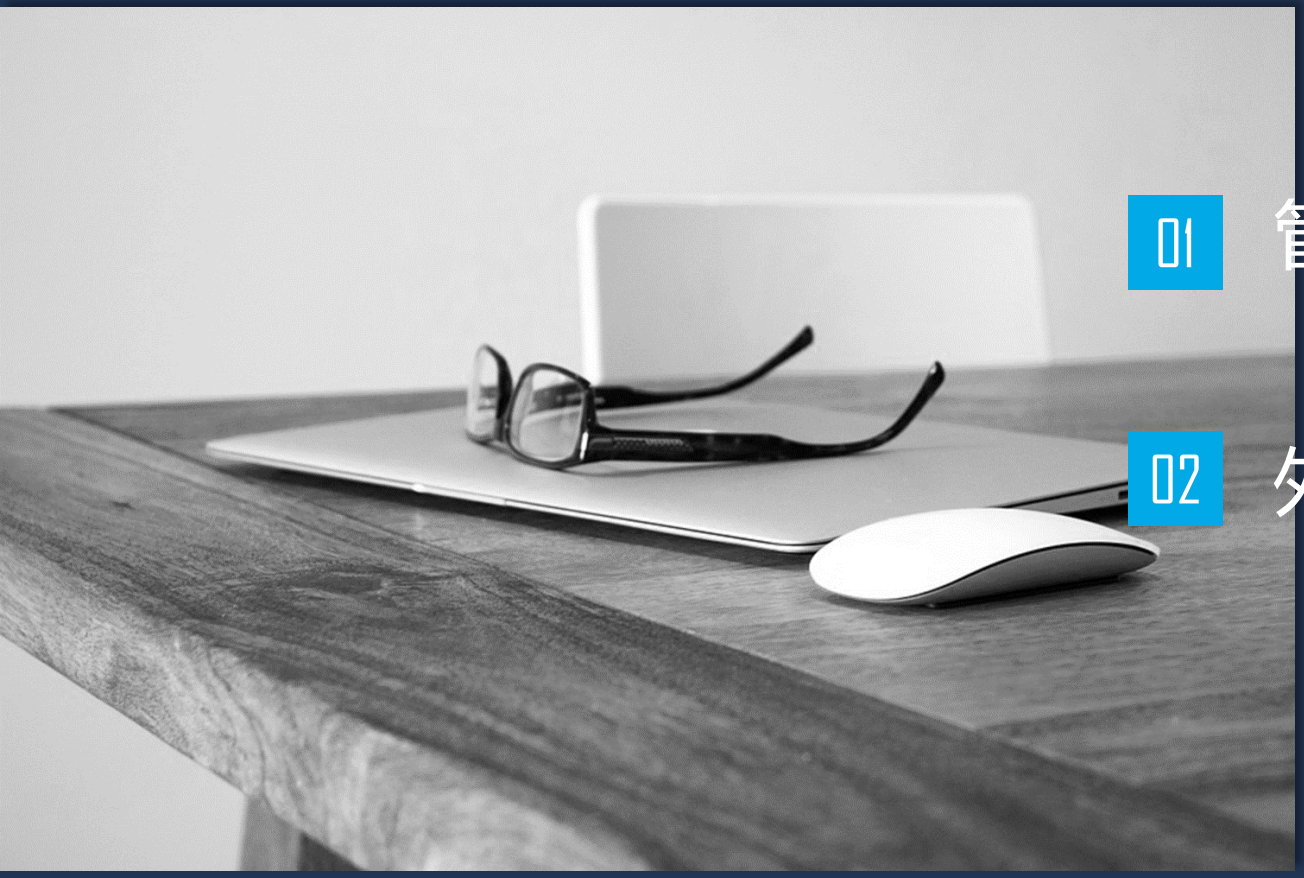
机动车驾驶人考试系统软件安全性管理要求

公安部交通管理科学研究所

2017年7月



01 管理规定概述

02 外挂软件测试要求

一、 管理规定概述

规定概述

目标

●加强公安交通管理信息系统外挂软件安全管理，提高外挂软件安全设计水平，规范外挂软件管理工作流程

范围

●适用于外挂软件的安全设计、安全测试、接口申请、访问授权、上线运行、下线停用等安全管理工作（安全运行环境，运行和使用管理制度；基于统一版核心信息系统应用库、分发库开发的应用软件）

总览

●规定条文：共8章，46条
●2017年5月9日发布，2017年7月1日起实施
●2017年12月31日前，完成已授权启用的外挂软件升级改造、上报测试和重新授权工作

