网络空间安全与信息安全课程设计要求

目录

网络空间安全与信息安全课程设计要求

一、课程设计的题目

可从以下多个题目中任选一个题目，完成课程设计。

（一）基础性题目

题目 1：基于安全认证、加密传输和加密存储的网络加密磁盘设计与实现

（1）基于网络编程技术，开发一个提供网络共享存储空间的系统。可为互联网、无线网络、移动通信等用户提供一个安全的网络存储空间。

（2）每个用户有自己的存储加密空间，支持数据和文件的加密传输和共享存储空间的本地加密存储，文件加密传输支持一次一密加密传输机制，支持防篡改和防中间人攻击。只有在共享存储空间加密存储的最初用户可以解密加密的数据，支持安全的加密数据找回机制。同时，支持多用户同时连接共享存储空间，每个用户组在共享存储空间有独立存储空间，不能登录其它用户组的空间，用户组中的用户可在多个终端登录自己的存储空间，用户组中的每个用户都可以访问用户组存储空间加密的数据并解密。

（3）每个用户登录要有安全的登录认证机制，可以采用口令、数字证书、短信、email、生物特征识别和微信/支付宝身份识别等登录认证方式中的 2 种登录方式进行登录，有密钥找回机制。要求密钥找回后，加密文件还可解密。

（4）用户登录认证过程中的网络传输数据需要采用加密传输机制，设计安全的密钥传输机制，支持防篡改和防中间人攻击。

（5）用户和网络磁盘空间之间，要求每次登录后的数据传输，采用自己开发实现的基于会话一次一密加密传输机制，并且网络磁盘空间中保存的数据，要求采用加密存储机制，只有创建磁盘空间的用户可以解密磁盘空间的加密数据，网盘服务器端不能解开用户加密的数据。

（6）测试环境：在一台计算机中安装此系统，共享出一块安全的存储空间。其它计算机可从 internet 等有线网络和 wifi 等无线网络安全登录此网络存储空间，并实现数据信息的安全传输和加密存储功能。

注：不能使用开源软件实现，不能直接调用 SSL、TLS 或 IPSec 等加密协议开源软件和函数实现。

题目 2：面向互联网中大型路由网络的自动探测和测绘系统设计与实现

（1）互联网路由网络的探测与测绘技术，旨在绘制出全球互联网的逻辑结构图（基于自治域、路由路径）和物理结构图（基于设备、地理位置）。互联网路由的本质是 “自治系统” 之间的互联。每个 AS 拥有独立的 IP 地址块和路由策略，通过 BGP 协议交换可达性信息。测绘的核心对象是：AS、IP 前缀(AS 所宣称拥有的网络地址块)、路由器与链路（构成 AS 内部及 AS 间连接的具体设备与物理/逻辑通道）、路径（数据包从源到实际经过的 AS 序列和路由器序列）。

（2）通过网络路由探测获取原始网络路由数据

主动探测向目标网络发送特制数据包，根据响应推断网络信息。可采用 Traceroute 及其变种程序 Paris-traceroute，同时，可考虑别名解析技术，向同一路由器的不同接口 IP 发送探测，通过分析响应特征（如 TTL 初值、IP-ID 序列）来判断这些 IP 是否属于同一台物理设备，从而将“IP 图”合并为“路由器图”。

被动监听是在不发送探测流量的情况下，收集网络自身产生的数据。可通过 BGP 路由信息监听，部署路由收集器，与多个 AS 建立 BGP 对等会话，接收并记录来自全网的 BGP 更新消息。也可直接参考 RouteViews 和 RIPE RIS 公共项目，提供全球数百个对等点的 BGP 表数据和更新流。这是绘制 AS 级拓扑和 IP 前缀-AS 映射关系的最权威数据源。

此外，也可参考公共数据集，收集互联网公开信息，如 WHOIS/RDAP 数据库（记录 IP 块和 AS 的注册信息）、IRR（互联网路由注册库，记录路由策略）、DNS 记录（尤其是反向解析 PTR 记录，常包含路由器接口命名信息）、证书透明日志（可发现域名对应的 IP）等。

