家庭网络安全技术白皮书

目录

第一章 概要 3
1.1. 安全概要 3
1.2. 互联网时代家庭网络 3
1.3. 家庭网络安全风险逐渐增大 4
第二章 家庭网络安全分析 5
2.1. 分析方法论 5
2.2. 家庭网络三个平面的威胁 6
2.2.1. 数据平面 6
2.2.2. 控制平面 6
2.2.3. 管理平面 6
第三章 家庭网络安全技术 7
3.1. 安全审计 7
3.2. 通信安全 7
3.3. 密码学支持 8
3.4. 用户数据保护 8
3.5. 标识和鉴别 9
3.6. 安全管理 9
3.7. 隐私保护 10
3.8. 安全功能保护 10
3.9. 资源利用 11
3.10. 访问控制 11
3.11. 可信路径 12
3.12. 硬件保护 12
3.13. 其他 13
第四章 总结 13

第一章 概要

1.1. 安全概要

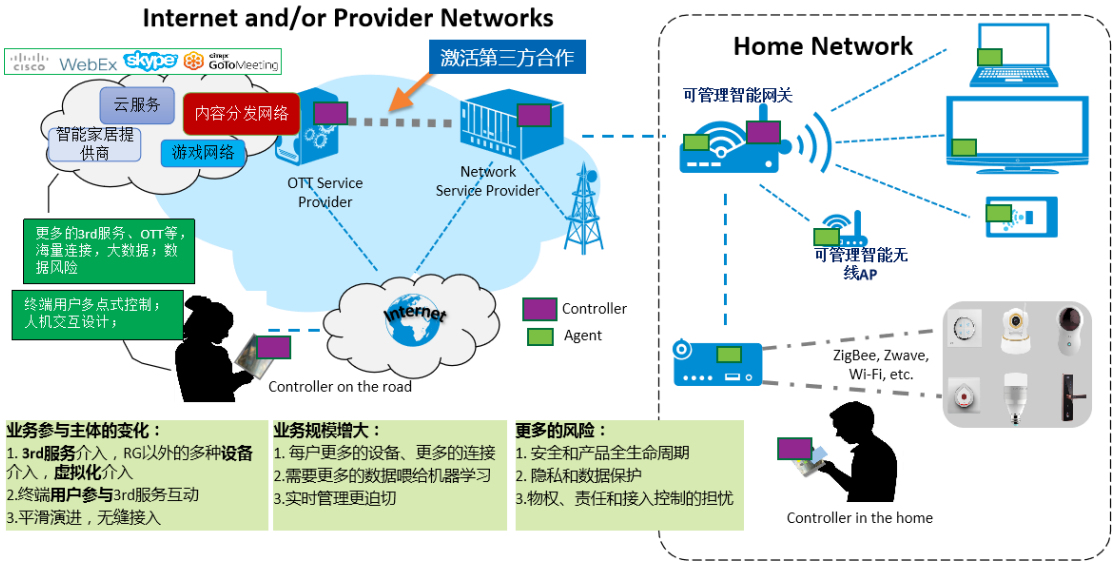
安全的目标是数据、客体和资源。确保目标安全的三原则为机密性(Confidentiality)、完整性（Integrity）、可用性（Availability）。机密性确保信息不会泄露给未授权的主体，其主要威胁来自于监控流量、盗取密码文件、社会工程等等。相应的防护措施包括加密传输数据、加密磁盘、培训教育等。完整性确保信息和系统不被恶意或者意外篡改；其主要威胁来自于篡改数据、删除文件、植入病毒等；相应的防护措施包括校验和、散列、数字签名、访问控制等。可用性确保授权用户能够对数据和资源进行及时的、可靠的访问；其主要威胁来自于自然灾害、设备故障、拒绝服务攻击等；相应的防护措施包括异地备用设施、冗余配置、数据备份、业务连续性等。