1. 安全设计

2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

1. 安全设计

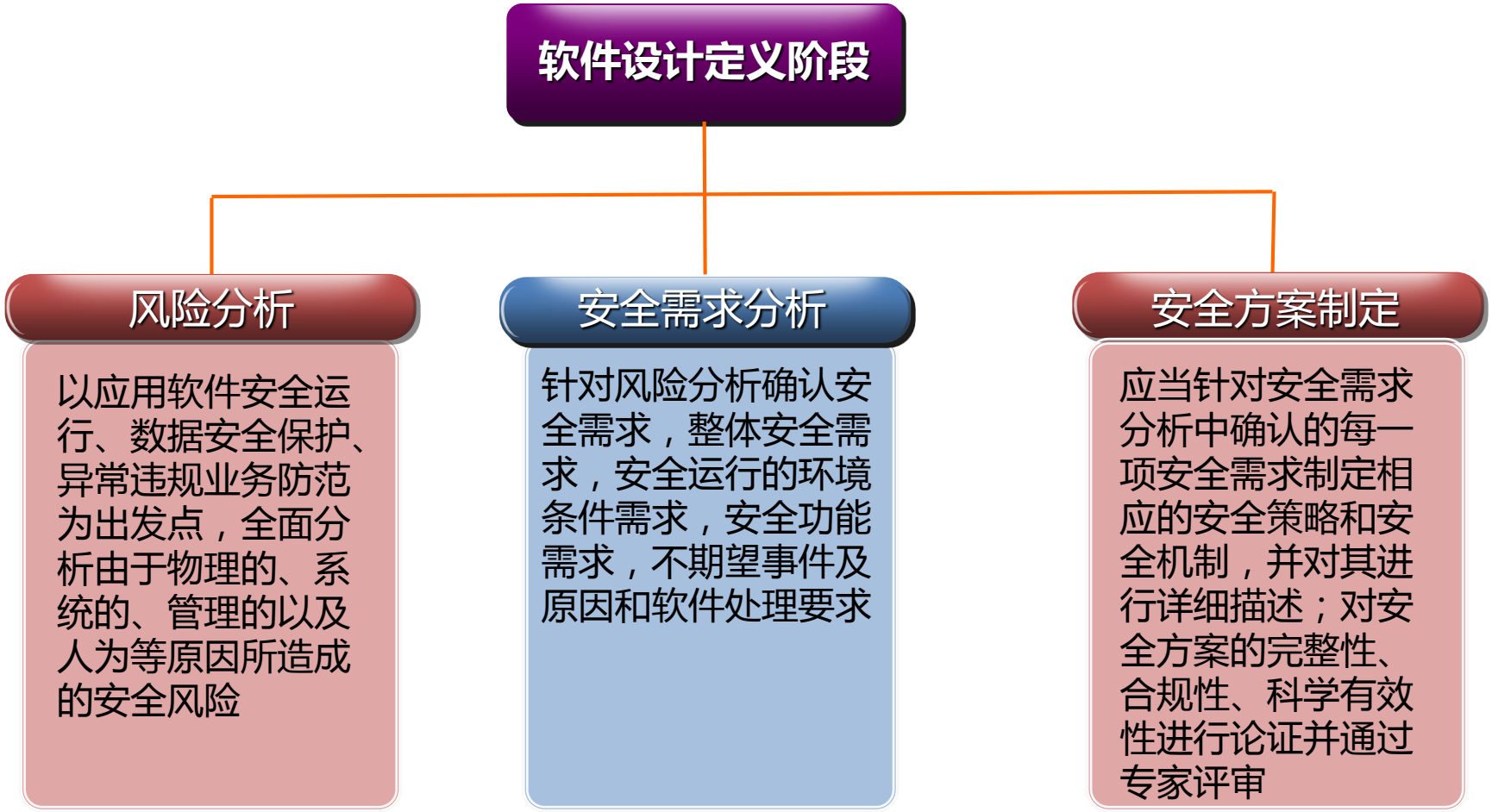
2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

1、安全设计


软件设计定义阶段
风险分析
以应用软件安全运行、数据安全保护、异常违规业务防范为出发点，全面分析由于物理的、系统的、管理的以及人为等原因所造成的安全风险
安全需求分析
针对风险分析确认安全需求，整体安全需求，安全运行的环境条件需求，安全功能需求，不期望事件及原因和软件处理要求
安全方案制定
应当针对安全需求分析中确认的每一项安全需求制定相应的安全策略和安全机制，并对其进行详细描述；对安全方案的完整性、合规性、科学有效性进行论证并通过专家评审

1、安全设计

访问全国统一版信息系统数据库	外挂软件应当通过全国统一版信息系统提供的请求服务接口查询、写入、修改、删除全国统一版信息系统的数据，不允许以数据库授权访问、数据库链路等方式直接访问全国统一版信息系统数据库
个性化请求服务功能	各地可以基于本地应用库、分发库设计实现个性化请求服务功能，但应符合本规定的安全设计要求，数据抽取应遵循按需最小化抽取原则，不抽取手机号码、联系住所地址、车辆轨迹等个人隐私信息
禁止事项	外挂软件不得以任何理由留有后门程序或者绕过软件的安全机制

1. 安全设计

2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

2、安全测试

测试依据	● 《公安交通管理信息系统运行管理规定》第七条和第二十一条、《公安交通管理综合应用平台使用规定》第四十六条、《互联网交通安全综合服务管理平台运行和使用规定（试行）》第十二条和第四十一条等管理规定 ● 公安交通管理信息系统外挂软件安全设计规范
软件调整测试要求	当外挂软件发生涉及软件安全设计、请求服务接口需求调整及其他重大功能调整的，应当通过安全测试

2、安全测试

安全测试应当至少提交资料

- 1、外挂软件安全需求分析报告，其内容应当符合本规定第十三条要求；
- 2、外挂软件技术方案，其内容应当包含信息安全技术方案并符合本规定第十四条要求；
- 3、外挂软件操作说明；
- 4、外挂软件请求服务接口调用情况说明，应当具体说明每一个功能菜单、调用场景所需请求的服务接口，并与外挂软件操作说明内容实现对应。

2、安全测试

安全测试应当至少包含内容

- 1、根据本规定第十五条、第十七条、第十八条及《公安交通管理信息系统外挂软件安全设计规范》的要求，对外挂软件安全设计、访问全国统一版信息系统方式等进行测试；
- 2、核实外挂软件功能是否存在违规业务办理功能，是否符合相关法律法规的规定；
- 3、对外挂软件请求服务接口调用需求进行确认；
- 4、采用应用软件漏洞扫描软件对外挂软件进行安全扫描，测试外挂软件是否存在“中危”及以上风险漏洞。

