# Client-side Security Assessment and Security Protection Scheme for Smart TV Network

Liang Bao, Songyang Wu, Shaohua Yu, Ju Huang
The Third Research Institute of Ministry of Public Security Shanghai, China
e-mail: baoliang@stars.org.cn

2020 IEEE 6th International Conference on Computer and Communications (ICCC) | 978-1-7281-8635-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICCC51575.2020.9345085

***Abstract*—TV networks are no longer just closed networks. They are increasingly carrying Internet services, integrating and interoperating with home IoT and the Internet. In addition, client devices are becoming intelligent. At the same time, they are facing more security risks. Security incidents such as attacks on TV systems are commonplace, and there are many incidents that cause negative effects. The security protection of TV networks mainly adopts security protection schemes similar to other networks, such as constructing a security perimeter; there are few security researches specifically carried out for client-side devices. This paper focuses on the mainstream architecture of the integration of HFC TV network and the Internet, and conducts a comprehensive security test and analysis for client-side devices including EOC cable bridge gateways and smart TV Set-Top-BoX. Results show that the TV network client devices have severe vulnerabilities such as command injection and system debugging interfaces. Attackers can obtain the system control of TV clients without authorization. In response to the results, we put forward systematic suggestions on the client security protection of smart TV networks in current days.**

***Keywords-TV network; security assessment; client-side; security protection***

## I. INTRODUCTION

With the application of new technologies such as 5G, IoT, big data, and cloud computing in the broadcast and television industry, and the evolution of the TV network's own architecture, the originally relatively closed TV network is interconnected with the outside world and faces new security threats and unprecedented severe challenges. The TV program may be interrupted due to the attack, and the content may be tampered with by the attacker, which will cause widespread influence. The Chinese Wenzhou cable digital TV system was illegally attacked to push illegal propaganda content. Many mainstream TV stations in South Korea were unable to log in due to an attack. The broadcast system of French TV5Monde was attacked and disrupted for several hours. Not long ago, Pakistan's mainstream media television station was suspected of being hacked and broadcasting the Indian flag. Similar security incidents emerge one after another.

Driven by the network integration, the radio and television network has evolved into a comprehensive information and communication network. In order to deal with the emerging security risks, researches pay more attention to network-side security protection [1]-[3], mainly by deploying security processing modules on boundary of different security areas, preventing illegal code streams, text, pictures and other information. An internal firewall is usually deployed in the home network to prevent illegal intrusion from the home network's clients such as smart Set-Top-Box or gateways. [4][5][6] theoretically analyzed the terminal-side security risks and gave corresponding countermeasures, but the client-side devices have not yet been evaluated practically. [7][8] focus on attack against the built-in media player feature of Smart TVs. At present, there is still a lack of comprehensive and overall security analysis from different dimensions for the terminal side equipment of the smart TV network. Until now, we hardly see an overall practical security research on smart TV devices.

The TV network is important national information infrastructure. Due to its relatively closed and independent evolution characteristics, there are few targeted and systematic security studies. New technologies, new business services and new situations require in-depth research on the threats and security of radio and television networks, and the construction of a network security protection system accordingly to ensure the safety of TV network.

This paper analyzes the security of the current TV network. We present that the client-side devices are faced with more new security risks. Therefore, security tests and assessment on the client-side devices in an actual operating TV network are carried out. Section 2 introduces the status of TV networks; section 3 conducts an overall analysis of the security of the radio and television network; section 4 conducts security tests and assessment for EOC cable bridge gateways and two common smart set-top boxes; section 5 introduces the security protection scheme for protecting TV network client-side devices. Section 6 summarizes the whole paper.

## II. TV NETWORK DEVELOPMENT

### A. HFC Network

HFC (Optical Fiber/Coaxial Cable Hybrid) networks are usually operated by local cable television network companies (stations). It is a broadband access technology developed on the basis of traditional cable television networks (CATV) [9]. When TV networks first appeared, they were small in scale, also known as Community Antenna Television, and generally consisted of pure coaxial cables. HFC combines optical fiber and coaxial cable to provide high-speed Internet access and analog or digital cable television program

transmission, with a theoretical rate of 38Mbps to the home. HFC network has good frequency band resources, coverage and comprehensive service capabilities. Traditional cable television networks generally carry one-way services such as TV and FM broadcasting. They only have signals from the central office (front-end) to users, but not from users to the front-end. The original HFC network is also a one-way structure.