从以上可以看出，安全本质其实是策略、过程和技术的综合体。

1.2. 互联网时代家庭网络

数字家庭网络是计算机、家电、通信设备等多种技术综合的产物，通过家庭网关(Home Gateway)将 Internet 网络功能以及业务应用延伸至家庭内部，并通过各种有线或者无线技术，连接各种信息终端，提供数据、语音、多媒体、物联网、智能家居、网管等业务功能，达到信息能够在家庭信息终端内部以及 Internet 充分流通和共享。

在互联网时代，家庭网络概念的进一步扩展和外延，万物互联，带来更多的机会和痛点。电信运营商和消费电子供应商业务的发展，带来更海量的连接设备；第三方业务蓬勃发展，云+端模式需要中间的更灵活的电信通信管道；业务规模大增，产生的数据更多，人工智能管理家庭网络应运而生；更大规模用户家庭信息的数字化，要求更更健康的隐私和数据保护。



1.3. 家庭网络安全风险逐渐增大

家庭网络快速发展带来巨大的便利性的同时，安全问题也随之突出。当前家庭网络安全面临的主要问题，从安全三原则角度看，包括：

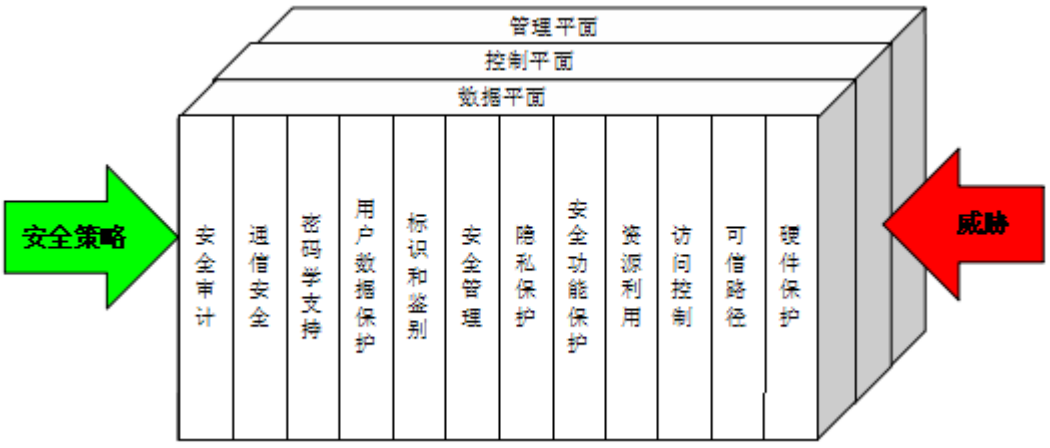
a) 家庭内部信息机密性被破坏，家庭内部信息泄露、截取、盗取等，相应的手段包括钓鱼网站、木马、病毒、冒充等。