1. 安全设计

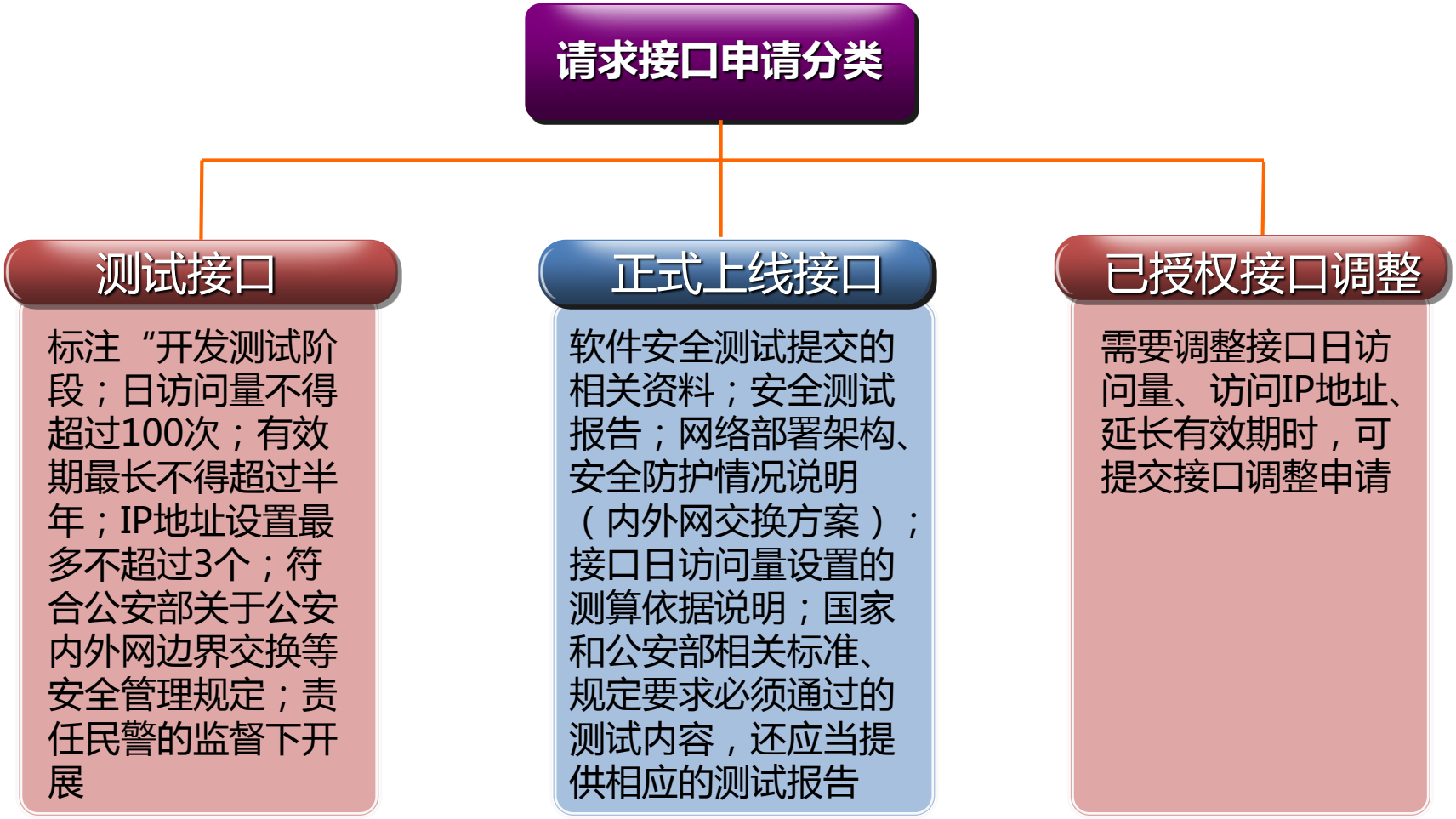
2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

3、接口申请和授权


请求接口申请分类
测试接口
标注“开发测试阶段；日访问量不得超过100次；有效期最长不得超过半年；IP地址设置最多不超过3个；符合公安部关于公安内外网边界交换等安全管理规定；责任民警的监督下开展
正式上线接口
软件安全测试提交的相关资料；安全测试报告；网络部署架构、安全防护情况说明（内外网交换方案）；接口日访问量设置的测算依据说明；国家和公安部相关标准、规定要求必须通过的测试内容，还应当提供相应的测试报告
已授权接口调整
需要调整接口日访问量、访问IP地址、延长有效期时，可提交接口调整申请

3、接口申请和授权

正式上线接口申请及审批授权流程

- 1、通过全国统一版信息系统填报并上传接口申请信息，以及外挂软件技术方案等相关资料；
- 2、省（区、市）公安交通管理部门审核后，报公安部交通管理科学研究所；
- 3、公安部交通管理科学研究所审核后，报公安部交通管理局；
- 4、公安部交通管理局完成审核后，公安部交通管理科学研究所生成接口授权码；
- 5、下载接口授权码，开通使用。

重点审核：

1、外挂软件是否已通过安全测试，软件版本是否一致，提交材料是否齐全；

2、申请的接口与安全测试报告确认的接口调用需求是否一致；

3、外挂软件网络部署、数据交换是否符合公安部相关安全管理规定，接口日访问量设置是否合理。

禁止事项：不允许未经安全测试、接口申请、授权的外挂软件共用已授权外挂软件的授权认证信息。

1. 安全设计

2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

4、下线停用

取消接口访问授权办理流程

- 1、通过全国统一版信息系统填报并上传接口访问授权取消申请；
- 2、公安部交通管理科学研究所取消外挂软件接口访问授权，并向公安部交通管理局报备；
- 3、下载更新接口授权信息，外挂软件关闭停用。

注意事项：
外挂软件不再使用的，应当及时卸载应用软件，清理外挂软件服务器。
禁止事项：
不得保留下线停用外挂软件的接口访问授权信息，提供其他外挂软件调用或者用于其他目的。

1. 安全设计

2. 安全测试

3. 接口申请和授权

4. 下线停用

5. 监督管理

5、监督管理

监督通报	公安部交通管理局对各地（省（区、市）公安交通管理部门应当对本地）外挂软件安全测试、请求服务接口申请、接口调用情况进行监督，定期通报。
预警分析 定期抽查	公安部交通管理科学研究所基于接口调用日志开展外挂软件异常访问分析预警工作，定期对各地已授权外挂软件进行抽检，并将分析情况和抽检结果上报公安部交通管理局。（发现运行环境不符合安全管理要求或者外挂软件存在安全漏洞以及安全测试时外挂软件与实际部署运行外挂软件不一致情况的，暂停接口授权）
倒查机制 应急处置	发现利用外挂请求服务接口窃取数据、违规办理业务以及提交虚假信息申请接口等行为的，追究相关单位和个人责任；发生大量敏感信息泄露、遭受大规模网络攻击等重大安全事件时，立即采取关停外挂软件等处置措施，并逐级上报部局
资格审查 保密协议	外挂软件设计、研发、测试及运维等阶段中，有承建单位、运维单位、外包服务承担单位及相关人员参与的

二、 外挂软件测试要求

《公安交通管理信息系统外挂软件安全管理规定》第二十九条

正式上线运行接口申请，应当提交以下资料：
（一）本规定第二十一条所要求的外挂软件安全测试提交的相关资料；
（二）外挂软件安全测试机构出具的安全测试报告；
（三）外挂软件在本次申请单位的实际网络部署架构、安全防护情况说明，涉及公安内外网数据交换的，应当详细说明数据交换方案；
（四）每个接口日访问量设置的测算依据说明；
（五）除本规定所要求的安全测试外，对于国家或者行业标准另有明确设计要求，或者国家和公安部相关规定要求必须通过的测试内容，还应当提供相应的测试报告。