### *B. HFC and Internet Integration*

In today's unprecedented prosperity of the Internet, TV networks are becoming integrated with the Internet. The two-way, broadband, and IP-based broadcasting and television networks are the prerequisites for effective integration. Cable TV is no longer just a simple audio-visual tool, but also an access device for the Internet. Two-way transformation is still the focus of today's TV network construction. There are mainly three technical solutions: CMTS, EPON+LAN and EPON+EOC.

CMTS: Based on the traditional wired network, add CMTS head-end equipment in the front-end server room, modulate the data signal into an RF signal for transmission, and receive the uplink data and convert it into a data signal to output to the data network; RF directly provides analog signals and digital TV signals; if you need to provide broadband Internet access, only to add a modem CM on the client side. The network architecture is shown in Fig. 1.

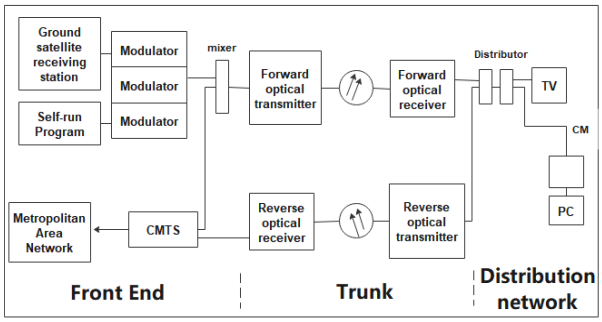



Figure 1. Network Architecture using CMTS.

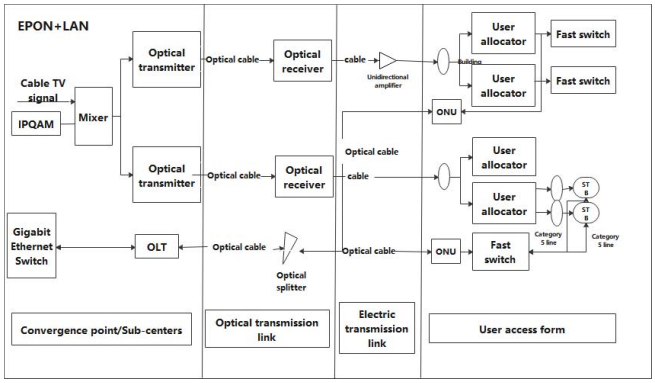



Figure 2. Network Architecture using EPON+LAN

EPON+LAN: The optical network adopts EPON (Ethernet over Passive Optical Network). A typical EPON system is composed of OLT (Optical Line Terminal), ODN (Optical Distribution Node) and ONU (Optical Network Unit). The access network uses Ethernet to reach home, and edge switch equipment and twisted pair cables are required. The network architecture is shown in the Fig. 2.

EPON+EOC: The difference between EPON+EOC and EPON+LAN is the final user access method. EOC (Ethernet over Coax) transmits Ethernet data on coaxial cables, which mainly solves the problem of extending the cables in order to cover the home buildings.

EOC technology mainly includes three types: passive EOC, low-frequency active EOC, and high-frequency active EOC. Passive EOC technology directly uses frequency division multiplexing technology for Ethernet data and cable TV signals, so that these two signals are transmitted in the same coaxial cable. Passive EOC cannot be applied to the tree network of radio and television, and the anti-interference ability is poor. Active EOC solutions are diverse in different scales and maturities. Low-frequency active EOC technologies include PLC, HomePNA, etc., and high-frequency active EOC includes MoCA, WLAN frequency reduction, etc., mostly based on modulation technology to modulate data signals to a certain frequency band that can be transmitted on the CATV coaxial network, the CATV signal and the modulated data signal are mixed and transmitted. The CATV and data modulation signals are transmitted in the downstream direction, and the data modulation signals are transmitted in the upstream direction.