b) 内部信息的完整性得不到保证，被恶意程序篡改或者删除。

c) 内部信息的可用性不完整，无法及时可靠的访问，被 DoS 攻击、被木马病毒删除、修改密码、设备故障等方式不可得。

第二章 家庭网络安全分析

2.1. 分析方法论



家庭网络设备安全分析

为了抵御来自外部网络、家庭内部的攻击，家庭网络基础设施设备必须具有一定的安全功能。安全功能包括：

a) 安全审计：能够提供日志等审计记录，这些记录可以用来分析安全威胁活动和指定安全对策，探测违背安全性的行为；

b) 通信安全：确保信息的发送者和接收者的身份不可抵赖；

c) 密码学支持：利用密码功能来满足安全目的，密码功能可用硬件，固件或软件来实现；

d) 用户数据保护：保护用户数据的完整性、可用性和保密性；

e) 标识和鉴别：确认用户的身份及其真实性；

f) 安全管理：安全功能、数据和安全属性的管理能力；

g) 隐私保护：提供了用户身份及相关数据不被其他用户发现或滥用的保护；

h) 安全功能保护：对实现系统关键功能包括安全功能所需要的数据(如用户身份和密码)的保护，确保相关数据的完整性、可用性和保密性；

i) 资源利用：控制用户对资源的访问，不允许用户过量占用资源，避免因为非法占用资源造成系统对合法业务拒绝服务；

j) 访问控制：管理和控制用户会话的建立；

k) 可信路径/信道：用户或其他设备与本设备之间通信的信道/路径要求可信，对于安

全数据的通信要同其他通信隔离开来；

1） 硬件保护：为了保护信息存储、信息传递和信息计算而增加的硬件资源。

2.2. 家庭网络三个平面的威胁

2.2.1.数据平面

家庭网络数据平面的安全威胁主要有以下方面，但不局限在这些方面：

a) 对数据流进行流量分析，从而获得用户数据的敏感信息

b) 未经授权的观察、修改、插入和删除用户数据，利用用户数据流进行 DoS 攻击。

限制外部用户对家庭网络设备内部目录文件的访问，以保证数据的完整性、可用性和机密性。

基于流量的攻击会对设备的性能造成很大影响，所以需要提供安全机制来限定用户流量行为，抵御来自网络攻击者对数据平面的恶意攻击。

2.2.2.控制平面

控制平面主要负责路由信息的学习，协议的处理和 IP 地址配置等。控制平面的安全威胁主要有以下几个方面，但不局限在这些方面：

a) 对协议流进行探测或者进行流量分析，从而获得转发路径信息

b) 利用协议的拒绝服务攻击，如利用路由协议、ICMP 协议的拒绝服务攻击，利用面向连接协议的半连接攻击等

c) 非法设备进行身份哄骗，建立路由协议的实体信任关系，非法获得转发路径信息

d) 针对路由协议转发路径信息的欺骗

e) DNS 域名劫持

f) 端口扫描，获取开启的服务和发现目标系统的安全漏洞。

2.2.3.管理平面

管理平面的主要功能是实现对设备系统参数配置以及设备状态信息的统计，其可能面临的主要安全威胁包括以下几个方面，但并不局限于这些方面：

a) 未授权的用户非法接入

b) 合法授权的用户越权使用

c) 账号密码的泄露

d) WLAN 采用非安全的加密方式

e) TR069 管理协议的数据泄露

f) 产品硬件上保留了串口等调试接口

第三章 家庭网络安全技术

3.1. 安全审计

所谓安全审计，指按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程，其主要利用了日志审计。安全日志审计，既可以满足企业和组织自身安全要求，能够帮助用户获悉信息系统的安全运行状态，识别针对信息系统的攻击和入侵，以及来自内部的违规和信息泄露，能够为事后的问题分析和调查取证提供必要的信息，又能满足国家法律法规和行业标准规范。

对于家庭网络设备，其系统应能提供安全日志功能，并且日志需要能够部署在开放环境，日志具备足够健壮性；可以对记录攻击端口行为，可以支持安全日志输出，并支持安全传输功能。

安全日志可以通过多种管理媒介如 TR069、WEB、APP、SSH 等启动、停止、查看，与系统时间同步，且对日志本身的操作也需要记录在案。

对常见攻击端口的攻击，需记录其详细信息，如时间、报文信息、IP、次数等。

3.2. 通信安全

通信安全是确保信息的发送者和接收者的身份的不可抵赖性（Non-repudiation）。通信的数据携带有实体特质、不可被模仿复制的信息，确保通信数据是可确认的实体发出的。

家庭网络设备重要的外联渠道 TR069 需要支持 HTTP+SSL/TLS（+证书）认证，支持使用证书方式与 ACS 建立 SSL 连接，支持正向和反向鉴权，支持可选用多级证书链。反向链

接 URL 需要随机且唯一。

加强通信协议安全性，如 TCP 的序列号随机化提供足够的 Relay 攻击防护、DNS 源端口和 ID 随机化降低 DNS 攻击风险。

对于家庭网关产品，其天生处于家庭网络内外部节点位置，对于 LAN 侧的 ARP 报文不得向 WAN 侧转发，同时，对于特殊地址如 IPv4/v6 本地链路地址、IPv4 本地回送地址、广播到局域网内所有主机（all hosts）的地址、直接广播地址、本地链路组播地址、目的地址为私有 IPv4 地址也不得向 WAN 侧转发。私有 IPv4 地址指 CPE/路由器实际使用的 LAN 地址等。

