Technical White Paper for Home Network Security

Contents

Overview

1.1. Security Overview

The targets of security 2.2are data, objects and resources. The three principles for ensuring the security of the targets are confidentiality, integrity and availability. Confidentiality ensures that information is not disclosed to unauthorized subjects. The main threats to confidentiality are traffic monitoring, password theft, and social engineering. Measures for protecting confidentiality include data encryption, disk encryption, training and education. Integrity ensures that information and systems are not tampered with maliciously or accidentally. The main threats to integrity are data tampering, file deletion, and virus implantation. Measures for protecting integrity include checksums, hashes, digital signatures, and access control. Availability ensures that authorized users can access data and resources in a timely and reliable manner. Its main threats are natural disasters, equipment faults, and Denial of Service (DoS) attacks. Measures for protecting availability include remote backup facilities, redundancy configuration, data backup, and service continuity.

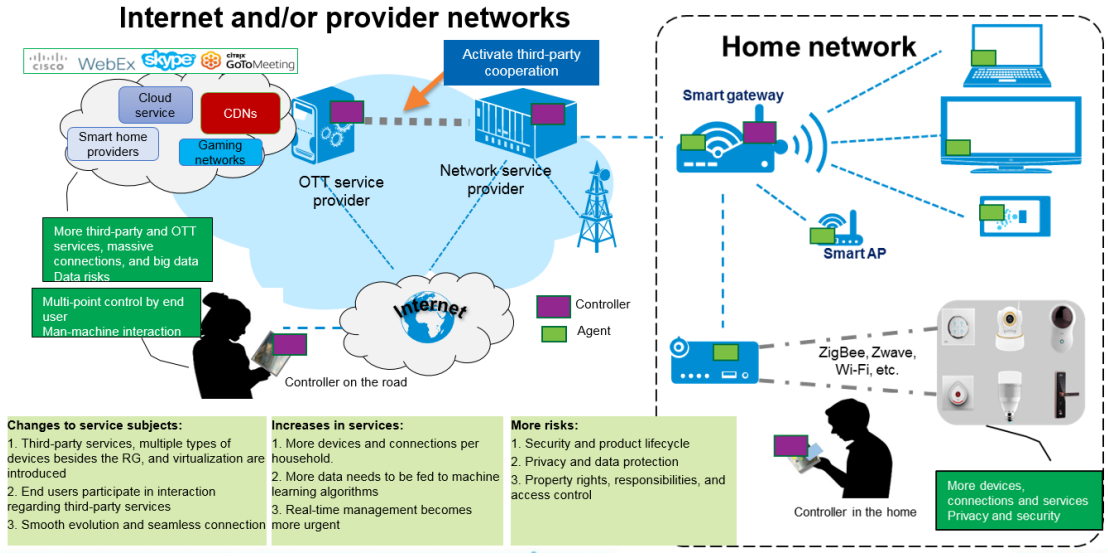
It can be seen from above that security is actually a combination of policies, processes, and technologies.

1.2. Home Networks in the Internet Era

The digital home network consists of multiple technologies including computers, household appliances, and communication devices. It uses a home gateway to extend Internet functions and service applications into the home, while also employing various wired or wireless technologies to connect a range of information terminals to provide such services as data, voice, multimedia, Internet of Things (IoT), smart home, and network management.

In the Internet era, the concept of the home network is expanded to connecting everything, which brings more opportunities and pain points. The service development of

telecommunications operators and consumer electronics suppliers brings about massive connections. With third-party services booming, the cloud + end mode requires more flexible intermediate telecommunications channels. The increase in home network services generates more data, prompting AI-based management of home networks. The digitization of home information on a larger scale requires more robust privacy and data protection.



1.3. Increasing Security Risks Faced by Home Networks

The rapid development of home networks brings both great convenience and notable security issues. According to the three security principles of confidentiality, integrity and availability, major security problems facing home networks can be classified as follows:

a) The confidentiality of home information is compromised, including by leakage, interception and theft through phishing websites, Trojan malware, viruses, and spoofing.