（3）将探测到的原始数据整合、关联、推理，形成结构化的路由网络拓扑。

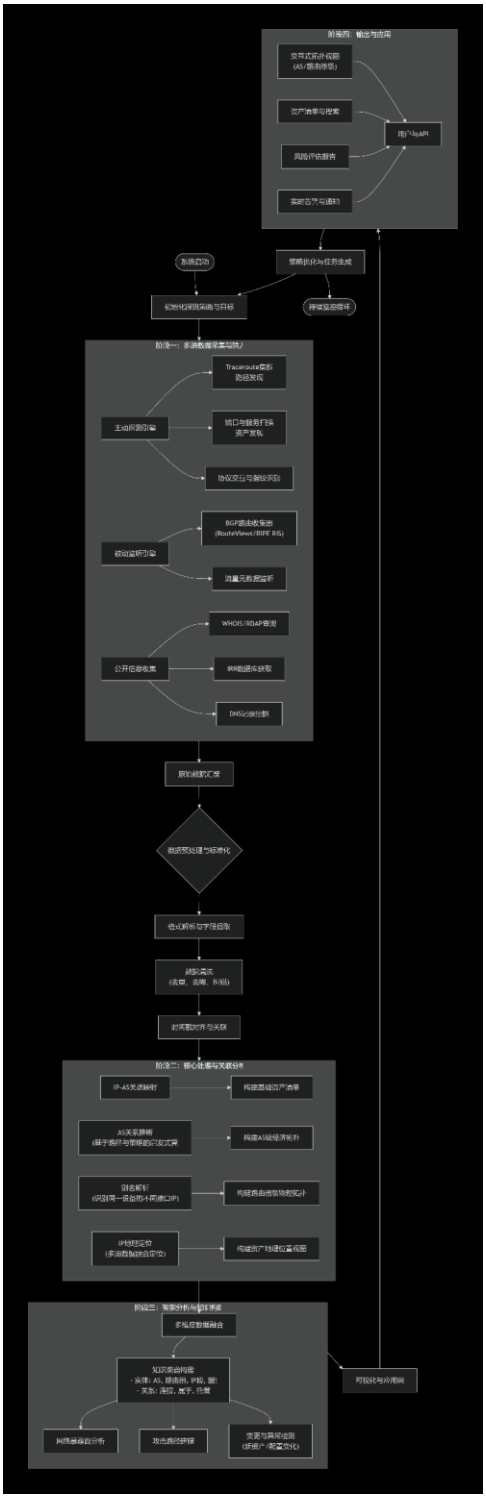
AS 级拓扑构建：首先，从 BGP 路径推导分析 BGP 更新消息中的 AS_PATH 属性。一条路径 AS1 → AS2 → AS3 表明 AS1 通过 AS2 连接到 AS3。海量路径数据聚合后，可以构建出 AS 之间的连接图。其次，推断 AS 间关系。可参考使用启发式算法（如 CAIDA 的 AS 关系推断算法）：在一条 AS_PATH 中，如果一个 AS 出现后又再次出现，通常第一次出现是作为供应商，第二次是作为客户。结合 WHOIS 的注册信息（所属公司）和 IRR 数据，可以高精度地推断出连接类型，从而绘制出互联网的经济拓扑。

路由器级拓扑与地理定位：首先，完成路径集成与别名解析： 将从全球多个探测点（如 CAIDA Ark 项目）发起的 traceroute 结果汇集，形成一个巨大的“IP 跳”图。其次，完成 IP 地理定位：并非直接探测，而是通过多技术融合的数据库查询。基于注册信息的定位：使用 WHOIS 中 IP 块的注册地址（精度低，常到城市级别）。基于地标/路由拓扑的定位： 先

精确定位一批已知位置的地标 IP（如大学 Web 服务器），目标 IP 若与某个地标在路由上非常接近（共享前缀、路径重合度高），则推断其地理位置相近。

（4）测试环境：针对互联网中广域网的大型路由网络，开展实网中路由网络的自动探测和拓扑测绘。

可参考的设计实现思路（无标准答案）：



题目 3：开源软件中后门木马和安全漏洞检测系统设计与实现

（1）针对 JAVA、Python、Go、C/C++语言的开源软件源代码，通过静态和动态的检测方法，检测代码中是否存在后门木马和安全漏洞等恶意代码，这类恶意代码可造成安装此类开源软件后，导致信息外泄或计算机被控制。可采用下面静态和动态的检测方法，开展检测系统的设计与实现。

（2）静态分析

通过分析源代码的语法、语义、控制流、数据流等来检测安全问题。可考虑采用下面技术实现静态代码安全分析

a.模式匹配：基于已知的漏洞模式或恶意代码模式进行匹配。例如，检测到代码中有执行系统命令的函数调用，且参数部分来自不可信的输入。

b.数据流分析：跟踪数据从输入点到敏感操作（如执行命令、写入文件）的路径。

c. 控制流分析：分析程序的控制流图，寻找异常的流程，如跳转到恶意代码的片段。

d. 污点分析：将来自外部的输入标记为“污点”，并跟踪污点数据在程序中的传播，如果污点数据到达了敏感操作点而没有经过过滤、条件限制，则可能有漏洞。

e.依赖检查:通过分析软件中使用的第三方库，与已知漏洞数据库（如 CVE）进行比对，发现已知漏洞。

以后门木马为例，静态分析可能会寻找一些特定的恶意行为模式，比如：非正常的网络连接（连接到可疑地址）、未授权的文件读写、执行系统命令、代码混淆或加密（试图隐藏恶意代码）、异常的权限提升等。

（3）动态分析

动态分析在运行程序时监控其行为，可以检测到实际运行中才暴露的问题。动态分析可以捕捉到运行时的行为，但对于代码覆盖不全，可能无法触发所有的恶意代码路径。可考虑动态监测：