The network architecture using EPON+EOC is shown in the following Fig. 3. Among them, EPON+EOC has become a mainstream technical solution due to the relatively simple network transformation.

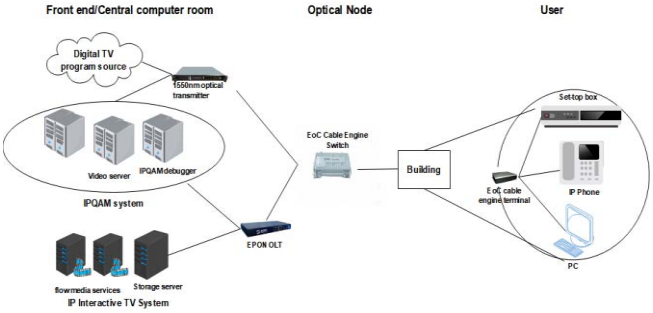



Figure 3. Network Architecture using EPON+EOC.

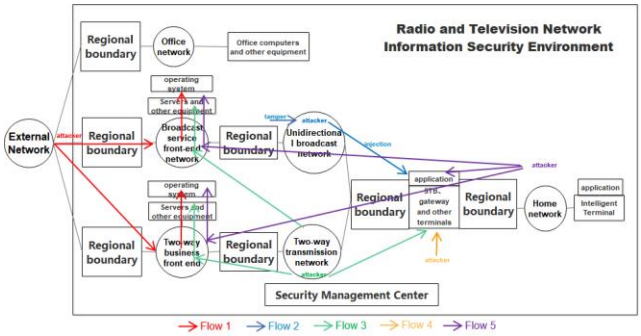



Figure 4. [2] Main components and their connected relations

## III. SECURITY RISKS OF TV NETWORK

Main components and their connected relations are shown in Fig. 4. We analyze the security risks based on the following figure and describes corresponding security programs adopted currently.

### A. Security Risks

1) Attacks may be initiated from an external network or office network, crossing the security zone boundary, invading the broadcast service front-end network or the two-way front-end transmission network, paralyzing the application system or illegally alters various data like text, pictures, videos, etc., which will make set-top boxes and other devices unavailable or display illegal information. Attacking flow is depicted as Flow 1 in Fig. 4.
2) Attacks may be initiated from the one-way broadcast network, injecting illegal information, such as replacing the front-end live broadcast or on-demand program stream with illegal untransparent streams, replacing the unencrypted text and pictures of EPG advertisements, and replacing the unencrypted text and images of data broadcast pictures, etc., which will make set-top boxes display illegal information. Attacking flow is depicted as Flow 2 in Fig. 4.
3) Attacks may be initiated from the two-way transmission network, crossing the security zone boundary, invading the two-way business front-end network, paralyzing the application system, or illegally tampering and replacing various data, text, pictures, videos, etc., which will make set-top boxes and other devices unavailable or display illegal information. Attacking flow is depicted as Flow 3in Fig. 4. If there is no isolation between the two-way service front-end network and the broadcast service front-end network, the server in the broadcast service front-end network can also be invaded. Attacking flow is depicted as Flow 3 in Fig. 4.
4) Attacks may be initiated from the home network, crossing the security boundary, invading the two-way business front-end network, paralyzing the application system, or illegally tampering and replacing various data, text, pictures, videos, etc., which will make set-top boxes and other devices unavailable or display illegal information. If there is no isolation between the two-way service front-end network and the broadcast service front-end network, the server in the broadcast service front-end network can also be invaded. Attacking flow is depicted as Flow 4 in Fig. 4.
5) Attacks may be initiated from a client-side device such as a set-top box, illegally flashing and replacing the software of the set-top box, downloading illegal applications, and displaying illegal information.

### B. Security Program

The security program of the radio and television network system is similar to the security program of traditional network and information systems. The network-side security strategy and protection plan of the traditional TV network has been maintained for many years and are relatively stable. For example, traditionally, in order to deal with attacks described by Flow 1,2,3,4 in figure 4, firewalls, IDS are deployed and corresponding security strategies are configured. To address attacks described by flow 5, vulnerability scanning is performed periodically.