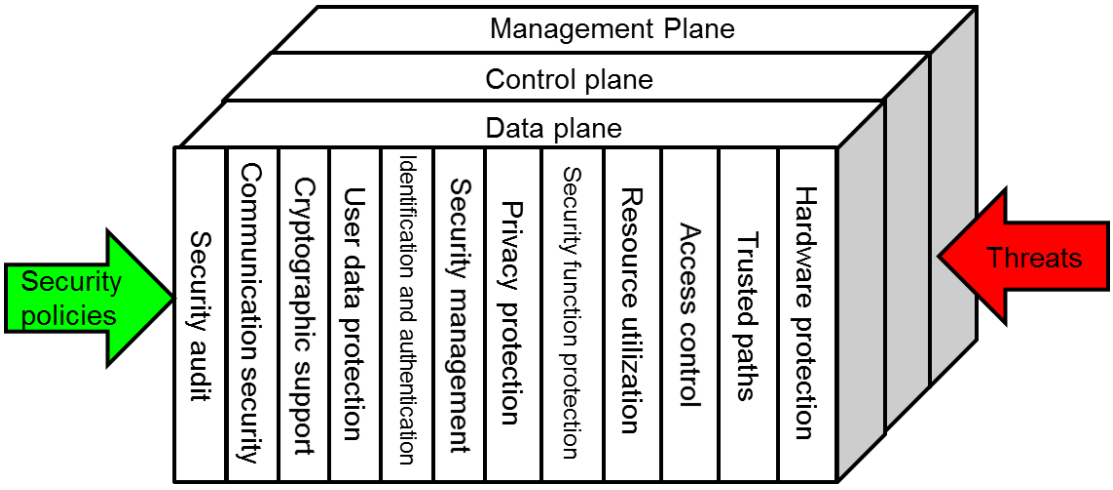
b) The integrity of home information cannot be guaranteed or is tampered with or deleted by malicious programs.

c) The availability of home information is incomplete and cannot be accessed reliably and promptly because of DoS attacks, detection by Trojan viruses,

password tampering, device faults, and so on.

Home Network Security Analysis

2.1. Analysis Methodology



Security Analysis for Home Network Devices

To protect against attacks arising from external networks and in the home, the home network infrastructure must provide certain security functions, including:

a) Security audit: Provides audit records such as logs, which can be used to analyze security threat activities, specify security measures and detect behaviors that violate security.

b) Communication security: Ensures that the identities of the sender and receiver of information cannot be repudiated.

c) Cryptographic support: Uses the password function to serve security purposes. The password function can be implemented by hardware, firmware or software.

d) User data protection: Protects the integrity, availability and confidentiality of user data.

e) Identification and authentication: Confirms the user identity and its authenticity.

f) Security management: Manages security functions, data, and security attributes.

g) Privacy protection: Protects user identities and related data from being discovered

or abused by other users.

h) Security function protection: Protects the data, such as user identities and passwords, required to implement key system functions including security functions. Ensures the integrity, availability and confidentiality of the data.

i) Resource utilization: Controls users' access to resources. Users are not allowed to excessively occupy resources so that the system does not refuse to provide valid services.

j) Access control: Manages and controls the establishment of user sessions.

k) Trusted paths/channels: The paths/channels of communication between other devices and a home network device must be trusted. The communication of security data must be separated from other communications.

l) Hardware protection: Hardware resources are added to protect information storage, information transfer, and information computing.

2.2. Threats to the Three Planes of the Home Network

2.2.1. Data Plane

Security threats to the data plane of the home network include but are not limited to the following:

a) Analyzing data traffic to obtain sensitive information of user data.

b) Observing, modifying, inserting and deleting user data without authorization, and conducting DoS attacks by using user data streams.