a. 系统调用监控：监控程序运行时的系统调用，查看是否有恶意操作。

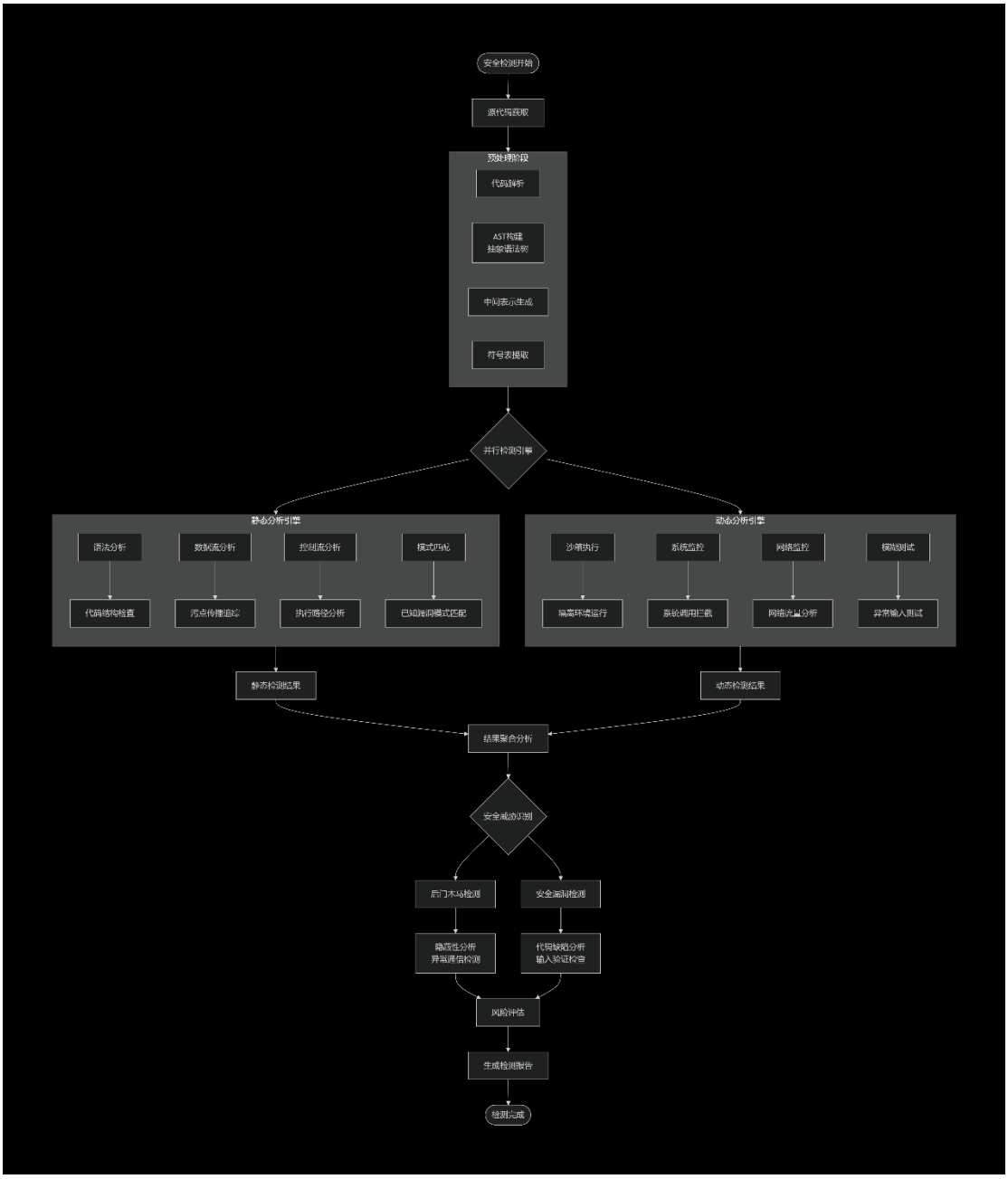
b. 网络活动监控：监控程序是否有可疑的网络连接。

c. 文件活动监控：监控程序对文件的读写，特别是敏感文件。

d. 内存分析：检测内存中是否有恶意代码注入。

（4）测试环境：下载并构建国内或国外开源软件的待测试目标环境，开展后门木马和安全漏洞检测。

可参考的设计实现思路（无标准答案）：


安全检测开始
源代码获取
预处理阶段
代码解析
AST构建
抽象语法树
中间表示生成
符号表提取
并行检测引擎
静态分析引擎
语法分析
数据流分析
控制流分析
模式匹配
代码结构检查
污点传播追踪
执行路径分析
已知漏洞模式匹配
动态分析引擎
沙箱执行
系统监控
网络监控
模糊测试
隔离环境运行
系统调用拦截
网络流量分析
异常输入测试
静态检测结果
动态检测结果
结果聚合分析
安全威胁识别
后门木马检测
安全漏洞检测
隐蔽性分析
异常通信检测
代码缺陷分析
输入验证检查
风险评估
生成检测报告
检测完成

题目 4：基于 C2 的 Linux/Windows 操作系统中的远程控制软件设计与实现

（1）基于 C2（Command and Control，命令与控制）系统的远程控制系统，是现代高级持续性威胁（APT）和恶意软件的核心，从传统的“集中式命令”演变为 “去中心化、隐蔽化、云化”的复杂网络。在 Linux 或 windows 系统最新版本中，开发一款远程控制软件。可从控制端对被控端计算机进行远程控制和信息获取，针对杀毒软件应具有免杀能力。同时，考虑远程控制软件在被控端的隐藏植入技术、自启动技术、自隐藏、自动网络链接，以及针对杀毒软件基于行为的主动防御功能的绕过技术。

（2）攻击者控制端具有图形化或 Web 版的管理控制台，用于查看在线主机、下发任务、收集数据。攻击者通过高度匿名化网络（如 Tor、多层跳板）接入，避免直接暴露真实 IP。