1. 概述

2. 软件设计要求

3. 接口调用需求

4. 漏洞扫描

1、概述

身份鉴别

3 访问控制
测试项目14个

4 安全日志及审计
测试项目11个

5 数据完整性和保密性
测试项目4个

6 抗抵赖
测试项目2个

7 软件容错
测试项目1个

8 资源控制
测试项目6个

9 软件代码安全
测试项目3个

10 外挂接口
测试项目1个

11 安全漏洞
测试项目1个

共计
11个安全层面
59个测试项目

1. 概述

2. 软件设计要求

3. 接口调用需求

4. 漏洞扫描

2、软件设计要求—身份鉴别

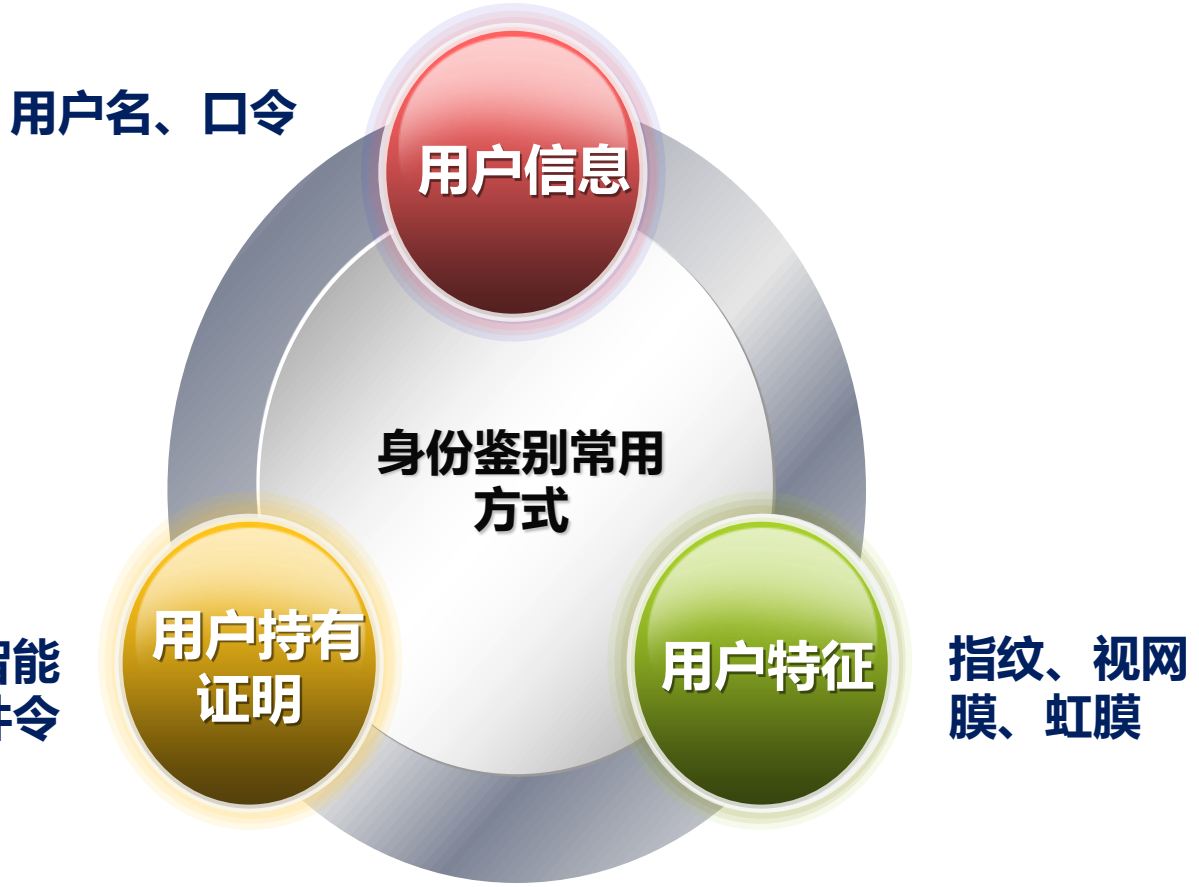
标识：用户向信息系统表明其身份

鉴别：信息系统验证用户所声称的身份

标识和鉴别是用来确保用户在信息系统中唯一性和可确认性，防止信息系统被非授权用户非法登陆的技术手段，也是实现访问控制的前提和基础。

2、软件设计要求—身份鉴别

用于身份认证的信息分类



2、软件设计要求—身份鉴别

➢ （1）基于用户所知道的信息

用户名、口令鉴别是使用最广泛，实现最简单的技术，鉴别强度也相对较弱。

其有效性由用户口令的安全性决定

2、软件设计要求—身份鉴别

➢ （2）基于用户所持有的物品

为了降低身份鉴别系统的复杂性而借助物理设备存储部分用户身份信息，系统通过用户持有的物理设备对用户进行鉴别。这些物理设备通称为令牌

记忆令牌	**记忆令牌存储但不处理信息，对令牌的读写通过专用读写器完成（如：银行卡、门禁卡等）**
智能令牌	**智能令牌内部装有集成电路及扩展令牌功能，与软件配合完成对用户身份的鉴别（如：动态口令卡、数字证书等）**