The access of external users to the internal directory files of the home network devices should be restricted to ensure data integrity, availability and confidentiality.

Traffic-based attacks have a great impact on device performance. Therefore, a security mechanism is required to restrict users' traffic behaviors and prevent malicious attacks on the data plane conducted by from network attackers.

2.2.2. Control Plane

The control plane is responsible for routing information learning, protocol processing, and IP address configuration. Security threats to the data plane of the home network include but are not limited to the following:

a) Detecting protocol streams or analyzing traffic to obtain forwarding path information.

b) Conducting protocol-based DoS attacks, such as DoS attacks based on routing and ICMP protocols or semi-connection attacks based on connection-oriented protocols.

c) Using illegal devices to conduct identity spoofing and establish an entity trust relationship for a routing protocol, thereby illegally obtaining the forwarding path information.

d) Spoofing for the forwarding path information of a routing protocol.

e) DNS hijacking

f) Conducting port scanning to obtain enabled services and detect security vulnerabilities in the target system.

2.2.3. Management Plane

The management plane of the home network configures device and system parameters and collects statistics on device status information. Security threats to the management plane include but are not limited to the following:

a) Illegal access by unauthorized users

b) Unauthorized use by authorized users

c) Account and password leakage

d) Insecure WLAN encryption

e) TR069 data leakage

f) Debugging interfaces such as serial interfaces are kept on the hardware of the product.

Home Network Security Technologies

3.1. Security Audit

A security audit refers to the process of inspecting, reviewing, and verifying the environment and activities of operation events by using information such as records, system activities, and user activities according to certain security policies. Security audits aim to discover system vulnerabilities, intrusion behaviors, and improve system performance. They main take the form of log audits. Security log audits can meet the security requirements of enterprises and organizations by helping users learn about the secure operation status of information systems, identify attacks and intrusions against information systems, and detect internal violations and information leakages. They can provide necessary information to assist in problem analysis, investigation, and evidence collection. On the other hand, they are required by laws, regulations, and industry standards.

Home network devices should provide the security log function. The logs should be deployed in an open environment and be robust enough. The devices should record port attacks, support security log output, and enable secure log transmission.

Security logs can be enabled, disabled and viewed through a variety of management mechanisms such as TR069, web, apps, and SSH. Log operations are synchronized with the system time and also need to be recorded.

For a common attack on a port, detailed information needs to be recorded, such as the time, packet information, IP address, and number of times.

3.2. Communication Security

Communication security ensures that the identities of the sender and receiver of information cannot be repudiated. Communication data carries information that has entity characteristics and cannot be imitated or replicated. It must be assured that communication data is sent by an entity that can be confirmed.

TR069, which an important mode of external connection for home network devices, needs to support authentication based on HTTP+SSL/TLS certificates. SSL connections between home network devices and the ACS can be established using a certificate, forward and reverse authentication, an optional multi-level certificate chain. The URL of the reverse link must be random and unique.

Communication protocol security should be enhanced. For example, TCP serial numbers can be randomized to provide sufficient relay attack protection, and DNS source ports and IDs can be randomize to reduce DNS attack risks.

The home gateway is located at the entry to the home network and should not forward the ARP packets of the LAN side to the WAN side. It cannot broadcasts special addresses, such as IPv4/v6 link-local addresses, IPv4 local return addresses, addresses broadcast to all the hosts in the LAN, direct broadcast addresses, link-local multicast addresses, and private IPv4 addresses to the WAN side, either. A private IPv4 address refers to an address at the LAN side actually used by the CPE/router.

3.3. Cryptographic Support

Cryptographic support includes key management and cryptographic operation. Key management addresses issues related to the management of keys, while cryptographic operation deals with the operation and use of these keys.

A key must be managed throughout its life cycle. Key management functions include key generation, key distribution, key access, and key destruction.