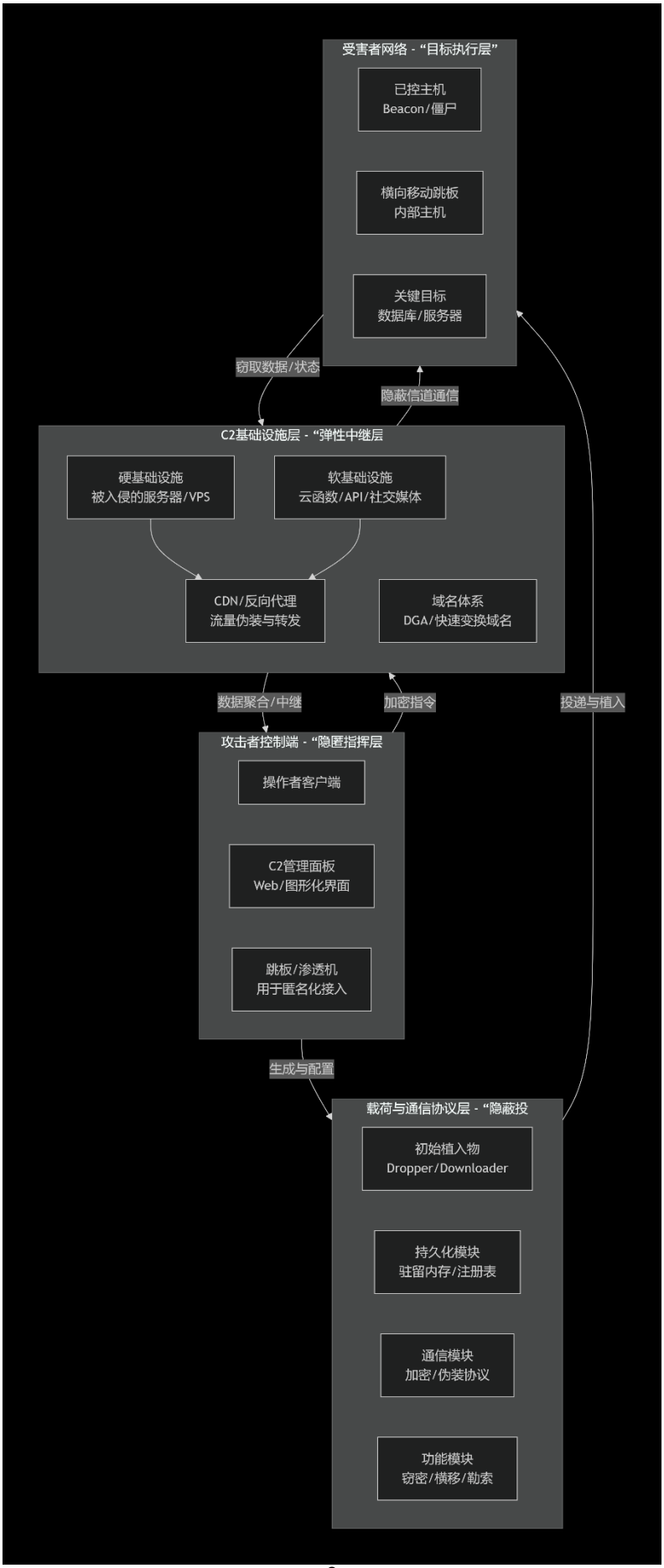
（3）C2 基础设施层作为攻击者和受害者之间的中介与缓冲，提高生存性和抗打击能力。作为传统 C2 服务器可采用硬件服务器，也可采用公有云服务作为无服务器 C2 或存储中继。这些服务信誉好、流量混杂，难以被简单封禁。流量伪装层使用 CDN（如 Cloudflare）或反向代理服务，将恶意流量隐藏在大量合法流量中，并隐藏真实 C2 服务器的 IP。采用域名生成算法（DGA） 生成大量伪随机域名，或频繁更换域名，逃避基于域名的封锁。

（4）通信协议层负责与受害者主机建立连接、维持心跳、执行指令、回传结果。常见采用 HTTP/HTTPS 伪装、DNS 隧道、云服务协议滥用通道作为指令传输通道。

（5）被控端程序安装在可执行攻击指令的被控端计算机终端根据指令进行横向移动、权限提升、数据窃取、环境破坏等操作。可采用下载器用于下载完整的 C2 载荷，内存驻留模块常驻内存负责定期回连 C2、获取指令、执行并返回结果，持久化模块确保系统重启后能重新激活。

（6）测试环境：搭建基于 C2 的 Linux/Windows 操作系统中的远程控制软件靶场环境，开展 C2 和远程控制软件功能验证。

可参考的设计实现思路（无标准答案）：


受害者网络 - “目标执行层”
已控主机
Beacon/僵尸
横向移动跳板
内部主机
关键目标
数据库/服务器
窃取数据/状态
隐蔽信道通信
C2基础设施层 - “弹性中继层
硬基础设施
被入侵的服务器/VPS
软基础设施
云函数/API/社交媒体
CDN/反向代理
流量伪装与转发
域名体系
DGA/快速变换域名
数据聚合/中继
加密指令
投递与植入
攻击者控制端 - “隐匿指挥层
操作者客户端
C2管理面板
Web/图形化界面
跳板/渗透机
用于匿名化接入
生成与配置
载荷与通信协议层 - “隐蔽投
初始植入物
Dropper/Downloader
持久化模块
驻留内存/注册表
通信模块
加密/伪装协议
功能模块
窃密/横移/勒索

（二）综合性题目

题目 1：基于物联网设备芯片可信根的 OTA 安全加密更新机制设计与实现

（1）OTA（Over-The-Air）是一种通过无线网络远程下载并安装软件更新、固件升级或配置更改的技术，无需物理连接设备即可实现远程升级。OTA 安全更新的原理是在不可信的网络信道中，安全、可靠地将新版固件交付给设备，并确保其完整性和真实性。它解决传输过程防窃听，固件版本防篡改，固件来防伪造。

（2）一个完整的 OTA 安全更新系统包括：第一，厂商管理的升级服务器，负责存储、管理和分发已加密签名的固件包。第二，需要升级的智能设备，内置 OTA 升级客户端和安全启动模块。第三，密钥管理系统。