2、软件设计要求—身份鉴别

典型的产品

动态令牌

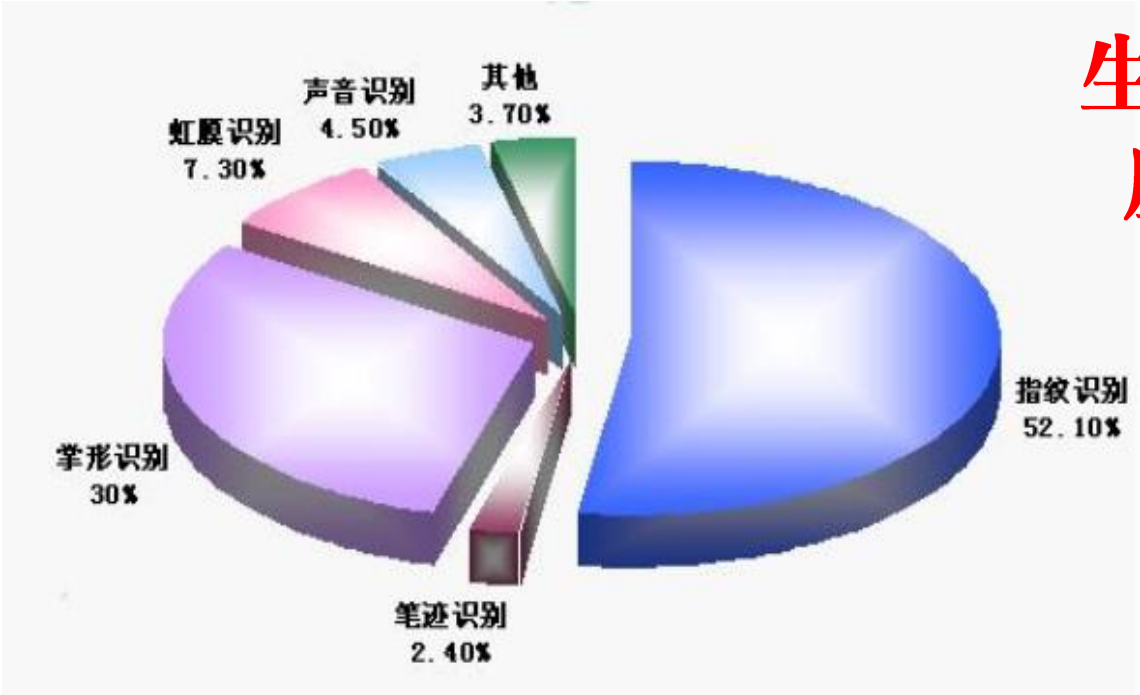
- 基于时间的动态令牌
- 基于挑战的动态令牌

数字证书

2、软件设计要求—身份鉴别

➢ （3）基于用户特征

通过计算机收集人体所固有的独一无二的生理特征或行为特征并进行处理来进行个人身份鉴别



生物识别的应用比例

2、软件设计要求—身份鉴别

用户注册

- 1、凡需进入外挂软件应用程序的用户，应当先进行注册登记。
- 2、外挂软件用程序的用户标识应当包含用户名、用户标识符（UID）、身份证明号码、警员编号或者员工编号、姓名等信息，对警员和非警员身份进行明确标识，并提供和启用用户身份唯一性检查功能，在外挂软件应用程序的整个生存周期实现用户标识符的唯一性，以及用户标识符、用户名、身份证明号码、警员编号或者员工编号、姓名之间的一致性。
- 3、*对提供单点登录的分布式应用软件系统，应当提供单点用户标识，且单点标识应当具有与常规标识相同的安全性。
- 4、*应当对用户标识信息进行统一管理，确保注册行为的合规性及标识信息的准确性，并确保其不被非授权地访问、修改或者删除。

2、软件设计要求—身份鉴别

用户登录

- 1、*具备公安数字证书用户身份鉴别功能，并可强制用户以公安数字证书鉴别机制进行用户身份鉴别。
- 2、*采用了公安数字证书或者生物特征鉴别机制的应用软件系统，对系统用户（如系统管理员、审计员和安全员）应当强制以公安数字证书或者生物特征鉴别机制进行身份鉴别。
- 3、应当提供用户密码校验功能，以确保用户密码长度不小于8位，且必须包含英文字符、数字及特殊符号。
- 4、鉴别信息应当是不可见的，并在传输时用加密方法或者具有相同安全强度的其他方法进行安全保护。
- 5、用户密码不允许在数据库中明文存储，应当以用户标识符、用户密码、姓名等鉴别信息组合后，用加密方法存储。

2、软件设计要求—身份鉴别

用户登录

- 6、应当预先定义鉴别失败次数的阈值，当用户鉴别失败次数达到阈值时，外挂软件应用程序应当退出登录过程并终止与用户的交互，并将信息写入安全日志。
- 7、对重复鉴别行为的限制应当提供基于访问终端和基于用户两种方式，当某一访问终端鉴别失败次数达到阈值时，应当将该访问终端信息写入黑名单，在一定时间段内限制其再次登录；当某一用户鉴别失败次数达到阈值时，应当锁定该用户，限制其再次登录。对提供访问终端黑名单和用户解锁功能的，解锁操作应当写入安全日志。
- 8、外挂软件应用程序应能通过设定用户有效期、密码有效期、IP/MAC地址或者登录地点、登录时间段等手段对用户登录行为进行限制。