However, the network types and devices on the client-side have undergone major changes, and the running forms are changing rapidly. The security protection for the client side is becoming more and more important. There are no relevant standards for the safety evaluation of client applications. Currently, vulnerability scanning is the main focus, and the malicious behavior of the clients cannot be fully evaluated. As a result, the overall security assessment and protection scheme for the client-side devices still require more attention.

EOC cable bridge gateways, various smart set-top boxes and other client-side devices are the key points of smart TV networks. The client-side devices more open, large in number, and widely used, meanwhile also expands the attack surface. As shown in Figure 3, the client-side equipment of the smart TV network is mainly used to connect to the EOC cable bridge gateways of the building, and various types of set-top boxes.

## IV. TV NETWORK CLIENT-SIDE SECURITY ASSESSMENT

We select one commonly used EOC cable bridge and two smart set-top boxes. These two set-top boxes are also the mainstream set-top boxes that are developed based on the TVOS system and are currently in use. Comprehensive safety testing and evaluation are conducted. The results can provide reference for client-side device manufacturers in terms of product security. Before the publication of this paper, high-risk vulnerabilities have been reported to the related device manufacturers. The tests and evaluation methods used include reverse analysis of device firmware, device local service tests, and device network service tests.

### A. EOC Cable Bridge Gateway

The function of this device is to separate the Ethernet data in the broadcast digital signal. For users, the device is a dual entrance to the Internet and broadcast TV. Embedded Linux system is used and the firmware model is PH02_js_WIFI_FIRMWARE_v3.0.03_20171205SignI.bin.

Test results show that a function iptablesWebsFilterRun in the back-end component firewall.cgi of the Web service has a command injection vulnerability, the variable addHostFilter. Replacing the web interface parameter addHostFilter in the data packet by the execution command, and sending the POST request in the same WLAN could execute any system command. The construction command is shown in the Fig. 5 below.

firewall=websHostFilter&addHostFilter='telnet -l /bin/sh -p 1341 -b 0.0.0.0'&addwebscontentfilter=%E6%96%B0%E5%A2%9E

Figure 5. Construction command.

The telnet service will be enabled on port 1341 on the device which is shown in Fig. 6. After the command was executed, the port was open, indicating that the command was executed successfully and the attacker could directly obtain the system control right. In addition,

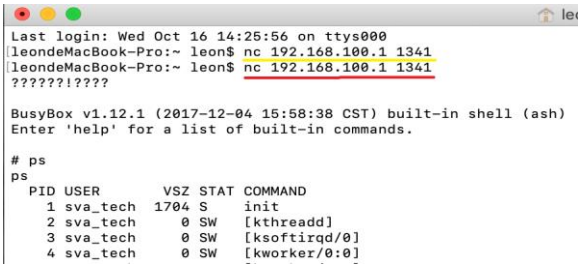



Figure 6. Successful execution of command injection.

In addition, an authentication bypass vulnerability has also been discovered. Simply adding login=1 to the Cookie field, then the gateway device will allow the attacker to exploit the above-mentioned security vulnerabilities with the authority of the login user. As shown in the Fig. 7, unauthorized users can execute download commands on the EOC gateway and control the gateway to connect to the remote server.

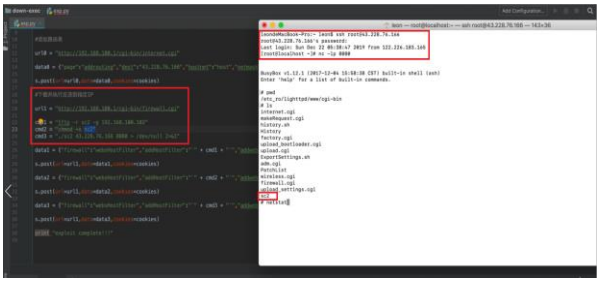


Figure 7. Successful execution of authentication bypass.

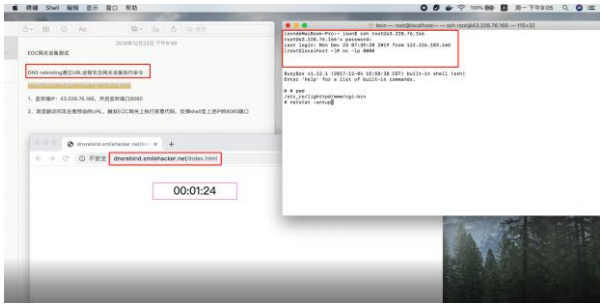



Figure 8. Successful execution of DNS redirection.