（3）身份认证与完整性保障模块

服务器端签名验证：使用厂商持有的私钥，对固件的哈希值（如 SHA256）进行加密，这个加密结果就是“签名”。然后将“固件+签名”打包下发。

设备端签名验证：设备出厂时已预置了对应的厂商公钥。它先计算下载固件的哈希值，再用公钥解密“签名”，得到服务器当初计算的哈希值。对比两个哈希值，如果一致，则证明：固件未被篡改（完整性）；固件来自合法私钥持有者（真实性）。

（4）传输内容保密模块

对称加密：服务器和设备共享一个预置的密钥。服务器用该密钥加密整个固件包，设备用同一密钥解密。效率高，但密钥管理安全性要求高。

非对称加密：使用设备的公钥加密（设备预置自己的私钥）。更安全，但加密大量数据效率低。通常用于加密一个临时生成的对称会话密钥。

（5）设备端芯片固件安全启动

OTA 安全加密升级的根本保障在于基于硬件芯片可信根的固件安全启动机制。设备上电后，首先运行不可更改的 Bootloader。它会去验证将要加载的应用程序固件（即 OTA 升级后的固件）的数字签名。Bootloader 使用预置的公钥验证应用程序的签名。只有验签通过的固件才会被加载执行。即使 OTA 过程被攻破，恶意固件被写入，在启动阶段也会被安全启动机制拦截，设备会“变砖”而不是运行恶意代码。

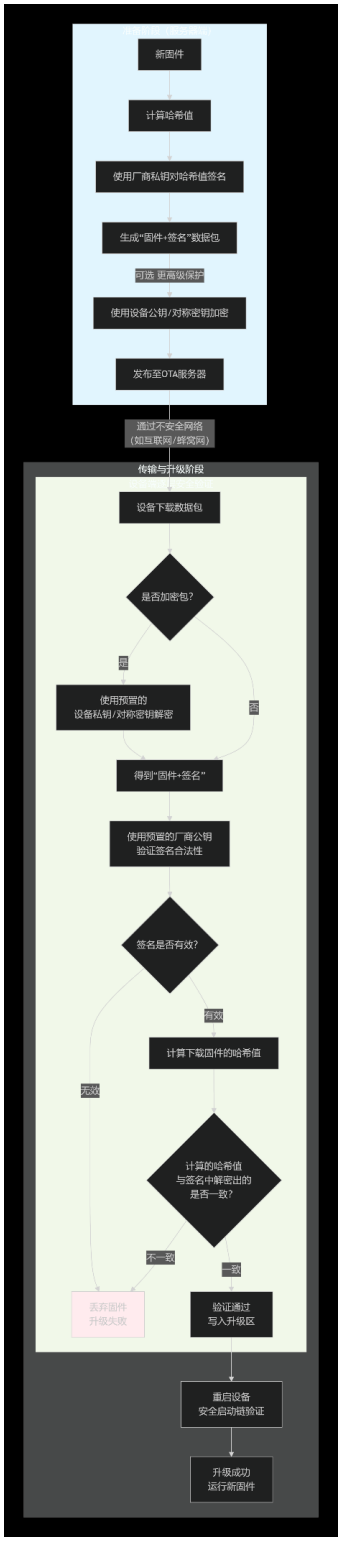
（6）密钥管理的支撑保障

根密钥用于签名固件的私钥，是系统的信任根，离线或硬件保护。设备密钥是每个设备预置的唯一密钥（用于身份标识或解密）。密钥轮换是设计支持未来更新设备中的公钥，以

应对私钥泄露的风险。

（7）测试环境：搭建基于设备芯片硬件可信根的 OTA 加密升级的靶场环境，开展 OTA 加密升级程序的验证。

可参考的设计实现思路（无标准答案）：



题目 2：基于主机日志、主机行为、网络流量的恶意攻击行为溯源分析系统设计与实现

（1）完成主机日志、主机行为、网络流量等多源数据采集与融合

主机日志采集与分析：1)日志的时间序列对齐，统一不同主机和设备的时钟源，确保事件时间准确性；2)日志范式解析：将不同格式的日志转换为统一范式；3)关键信息提取：识别日志中的关键实体（用户、进程、文件、注册表键值）;4)登录会话重建：通过登录/注销事件重建用户会话时间线和源 IP。

主机行为监控：1）系统调用拦截：在内核层监控所有系统调用，捕获文件、进程、网络操作；2）进程行为链分析：构建进程父子关系树，识别异常进程创建模式；3）文件操作监控：监控文件创建、修改、删除、读取操作，检测敏感文件访问；4）内存行为分析：检测进程内存中的异常代码注入和反射加载。

网络流量分析：完成流量捕获与解析、异常协议行为建模、网络会话重建、隐蔽信道检测（识别 DNS 隧道、HTTP 隐蔽信道、ICMP 隧道等）。

（2）完成攻击链的检测与关联分析

基于 ATT&CK 框架的攻击链识别，将检测到的事件映射到 ATT&CK 的不同阶段；识别同一攻击者使用的多个技术之间的逻辑关系；与已知 APT 组织的攻击剧本进行相似性匹配。