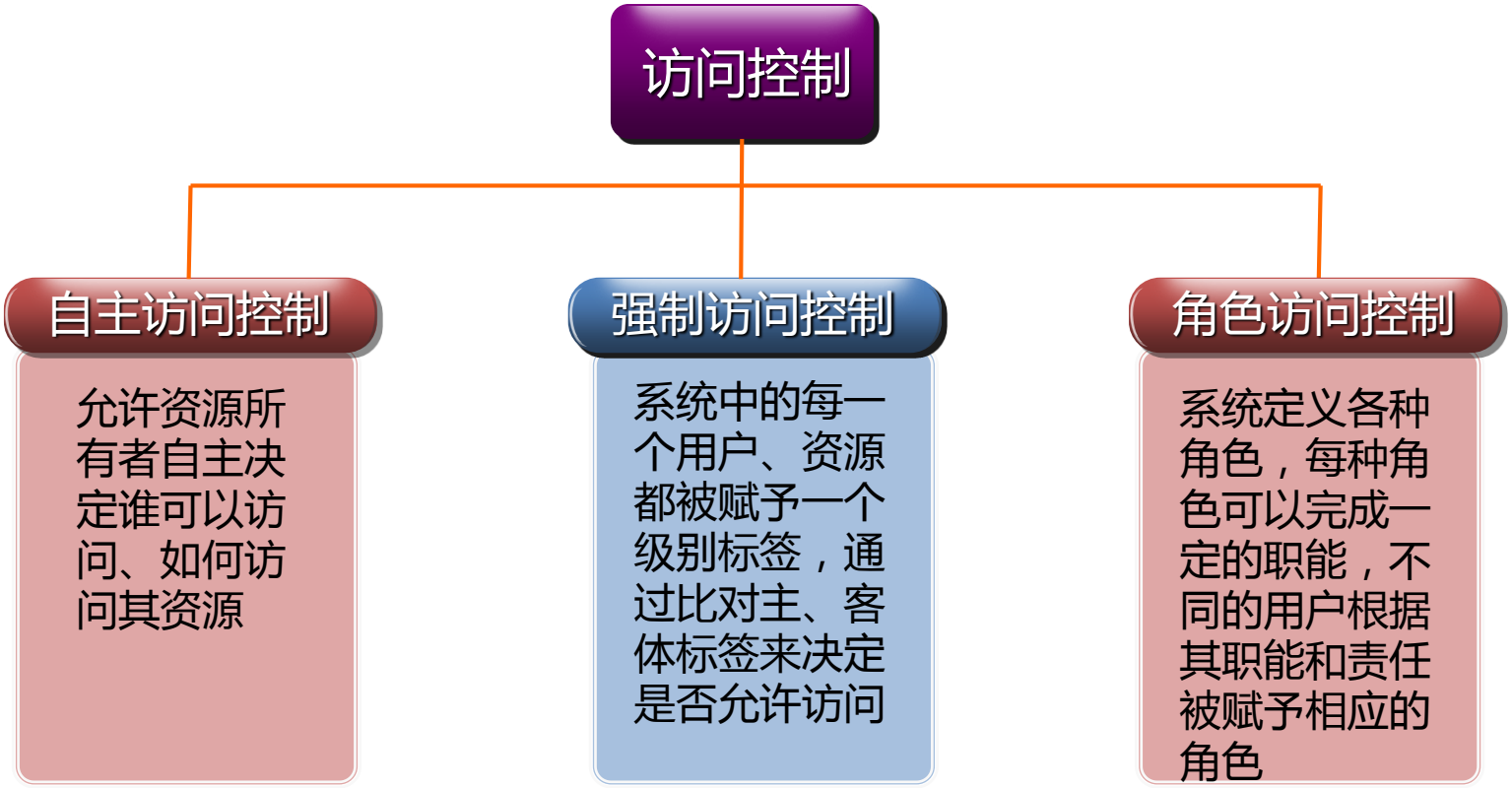
2、软件设计要求—身份鉴别

用户登录

- 9、超过用户有效期的用户只有经系统管理员激活并延长有效期后方可登录外挂软件应用程序；该用户激活后，应当强制其修改密码，成功后方可登录，并延长密码有效期。
- 10、*对提供单点登录的分布式应用程序的用户应当提供单点用户鉴别，且单点鉴别应当具有与常规鉴别相同的安全性。
- 11、具备对同一用户多地、同时登录外挂软件应用程序的异常情况进行检测和限制的功能。
- 12、用户登录成功后，外挂软件应用程序应当记录并向用户显示日期、时间、来源和上次成功登录的日期、时间、来源，以及上次成功访问之后用户身份鉴别失败的情况、用户和密码距离到期的天数。

2、软件设计要求—访问控制

按访问控制策略划分的分类



2、软件设计要求—访问控制

- 1、外挂软件应用程序应当提供对软件功能和资源的访问控制功能，控制用户对应用软件系统各项功能、文件、数据等客体的访问。
- 2、访问控制的覆盖范围应当包括访问主体、客体及它们之间的操作。应当由授权主体配置访问控制策略，并严格限制默认账户的访问权限。
- 3、应当实现以软件功能和用户操作行为特征为基本粒度的访问控制。
- 4、基于用户的访问控制策略应当实现授予不同用户完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。应当禁止用户同时具有业务办理、系统管理、安全管理、审计管理中两种及以上功能，禁止用户同时具有业务申请、业务审批的权限或者通过系统逻辑禁止用户对自身发起的申请进行审核。
- 5、系统初始化默认用户应当按照最小授权原则，只授予系统运行所必需的初始化参数设置、管理部门和用户维护、权限管理等功能。

2、软件设计要求—身份鉴别

- 6、*采用基于角色的访问控制策略。
- 7、外挂软件应用程序应当根据警员和非警员身份信息，严格控制非警员身份人员允许访问的软件功能和资源。
- 8、“授权传播”指将授权的权力传播给其他用户，使其可以获得将指定客体的访问权限授予其他用户的权限。具有“授权传播”分级功能的外挂软件应用程序，获得“授权传播”的用户，并未获得访问指定客体的权限，仅可将授权传播给不包含其自身的其他用户，如需访问指定客体，需同时得到“访问授权”。
- 9、具有分级“授权传播”功能的应用软件系统，应对授权传播进行限制，对不可传播的授权进行明确定义，由系统自动检查并限制这些授权的传播。

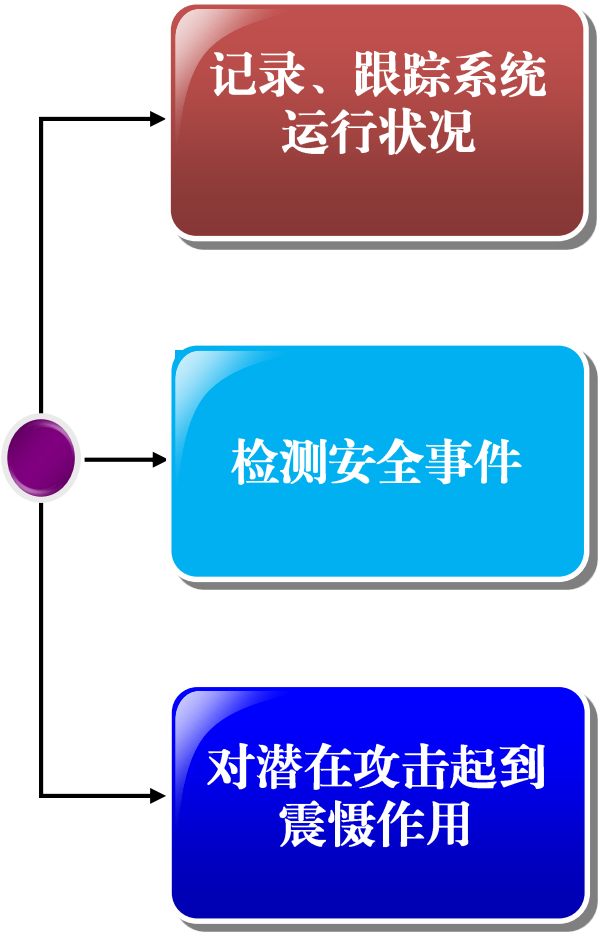
2、软件设计要求—身份鉴别

- 10、*对分布式外挂软件应用程序，应当实行统一的访问控制安全策略，确保每一个场地的主、客体具有一致的安全属性，并执行相同的访问规则。
- 11、对重要数据的访问与重要进程的操作，采用客户端IP地址和用户绑定等技术实现客户端访问授权管理。
- 12、*提供对重要数据访问频率的控制，通过对过高访问频度的预警及阻断，加强对重要数据的安全管理。
- 13、服务端、客户端、数据库各层之间接口进行信息交互时，应对接口访问的授权进行确认，非授权的接口访问应视为攻击行为，记入安全事件日志。
- 14、*通过对主体、客体设置敏感级别标记，对用户访问敏感信息的行为进行控制。