To ensure that the cryptographic operation function is properly performed, the execution must be based on a specific algorithm and a key with a specified length.

The keys and passwords used by home network devices include but are not limited to information encryption keys, certificate authentication keys, Wi-Fi keys and passwords, passwords for digest and basic authentication, and different service accounts and passwords generated by the device manufacturers. (The service accounts and passwords given by the device manufacturers are mainly used to register and log in to operator service accounts, including but not limited to broadband accounts, SIP accounts, TR-069 accounts

and cloud accounts.)

Keys and passwords must be unique. Keys must be generated randomly and should not be calculated by using a fixed algorithm. In particular, hard coding cannot be used to generate keys. Passwords must comply with strong-password rules, strength checks should be conducted during password modifications, and well-known common passwords cannot be used. Meanwhile, default keys and passwords should use high entropies and should not be generated based on easily available information such as the device SN, MAC address, Wi-Fi SSID, product name, and product model.

Different keys should be used to encrypt user configurations and default configurations. Both storage encryption and communication encryption should use reliable algorithms. Algorithms known to be insecure, such as DES and MD5, should be rejected. Public algorithms are required.

3.4. User Data Protection

User data protection covers access control of user data, information flow control of user data, and integrity and confidentiality of user data storage and transmission.

Sensitive information such as user accounts, passwords, private keys for authentication, operator server addresses, and firewall rules cannot be stored in the flash in plaintext, must be masked, and cannot be displayed in plaintext in man-machine interaction interfaces such as TR069, web, CLI and apps. Client certificates must be confidential and cannot be viewed or obtained by users through interfaces. In addition, these types of sensitive information cannot be transmitted in plaintext. The configuration files that store the sensitive information must be encrypted.

SSID hiding needs to be supported, while routing requests, DNS forwarding requests, DHCP requests and ARP requests from the WAN side of the home network devices need to be all rejected.

Voice-enabled home network devices need to verify the validity of SIP signaling.

3.5. Identification and Authentication

Identification and identification is a process involving the home network system and users. Identification is used to distinguish different users, while authentication is used to verify the authenticity of user identities.

User authentication: Provides multiple authentication mechanisms for users, including one-factor authentication and multi-factor authentication.

Authentication failure: Defines the number of failed authentication attempts and the time threshold used to terminate the session establishment process and invalidate the account.

User identity: Establishes and verifies the claimed user identity. Ensures that the user is associated with the correct security attributes, such as identity, group, role, and security level.

Web, Telnet, CLI, and SSH support delayed login after the username and password are incorrectly entered multiple times, thereby protecting against WPS brute force attacks.

Voice-enabled home network devices need to support SIP user authentication.

Web needs to provide login authentication mechanisms and support authentication through IP addresses and cookies. The corresponding rights should match the account rights.

Plug-ins require rights control so that the home network system can resist illegal and malicious attacks from them and does not break down after being attacked. After the attack is stopped, the system can recover immediately and the devices do not need to be restarted.

3.6. Security Management

Security management needs to cover security function management, data management of security functions, security attribute management, and security role definitions.

Command line configuration interfaces should use customized CLIs or rights-

restricted shells**.** On the web interface, the CPE needs to support multi-level account rights, data configuration through HTTP GET should be prohibited, and HTTP POST should be used to configure data. Key product information, such as hardware and software version numbers, can only be viewed through the management interface, and no system and application identifiers are displayed before login. It is not allowed to extract any executable file from a device. For example, executable files cannot be obtained through Telnet, SSH, Web, FTP, and Samba.

After a sharing service is enabled, the user can access the corresponding service directory, which is usually “USB drive directory/file” or “cloud directory/file” (usually in the/mnt directory). Accessing other directories/files is forbidden.

Error or prompt messages should not display any device information, such as whether a page exists. Web source code viewed through a browser should not contain developer information.

A version file includes a version header and version contents. The version header stores various verification data to identify the version files and verify the version contents. Version files need to be encrypted.