多源数据时间线关联分析，通过在特定时间窗口内聚合相关事件，基于时间先后和逻辑关系推断事件因果关系，从而识别攻击各阶段的时间间隔和模式。

实体关系图构建，从日志和流量中抽取实体并建立链接关系。

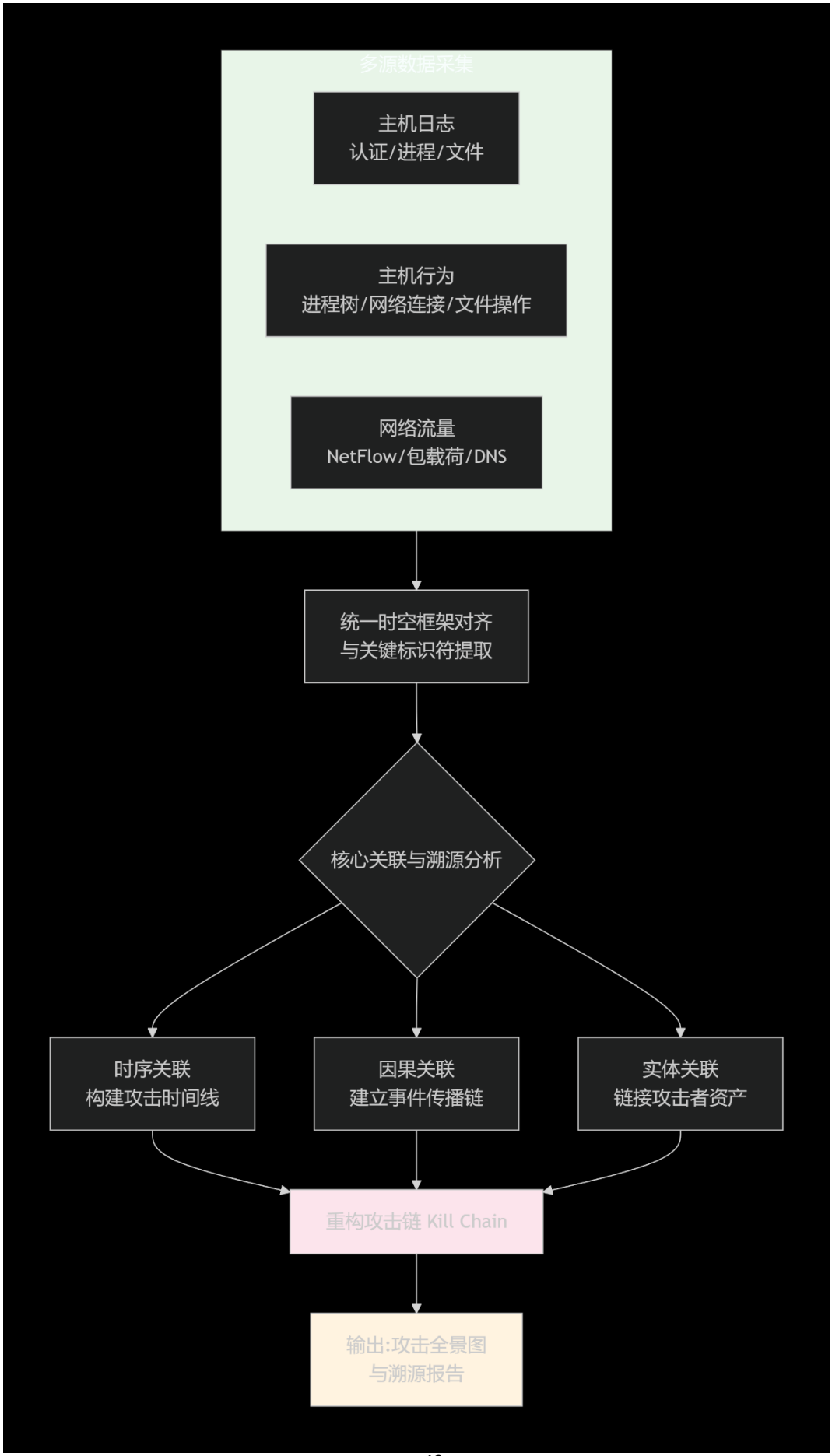
（3）攻击溯源关键技术

攻击路径重建，首先，通过边界设备日志识别初始入侵点；其次，基于认证日志和网络连接追踪攻击者在内网的移动路径；最后，分析权限提升路径分析，发现跟踪数据从存储到外传的完整路径。

攻击者身份溯源，从攻击工具、脚本、配置文件中提取攻击者指纹特征，分析攻击者和 C2 服务器的基础设施关联信息，包括分析 C2 服务器的注册信息、历史记录、关联域名等；开展行为模式分析和组织特征匹配，与已知 APT 组织的 TTP 进行匹配分析。

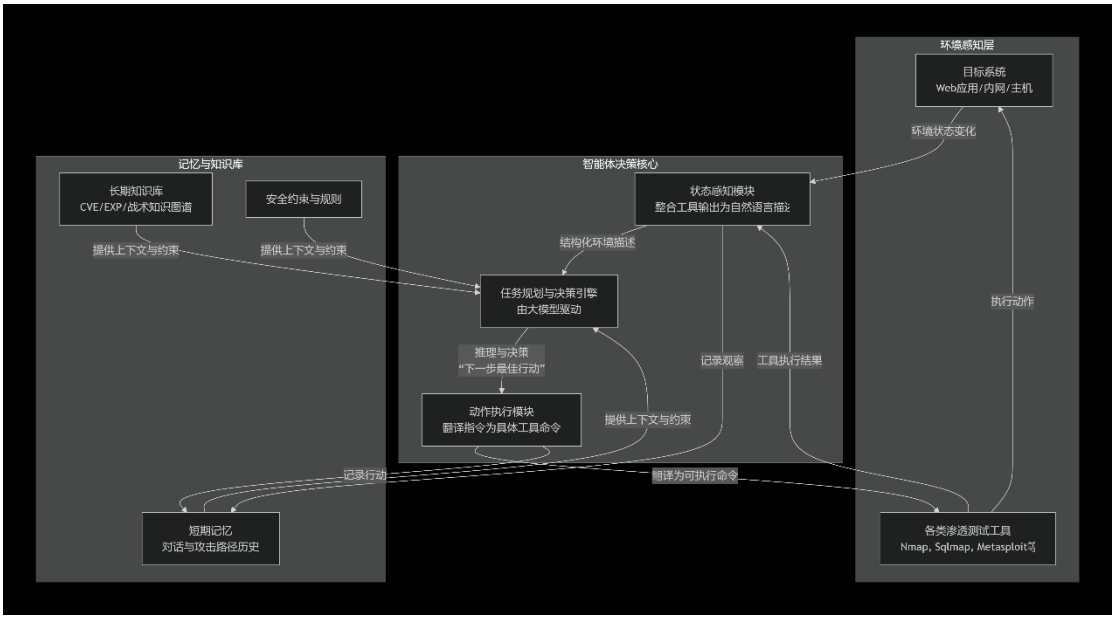
（4）测试环境：搭建包含不少于 5 个节点的靶场环境，在靶场环境中，开展主机日志、主机行为、网络流量等多源数据采集下的恶意攻击行为溯源分析结果验证。