2、软件设计要求—安全日志及审计

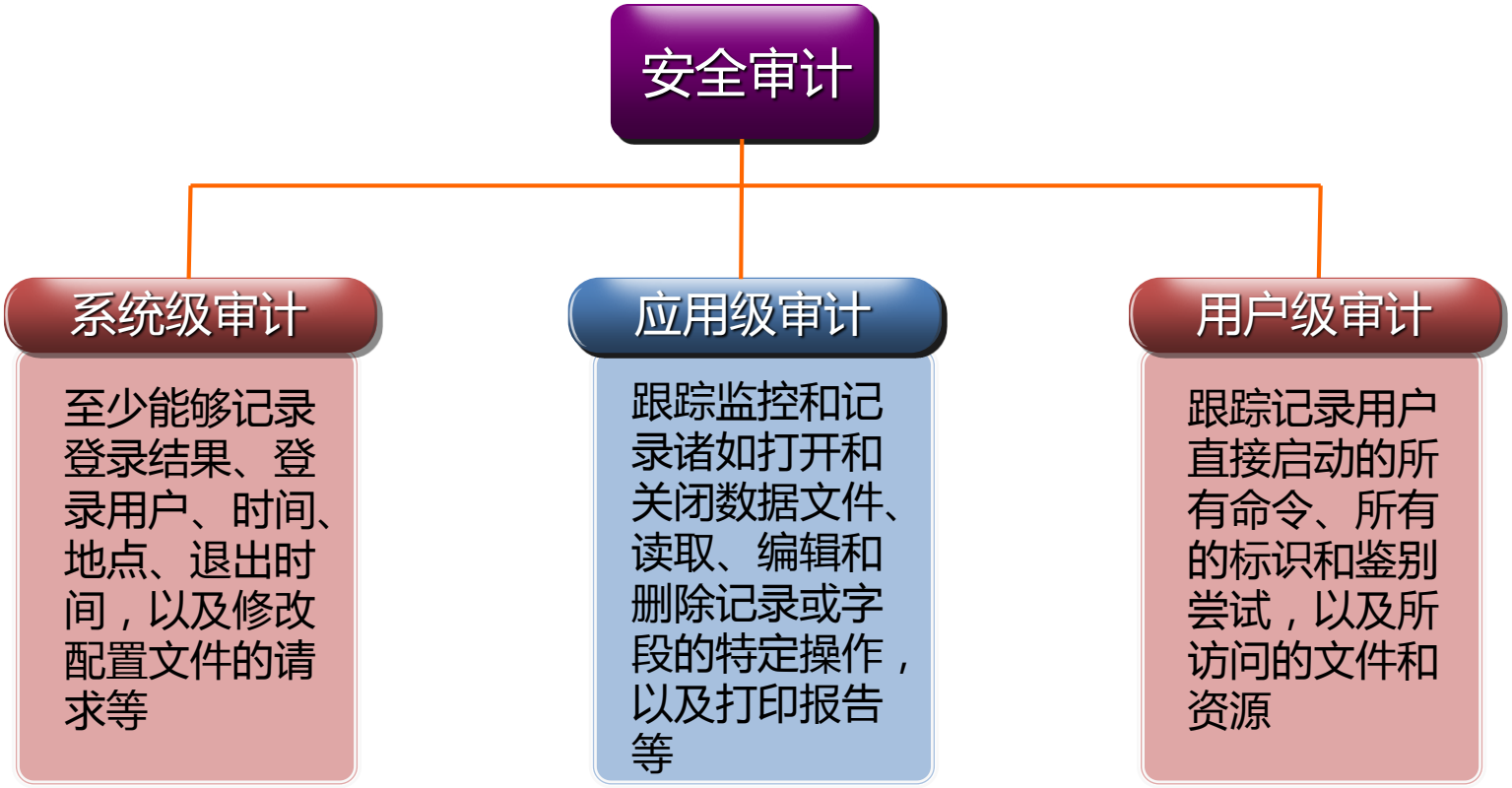
安全审计是指针对信息系统中与安全活动相关的信息进行识别、记录、存储和分析的整个过程

安全审计主要功能



2、软件设计要求—安全日志及审计

按审计对象分类划分



2、软件设计要求
—安全日志及审计

- 1、外挂软件应用程序应对所有用户的重要行为（如用户登录、业务操作、重要数据查询）记录日志。
- 2、日志的内容应当包含用户标识、操作时间、来源、行为、结果、关联数据及资源等信息。
- 3、提供基于用户的安全审计策略设置、审计日志存储和异常情况预警功能。
- 4、*提供应用程序运行状态监控、监控日志存储和异常情况预警功能。运行状态包括应用软件功能模块运行、版本升级、后台任务运行及主机系统资源使用等。
- 5、提供应用程序核心功能定义、核心功能操作审计、审计日志存储和异常情况预警功能。
- 6、具备数据异常情况告警功能。异常情况包括数据异常篡改、数据不一致等。