3.3. 密码学支持

密码学支持包括密钥管理和密码运算。密钥管理解决密钥管理方面的问题，而密码运算关注这些密钥的运算使用情况。

密钥在其整个生命周期内都必须进行管理，需要考虑密钥生命周期相关功能，包括：密钥生成、密钥分发、密钥存取和密钥销毁。

为了确保密码运算功能的正确执行，必须按照一个特定的算法和一个规定长度的密钥来进行运算。

家庭网络设备涉及的密钥和密码包括但不限于信息加密的密钥、证书认证的密钥、Wi-Fi 密钥和密码、用于 Digest 和 Basic 认证的密码、设备商生成的用户不同业务帐号和密码。（主要用于注册登录运营商业务服务，包括但不限于：宽带帐号密码、SIP 注册帐号密码和 TR069 帐号密码、云空间帐号密码。）

密钥密码必须是唯一的，密钥应当是随机生成，而不是固定算法计算而出，尤其是不能使用硬编码；密码需要遵循强密码规则，支持密码修改时进行强度校验，且不能使用已经被公开的常用密码。同时，默认密钥和密码应使用高质量熵，不能根据设备 SN、MAC 地址、wifi SSID、产品名称、产品型号等容易获取的信息生成。

针对用户配置和默认配置加密，需采用不同的密钥。存储加密、通讯加密都需要使用可靠算法，摒弃已知不安全的 DES、MD5 等算法；需使用公开算法。

3.4. 用户数据保护

用户数据保护主要包括对用户数据的访问控制、对用户数据的信息流控制以及用户数据

存储和传输的完整性、保密性。

用户帐号、密码、认证使用的私钥、运营商服务器地址、防火墙规则等敏感信息不能以明文存储在 flash 中，需要脱敏，在 TR069、WEB、CLI、APP 等人机交互界面中不能以明文显示。对于客户端的证书需要保证机密性，不得有接口供用户查看、获取。同时针对这些敏感信息，也不得能够明文传输。存储这些敏感信息的配置文件，必须使用加密存储。

需要支持用户 SSID 隐藏，针对家庭网络设备 WAN 侧的路由请求、DNS 转发请求、DHCP 请求、ARP 请求，都应该拒绝。

具备语音功能的家庭网络设备，需要对 SIP 信令合法性过滤和校验功能。

3.5. 标识和鉴别

标识与鉴别是涉及系统和用户的一个过程，标识用于区别不同的用户，而鉴别用于验证用户身份的真实性。

用户鉴别：为用户提供多种鉴别机制，分为一次性鉴别和多重鉴别。

鉴别失败：定义不成功的鉴别尝试次数、时间门限值，终止会话建立进程、使账户无效。

用户身份：建立和验证所声称的用户身份的功能要求；确保用户与正确的安全属性相关联（如身份、组、角色、安全等级）。

Web、Telnet、CLI、SSH 支持用户名与密码多次输错后延时登录，抵御 WPS Brute Force。

具备语音功能的家庭网络设备，需支持 SIP 用户认证。

WEB 需提供登录认证机制，支持 IP+Cookie 方式鉴权，相应的权限需要与账户权限相匹配。

针对插件，需要有权限控制，系统能抵御插件的非法、恶意攻击。受插件攻击中，系统不死机。攻击停止后立即恢复，不需重启设备。

3.6. 安全管理

安全管理方面需要包括：安全功能管理、安全功能的数据管理、安全属性管理、安全角色定义。

命令行配置接口须使用自定义 CLI 或者权限受限的 Shell。WEB 需要支持多级权限账户，并禁止通过 HTTP GET 方法配置数据，配置数据使用 HTTP POST 方法。产品的关键信息如硬件和软件版本号只能通过管理接口查看，未登录不显示系统和应用的标识符。不允许