可参考的设计实现思路（无标准答案）：


多源数据采集
主机日志
认证/进程/文件
主机行为
进程树/网络连接/文件操作
网络流量
NetFlow/包载荷/DNS
统一时空框架对齐
与关键标识符提取
核心关联与溯源分析
时序关联
构建攻击时间线
因果关联
建立事件传播链
实体关联
链接攻击者资产
重构攻击链 Kill Chain
输出:攻击全景图
与溯源报告

题目 3：基于智能体与大模型的自动化渗透决策系统设计与实现

（1）基于智能体和大模型的自动化渗透决策系统的原理，是将大模型的战略性、关联性推理能力与渗透工具的海量战术执行能力相结合，通过一个感知-决策-行动-学习的自主闭环，模拟人类渗透专家的思维过程，实现网络攻防的认知自动化。传统自动化渗透工具（如 Metasploit 的自动化脚本）本质上是预设流程的线性执行。而基于智能体的系统是基于目标的动态决策循环。一个典型的自动化渗透决策系统包含以下核心模块，它们协同工作，形成一个 “观察-思考-行动” 的强化学习式闭环。



（2）工作流程说明

第一，实现状态感知：系统通过工具扫描（如发现开放了 80 端口，运行 Nginx 1.18）或直接交互，将非结构化的机器输出（命令行结果、HTTP 响应）转化为结构化的自然语言描述，供大模型理解。

第二，实现决策与规划：大模型接收到当前状态、历史行动和最终目标（如“获取 Web 服务器根权限”）。进行战略规划和战术选择，战略规划是分解大目标为子任务（如：信息收集 -> Web 漏洞探测 -> 获取 Webshell -> 提权 -> 内网横向移动）。战术选择是根据当前状态，选择最有可能成功的具体技术（如：看到?id=1，决定尝试 SQL 注入；看到 upload.php，决定测试文件上传漏洞）。

第三，开展动作执行：决策引擎输出一个高级动作指令（如“对/login.php 进行基于字典的密码爆破”）。执行模块将其翻译为具体的工具命令（如调用 hydra 命令），并在受控环境中安全执行。

第四，学习与适应：系统记录“状态-动作-新状态-奖励”四元组。成功（如发现漏洞）获得正奖励，失败或造成破坏（如导致服务崩溃）获得负奖励。最终实现优化未来的决策。

（3） 大模型和智能体的支撑技术

第一，大模型作为系统的大脑，负责理解复杂、模糊的网络环境，进行因果推理（“因为返回了 SQL 错误，所以可能存在注入点”）、知识关联（“这个 Struts2 版本对应 CVE-2017-5638”）和创造性思维（“尝试将 XSS 与 CSRF 组合攻击”）。输入是渗透领域微调过的提示词，包含目标、约束、当前状态、历史动作。输出是结构化的下一步行动建议。

第二，工具调用与自动化集成的需求。系统将大模型的决策动作落地，需要工具库的支持，将自然语言指令映射到具体的工具调用，需要构建包含侦察工具（nmap, dirsearch, subfinder 等）、漏洞利用工具（sqlmap, Metasploit 模块, 自定义 EXP 等）、后渗透工具（Mimikatz, BloodHound, 端口转发工具）等，工具执行可在沙箱环境中开展验证。

第三，知识增强通过长期记忆和短期记忆来实现。长期记忆可构建向量数据库存储渗透知识（CVE 详情、攻击技术 TTPs、Payload、以往的成功案例），供大模型在决策时检索（RAG）。短期记忆可记录当前渗透测试的完整上下文，确保动作连贯，避免循环重复。

第四，多智能体协作。复杂渗透需要团队分工，为此系统可部署多个智能体来协同实现。侦察智能体可专注于信息收集和资产发现，攻击智能体可专注于漏洞利用和初始入侵，横向移动智能体可专注于内网渗透和权限提升。协调智能体可接收各智能体汇报，综合信息，分配新任务。

（4）测试环境：搭建包含 2 层防护网络不少于 10 个节点的网络靶场运行环境，应用基于智能体和大模型的自动化渗透决策系统，实现对靶场环境的自动化渗透最优决策，开展靶场环境的自动化渗透。