3.7. Privacy Protection

Information security laws and regulations require that user identities should not be discovered or abused by other users. User identity protection usually takes the forms of anonymity and aliases.

Anonymity: Ensures that the user identity is not disclosed when the user uses the CPE or its services.

Alias: Also ensures that the user identity is not disclosed when the user uses the CPE or its service, but the user identity can be determined based on the alias.

Users’ personal data can be classified into sensitive data and non-sensitive data, and some ways of classifying the data may be controversial. For home network devices, personal account information should be a priority for privacy protection.

The user's accounts and passwords for services (including but not limited to Web, Telnet, CLI, SSH, Samba, FTP, PPPoE, L2TP, IPSec, VoIP and Wi-Fi), phone number, SN, and other personal information cannot be exported to logs and need to be masked.

Likewise, these data should not be stored and transmitted in plaintext. Individuals have the right to view, modify and clear their personal data. In addition, if the personal data is to be transmitted and stored, the user must be notified through some channel(s) and the user's authorization must be obtained. Information such as data used to open an account with the operator and the SN of the device cannot be sent to a destination other than the operator.

Personal data has to be masked. Data masking means that the target data is irreversibly anonymized so that the original data cannot be derived from the target data. The target data should be easy to check and verify**.**

The autocomplete="off" attribute should be added to the username and password boxes for web login**.** This attribute is used to prevent browsers from saving passwords.

3.8. Security Function Protection

The protection of security functions is the cornerstone of security functions themselves.

To ensure the security of keys during storage and distribution on devices, the keys and certificates must be encrypted before being stored. Private keys must be accessible only through the management interface and cannot be transmitted over any network.

Before a version upgrade, the new version files must be obtained through an encrypted network channel. During the upgrade, the validity of the new version and configuration must be verified. Meanwhile, an integrity check of the new version can be performed through mechanisms like signatures. Similarly, validity and integrity checks are required for downloaded plug-ins.

The Operating System (OS) supports memory address randomization. The CPE filters DNS requests to mitigate DNS rebinding attacks and provides reliable timestamps for their own applications.

Web functions need to be protected against Open Web Application Security Project (OWASP) vulnerabilities, such as Cross-Site Scripting (XSS) attacks, formatted string attacks and Cross-Site Request Forgery (CSRF) attacks, to prevent illegal contents from being injected into the CPE through the management media entries. The user interface

uses defensive code to defend against clickjacking attacks.

3.9. Resource Utilization

Ensuring the availability of resources is a basic requirement for system security. The home network system controls the use of resources by users and subjects, such as by limiting rates or restricting the number of current connections, to prevent DoS attacks. The resource utilization requirements include providing fault tolerance and resource allocation capabilities.

The DoS attack protection function applies to all the IP addresses terminated on the CPE. After the attack stops, the CPE can resume operations without being restarted. During the attack, the CPE does not crash. In particular, after the attack stops, the TR-069 and VoIP services are restored immediately without a restart. If the strength of the DoS attack does not exceed a certain threshold, services are not interrupted.

Voice-enabled home network devices should pass the SIP robustness tests of RFC4475, including the resolver test, transaction layer test, and application layer test.

Public Wi-Fi networks are more vulnerable to attacks and should be isolated from private home domains. Public users should be provided with only necessary Internet services but not additional services and their speed should be limited to prevent them from occupying too many resources. Attacks from public users, mainly DoS attacks, should be defended against. The attacks should not be allowed to affect private users' use of the services of home network devices.

System security should be guaranteed during upgrades. Resources should be checked before an upgrade to ensure that they are fully available for the operation. During the upgrade, operations like restart, factory reset, and configuration modification should be restricted. After the upgrade fails, the system should be able to fall back to the previous version.

The system needs to control the use of system resources, such as CPU/Flash/RAM, by plug-ins. When a plug-in is running, the devices should operates properly and services other than the plug-in should not be affected.