从设备上提取出任何可执行文件。例如，不能通过 telnet、SSH、web、ftp、samba 等获取可执行文件。

开启相应共享服务时，用户可通过该服务访问对应的业务目录，一般是 U 盘目录/文件和网盘目录/文件（通常在/mnt 目录下），禁止访问其他目录/文件。

错误或者提示信息不能暴露任何有可能泄漏设备内容的信息，例如某页面是否存在等。浏览器查看 WEB 源代码不得显示开发者信息。

版本文件包括版本头和版本内容。版本头存放各种校验数据，用于识别版本文件、校验版本内容。版本文件需要加密。

3.7. 隐私保护

按各国信息安全法律法规，要求为用户身份提供不被其他用户发现或滥用的保护。通常有匿名和假名两种方式。

匿名：确保使用或服务时不暴露用户的身份，对用户的身份提供保护。

假名：同上，但是根据化名能够确定原始用户身份。

用户个人数据有敏感数据和非敏感数据，部分个人数据的归类可能存在一定的争议性。针对家庭网络设备，跟个人相关的帐号信息是比较重点需要关注的范围。

用户的帐号和密码（包括但不限于 web、Telnet、CLI、SSH、SAMBA、FTP、PPPoE、L2TP、IPSec、VoIP、Wi-Fi 等）以及电话号码、SN 等用户个人信息不能输出到日志中，需要脱密处理；同样针对这些数据，不得以明文形式进行存储和传输。针对个人相关数据，个人的主体权利包括查看、修改、清除，同时如果加密传输、存储个人数据，需要有渠道通知到用户，取得用户授权。在运营商开户相关信息、设备本身 SN 等信息，不得发送到运营商之外的目的地。

个人数据处理需要脱敏。脱敏，是指将目标数据进行不可逆的匿名化，导致不能在最终的目标数据上，反推出原始数据；最终的目标数据需要做到易于检查和检验。

WEB 登录用户名和密码框增加 autocomplete="off"属性。该属性用于禁止浏览器保存密码。

3.8. 安全功能保护

对安全功能的保护是安全功能本身的基石。

保证密钥在设备中的存储和分发安全，需要对密钥、证书加密存储；私钥需要保证只能

从管理接口访问，禁止任何网络传输。

版本升级，需要通过加密网络通道获取版本；升级时进行版本和配置的合法性校验，同时对版本可以通过签名等方式进行完整性校验。同样的，针对下载下来的插件，也需要进行合法性、完整性校验。

操作系统 OS 运行支持内存地址随机化机制；对 DNS 请求进行相应过滤，缓解 DNS rebind 攻击。家庭网络设备应能为自身的应用提供可靠的时间戳。

针对 WEB 功能，需要抵御 OWASP 漏洞，如跨站脚本攻击 XSS、格式化字符串攻击、跨站请求伪造（CSRF）等，防止通过管理媒介入口，注入各种非法内容到设备上。用户界面中使用防御性代码，抵御点击劫持（Clickjacking）。

3.9. 资源利用

保证资源的可用性，是系统安全性的基本要求。控制用户和主体对资源的使用，防止出现拒绝服务攻击，如限速、限并发连接数。需求包括：提供容错、资源分配的能力等。

拒绝服务（DoS）攻击保护，该保护作用在所有终结在本设备的 IP。停止攻击后，设备不需重启就能恢复正常工作；攻击过程中，设备不能死机。特别地，TR069 业务和 VOIP 业务的防攻击，攻击停止立即恢复，不需重启。DoS 攻击在一定强度范围内，保证业务连续性。

针对有语音功能的家庭网络设备，满足 RFC4475 的 SIP 健壮性测试要求。主要包括如下：解析器测试、事务层测试、应用层测试。

Public Wi-Fi 更容易受到攻击，需要与家庭 Private 域相隔离。只对 Public 用户提供必要的上网业务，禁止提供额外业务，并对其进行限速控制，避免占用资源太多。抵御来自 Public 用户的攻击，主要是各种 DoS 攻击，并保证不影响家庭网络设备正常业务，不影响 Private 用户使用。