（三）开放性题目

题目可自拟、可请辅导老师讨论出题，综合运用信息安全、网络安全、密码技术等专业相关理论与技术，围绕真实场景提出问题，完成一个完整的安全问题分析与解决方案设计。

通过“课程设计—创新训练—学科竞赛”相结合的方式，培养学生发现问题、分析问题和解决复杂工程问题的能力，为后续参加中国国际大学生创新大赛及相关学科竞赛奠定基础。

题目评审：以 ppt 介绍和作品演示的方式进行题目验收，评审规则如下：

评审要点	评审内容	分值
个人成长	1.**立德树人。**项目弘扬正确价值观，厚植家国情怀，恪守伦理规范，有助于培育创新精神。 2.**调研深入。**项目扎根中国大地了解国情民情，鼓励学生深入社会、行业、实验场所选题立项、调查研究、试验论证。 3.**逻辑正确。**项目符合将专业知识与商业知识有效结合并转化为商业价值或社会价值的创新创业基本过程和基本逻辑，展现创新教育对大学生基本素养和认知的塑造力。 4.**知识掌握与应用能力。**体现对创新创业所需知识（专业知识、商业知识、行业知识等）与技能（计划、组织、领导、控制、创新等）的娴熟掌握；体现用课堂和实验室学到的知识解决实际问题的综合能力和高级思维；体现项目成长对团队成员创新精神、创新意识、创新能力的锻炼和提升作用，展现创新教育提升大学生综合能力的效力。 5.**人才培养成效。**项目能充分体现院校扎实推进新工科、新医科、新农科、新文科建设方面取得的成果；体现院校在项目的培育、孵化等方面的支持情况；体现产教融合、科教融汇、多学科交叉、专创融合、产学研协同创新等模式在项目的产生与执行中的重要作用。	30
项目创新	1.**问题导向。**项目遵循从创意到研发、试制、生产、进入市场的创新一般过程，进而实现从创意向实践、从基础研发向应用研发的跨越。 2.**目标导向。**团队能够基于学科专业知识并运用各类创新的理念和范式，解决社会和市场的实际需求。 3.**创新成效。**项目能够从产品创新、工艺流程创新、服务创新、商业模式创新等方面着手开展创新创业实践，并产生一定数量和质量的创新成果以体现团队的创新力。	30
产业价值	1.**产业认知。**对所在产业（行业）的产业规模、增长速度、竞争格局、产业趋势、产业政策等情况充分了解，形成完备、深刻的产业认知。 2.**市场定位。**项目具有明确的目标市场定位，对目标市场的特征、需求等情况有清晰的了解，并据此制定合理的营销、运营、财务等计划，设计出完整、创新、可行的商业模式，展现团队的商业思维。 3.**落地前景。**项目落地执行情况，对促进区域经济发展、产业转型升级的情况；已有盈利能力或盈利潜力情况。项目是否具备国际化发展的潜力。 4.**社会影响。**项目直接或间接带动就业的数量和质量，对社会文明、生态文明、民生福祉等方面的积极推动作用。	25
团队协作	1.**团队精神。**团队具有明确的使命愿景，具有团结协作的创新精神，具有支撑项目成长的知识、技术和经验。 2.**团队结构。**团队的组织构架、人员配置、分工协作、能力结构、专业结构、合作机制、激励制度等的合理性情况。鼓励留学生参与，促进中外合作交流。 3.**团队效能。**团队与项目关系的真实性、紧密性情况；对项目的各项投入情况；创立创业企业的可能性情况。 4.**团队资源。**支撑项目发展的合作伙伴等外部资源的使用以及与项目关系的情况。	15

二、课程设计组队方法

基础性题目每个题目最多 5 人组成开发小组，合作完成。

综合性题目每个题目最多 10 人组成开发小组，合作完成。

开放性题目最多 10 人组成开发小组，合作完成。

可在班内或班间自由组合，在任务分工文件中详细描述各个成员的分工，以及相应的工作量占比。

三、课程设计考核方式

1. 报告提交要求：打包提交任务分工说明、作品技术原理介绍、概要设计报告、详细设计报告、测试分析报告、程序编译和安装使用文档、程序源代码、ppt、截屏录像。包命名方式：组长班级+组长姓名+学号.rar/ZIP。

2. 考核要求：采用 ppt+现场产品展示的方式，ppt 和文档报告按照功能完成情况、技

术可行性和合理性、技术的难度和工作量、内容条理性、格式规范性进行考核打分。现场作品根据小组提交程序的完成情况、完成的功能、稳定性、存在问题的多少、技术的合理性、技术的难度和自主性、程序的开发工作量等给予打分。

3.分组表和答辩顺序：各班学委将分组表汇总到大班学委，大班学委将分组表发到email：yuanjie@bupt.edu.cn 和 cuibj@bupt.edu.cn 中，包括分组序号、所选题目号、组长（留手机号）和组员的学号和姓名、班号，按照班号由小到大排序，答辩顺序按照组长学号顺序由小到大答辩。

4.课程考核信息：2026 年 1 月 16 日验收考核，地点沙河校区 N108，每组进行 10 分钟的 ppt 介绍和作品演示（每组限制时间），提前到教室来试好演示环境。考核的顺序：按照班号由小到大排序，每个班按照组长的学号由小到大为顺序先后介绍。上午 8：00－12：00，下午 1：00－全部答辩完。按照老师意见修改并完成报告和提交材料，晚上 20 点前提交报告至 email：yuanjie@bupt.edu.cn。

建议同学提前一天自行去教室测试环境和设备，保证验收时的正常演示。

四、授课老师联系方式

崔宝江 13611330827　苑洁 13810019079 李灵慧 15510108093

课程群二维码


群聊：2025课程设计群
该二维码7天内(1月19日前)有效，重新进入将更新
保存图片