3.10. Access Control

Access control restricts a user's access to some information items or limits the user's use of some control functions according to the user's identity and a definition group that the user belongs to.

Web source files do not contain redundant or unused functions and parameters so that they cannot be modified by constructing packets.

The firewall cannot be completely shut down, and the CPE should not be customized to the Custom level. If the Custom level is used, the "fwinput" subchain (preset incoming packet) rule will be cleared, resulting in leakage on uncontrolled ports.

It is forbidden to open system access channels without user or operator approval by employing methods such as pinging packets of a certain length and using combination keys. It is also prohibited to provide any tools or services that can be used to bypass system access control and access the system without the user or operator being aware. For example, the CPE should not allow Web/Shell and other debugging pages or have serial port pins. The CPE does not allow the provision of accounts unknown to the user or operator for services including but not limited to Web, Telnet, SSH, Samba and Shell.

After a remote management operation such as a TR-069 session ends, all ports other than the reverse link ports specified in TR-069 must be closed immediately. Web, Telnet, CLI and SSH support automatic logout after a logged-in session times out.

If the user selects Wired Equivalent Privacy (WEP), which is known to be insecure, as the Wi-Fi encryption mode, an alert should be given. It is not recommended to provide WEP as an option.

3.11. Trusted Paths

The CPE provides trusted communication paths between users and security function modules. Information exchanged via a trusted path cannot be modified or leaked, making it applicable to scenarios that require confidential communication.

WAN-side network management must use encrypted transmission channels or operator-customized dedicated channels. Dedicated network management channels such

as TR-069 and OMCI are recommended, while Telnet, SSH, Web and UPnP management interfaces are forbidden.

LAN-side network management must use encrypted transmission channels or trusted paths, and Web and SSH management interfaces are recommended.

TR-069, Web and TR-064 support HTTPS, which runs TLS. For TLS, at least TLS1.0 is supported, while TLS1.2 or above is recommended. SSL supports encryption keys of at least 128 bits. Note: SSLv3.0/2.0 has known security vulnerabilities and are not recommended.

SSH must be v2.0 or above, and it should be disabled at the WAN side completely and enabled at the LAN side only when necessary.

The RSA and DSA keys used in network communication encryption must consist of no less than 2,048 bits.

3.12. Hardware Protection

The hardware protection function is different from the hardware redundancy measures provided to improve system reliability, such as the use of dual power supplies and a Redundant Array of Independent Disks (RAID). Here hardware protection means that hardware resources are added to protect information storage, information transfer, and information computing. For example, a metal casing is added to protect the chip pins from being detected, or anti-disassembly hardware is installed to prevent the flash drive from being removed.

To prevent memory and firmware chips from removal, flash modules can be encapsulated in Ball Grid Array (BGA) mode to make them difficult to remove by ordinary users.

Chips are encapsulated in an iron boxes to prevent users from detecting pin signals and keep users from using third-party tools and hardware to extract chip firmware. SoCs support secure boot to prevent illegal third-party firmware from being burned.

The PCB of the shipped CPE does not have any debugging interface (JTAG/serial port), including the sockets, solder joints and PCB wiring needed for producing debugging

interfaces.

To prevent internal communication buses from being listened in on, information transmitted through them is scrambled or encrypted.

3.13. Others

The CPE must not be exposed to any copyright or intellectual property risks. A statement on the use of third-party software, which is similar to a General Public License (GPL), should be provided.

The kernel of embedded Linux systems should be continuously evolved using official versions..

Summary

As the "new infrastructure" of the modern home, the digital home network will carry the highly-promising, still-emerging information consumption services, whose successful delivery is predicated on high security. With network threats steadily increasing, it is imperative to build a secure home network environment. Through careful analysis of security threats, deployment of well-developed security policies, and application of the latest security technologies, we can maximally protect the security of the information and devices in the home network.