升级过程中，需保证系统的安全。升级前检查升级必备的资源；升级过程中，需限制其重启、恢复出厂、配置修改等操作；升级失败后，系统能够恢复到前一个正常版本状态。

系统需对插件占用 CPU/FLASH/RAM 等系统资源进行控制。插件运行中，保证设备正常工作，插件以外的其他业务不受影响。

3.10. 访问控制

访问控制，按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限

制对某些控制功能的使用。

Web 后台文件中不带有多余、未使用的函数和参数，防止通过构造报文而被修改。

防火墙功能不能被完全关闭，不允许产品定制 Custom 等级。如果使用 Custom，"fwinput" 子链（预置的进入报文）规则会被清空，导致非受控端口泄露。

严禁使用诸如 ping 多少长度报文、组合按键等用户/运营商未知的方法打开访问系统的通道。严禁提供任何工具或服务绕过系统的访问控制，在用户/运营商不知情的情况下访问系统。例如，不允许有 WEB/Shell 等调试页面、商用产品不得有串口排针。产品的 WEB、TELNET、SSH、SAMBA、Shell(包括但不限于)不能提供用户或运营商未知的帐号。

远程管理如 TR069 session 结束后，所有端口必须立即关闭，除了 TR069 协议规定的反向链接端口。Web、Telnet、CLI、SSH 支持用户登陆会话超时后，自动退出登录状态。

如果用户 Wi-Fi 选择已明确不安全的 WEP，需要给出告警，不建议提供该项。

3.11. 可信路径

产品需提供关于用户和安全功能模块之间可信通信路径。通过可信路径交换的信息不会被修改或泄漏，用于需要保密通信的场合。

WAN 侧网管必须使用加密传输通道，或者使用运营商定制的专用通道。建议使用 TR069、OMCI 等专用网管，禁止使用 telnet、SSH、Web 和 UPnP 管理接口。

LAN 侧网管须使用加密传输通道，或者可信通道，建议使用 Web、SSH 管理接口。

TR069、Web 和 TR064 支持 HTTPS，至少支持 TLS1.0 版本，推荐 TLS1.2 以上版本。支持至少 128 位密钥加密。注：SSLv3.0/2.0 存在已知安全漏洞，不建议使用。

SSH 须使用 SSH2.0 以上版本，WAN 侧禁用，LAN 侧酌情开启。

网络通信加密中使用的 RSA 和 DSA 密钥长度不小于 2048 位。

3.12. 硬件保护

硬件保护功能不同于为了提高系统可靠性而提供的冗余硬件。如双电源、硬盘 RAID 等。这里所指的硬件保护是为了保护信息存储、信息传递和信息计算而增加的硬件资源。如为了保护芯片引脚不被探测而额外增加的金属壳封装。为了防止 Flash 被拆除而额外增加的防拆卸硬件等。

对内存、固件芯片防止移动的保护，对于一般用户保证其移动 Flash 模块困难，可采用

BGA 封装方式。

对芯片采用铁盒封装方式防止用户探测引脚信号，防止用户使用第三方工具和硬件对芯片固件进行提取。SoC 支持 Security Boot，防止第三方非法固件烧录。

正式发货的终端设备 PCB 不留任何调试接口(JTAG/串口)，包括插座、焊点、PCB 走线。

防止监听内部通讯总线导致信息泄露，内部总线通讯采用加扰或加密。

3.13. 其他

产品必须保证不置于任何版权和知识产品风险中。提供使用第三方软件的声明。类似 GPL 版权授权风险。

嵌入式 Linux 系统需使用主线长期演进 Linux kernel 版本。

第四章 总结

数字家庭网络作为现代化数字家庭生活的“新基建”，将会承载极具潜力的信息消费新兴市场业务，而安全是数字生活的的基础保障，随着网络威胁日益变大，构筑安全放心的家庭网络环境显得越发重要。通过细致分析安全威胁，部署实施完善的安全策略，迭代应用最新的安全技术，可以最大限度的保护家庭网络中的信息及设备的安全。