2、软件设计要求
—安全日志及审计

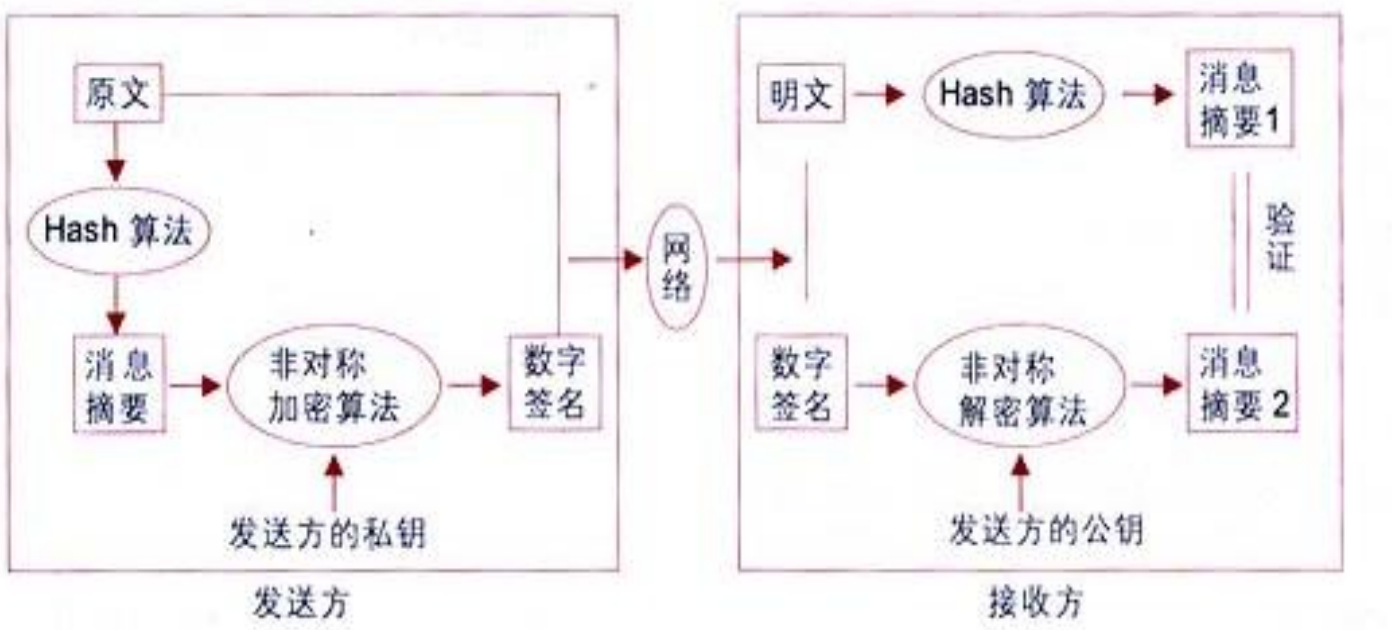
- 7、安全审计策略的设计应当与用户标识与鉴别、访问控制等安全功能的设计紧密结合，还应当对许可访问的行为制定安全审计策略，如用户高频访问、规定时段外访问、账户长期未使用、非常规业务的办理等。
- 8、安全审计信息应当采取加密存储、生成校验码或者其他安全存储措施，避免存储的安全审计日志被非法查看、修改或者删除。
- 9、安全审计日志的存储期限不得少于1年。
- 10、应当提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
- 11、按照公安部制定的公安信息系统应用日志安全审计相关规定，设计应用程序中用户操作行为和接口服务的日志格式，并在调用公安交通管理综合应用平台等核心系统请求服务接口时将相关审计信息写入核心系统。

2、软件设计要求
—数据安全性和保密性

- 1、通过使用数据校验码算法，生成源数据的校验码，在存储、传输及处理过程中对重要数据的完整性进行校验，防止关键数据被非法篡改。
- 2、在对重要数据完整性检测时，发现其完整性被破坏的，应当记入系统安全审计日志。在数据更新时，发现原有数据完整性被破坏的，应当拒绝数据更新操作。
- 3、应当采用加密技术对应用软件系统的重要数据、隐私信息进行加密，实现数据保密性保护，防止信息泄露。
- 4、*对外挂软件应用程序中使用的缓冲存储器及其他动态记录介质，通过在释放其使用权时对剩余信息进行删除等措施，确保不会由于动态记录介质中的剩余信息（ 用户在完成信息系统使用后，保留在存储空间中的用户鉴别信息、用户使用信息等资源）引起信息泄漏。

2、软件设计要求—抗抵赖性

- 1、*抗原发抵赖：对于在网络环境进行数据交换的情况，通过提供选择性原发证据，实现抗原发抵赖功能。
- 2、*抗接收抵赖：对于在网络环境进行数据交换的情况，通过提供选择性接收证据，实现抗接收抵赖功能。



2、软件设计要求—软件容错

- 应当对人机接口或者通信接口输入的数据格式、长度等进行严格的逻辑校验，确保输入数据符合应用软件的设定要求以及数据的准确性、完整性。

2、软件设计要求—资源控制

- 1、应当具备自动结束会话功能。通信双方的一方在一段时间内未做响应时，另一方能自动结束会话。
- 2、应当具备对应用程序最大并发会话连接数进行限制的功能。
- 3、具备对单个用户账户的多重并发会话进行限制的功能。
- 4、*具备对一个时间段内指定重要业务操作数进行限制的功能，防止对重要业务和数据的高频访问。
- 5、*具备对应用软件服务水平降低到预先规定的最小值进行检测和报警的功能。
- 6、*按应用软件系统的功能优先级进行资源的管理和分配。

2、软件设计要求—软件代码安全

- 1、用户界面提示的错误信息应当简洁、清晰，不应直接显示与系统底层代码相关的信息。如需作错误诊断的，可在展现时将错误代码信息加密，用户可提交开发人员，经解密后再进行故障诊断工作。
- 2、*采用代码混淆、自定义装载器等技术提高系统代码的安全性，避免代码被反编译。
- 3、系统控制数据，如口令、密钥、数据库连接参数等，不应当在未受保护的程序或者文档中以明文形式存储。

1. 概述

2. 软件设计要求

3. 接口调用需求

4. 漏洞扫描

3、接口调用需求

《公安交通管理信息系统外挂软件安全管理规定》第二十一条

01	外挂软件安全需求分析报告，其内容应当符合本规定第十三条要求。
02	外挂软件技术方案，其内容应当包含信息安全技术方案并符合本规定第十四条要求。
03	外挂软件操作说明。
04	**外挂软件请求服务接口调用情况说明，应当具体说明每一个功能菜单、调用场景所需请求的服务接口，并与外挂软件操作说明内容实现对应。**

1. 概述

2. 软件设计要求

3. 接口调用需求

4. 漏洞扫描

4、漏洞扫描

B/S架构	C/S架构
Web应用弱点扫描器	主机漏洞扫描工具（安装前后各扫描一次，比对扫描结果）

《公安交通管理信息系统外挂软件安全管理规定》 第二十三条

01 根据本规定第十五条、第十七条、第十八条及附件《公安交通管理信息系统外挂软件安全设计规范》的要求，对外挂软件安全设计、访问全国统一版信息系统方式等进行测试。

02 核实外挂软件功能是否存在违规业务办理功能，是否符合相关法律法规的规定。

03 **对外挂软件请求服务接口调用需求进行确认。**

04 **采用应用软件漏洞扫描软件对外挂软件进行安全扫描，测试外挂软件是否存在中危及以上风险漏洞。**