Besides, there is a more advanced way of exploiting the vulnerability. Through DNS redirection, the victim can trigger the attack by clicking a URL. The process of exploiting the vulnerability is shown in the Fig. 8 below. After the victim's browser in the lower left corner visits the specified URL link, there is an interval of about 1 minute, and the EOC gateway where the victim is located is controlled by the remote server. After controlling the EOC gateway, the attacker can attack other devices, such as turning off the network card through which the video of the downstream set-top box flows, causing the video to be interrupted.

## B. *Smart set-up boxes*

### 1) *Set-up box 1*

This set-top box adopts the TVOS 3.0 system, the RF interface and LAN interface can receive broadcast and TV signals and network data. It comes with multiple APP applications including TV services, video on demand, online shopping, and community services. The vulnerability of this device lies in the opening of the TVOS 3.0 system debugging interface, which allows unauthorized access to the TVOS system through TCP port 5555, and uses the ADB debugging tool to obtain the system shell. As shown in the figure 9, you can see that the current user authority is the highest root authority of the system. The 5555 debugging port is open on 0.0.0.0, which represents all IPv4 addresses, so it can be accessed remotely through the LAN.

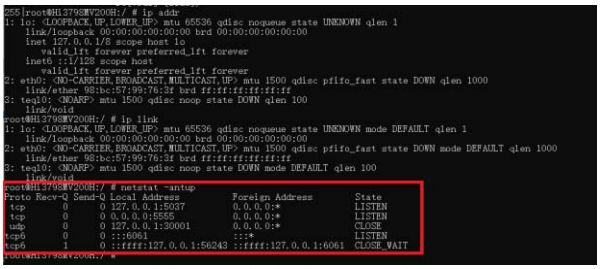
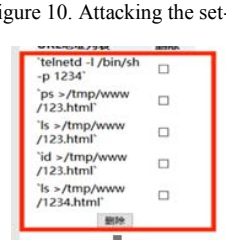



Figure 9. Gaining unauthorized access to the TVOS system.

This vulnerability can be used to replace local set-top box resources. Firstly, the attacker obtains the local set-top box shell through ADB, locate the booted video animation resource, analyze the resource file compression format, re-compress the content after replacement, and finally restart the set-top box to complete the replacement. The replacement results are shown in the Fig. 10. Fig. 10 (a) is the original picture, and Fig. 10 (b) shows the replaced on.


(a) The original picture on TV (b) The replaced picture

Figure 10. Attacking the set-up 1.




(a)


(b)

Figure 11. Attacking the set-up 1

By exploiting this vulnerability, attackers can even take over the remote set-top box without authorization. Obtain the shell of the local STB through ADB, detect the survival of other IPs in the LAN and the open status of debugging port 5555, and try to establish an ADB shell connection with the remote IP.

### C. *Set-up box 2*

This set-top box adopts dual systems: COS and embedded Linux. Open services are detected: Web services, Telnet services. Results show that there is command injection vulnerability in the Web service, and arbitrary commands can be added to the URL address filtering as shown below. The results of the successful execution of the command in figure 11(a) and figure 11(b), indicating that the currently acquired authority is the highest root authority. In addition, there is another vulnerability. The telnet service is open on two ports (2608, 8062), and there is a weak password "12qwaszx", and the users are all root users.

### D. *Testing apps of Set-up box 1 and Set-up box 2*

Tests of the local app of the two set-top boxes have found that several services are vulnerable to backing-up and debugging at will.

## V. CLIENT-SIDE SECURITY PROTECTION SCHEME FOR SMART TV NETWORK

The security vulnerabilities discovered during the tests allow attackers to obtain the highest control of digital TV client-side devices such as EOC gateways and set-top boxes through various methods to perform sniffing, blocking, and tampering, then disrupting broadcast, stealing user accounts, hijacking access, etc. Attacks can be extended to other devices in the radio and television network and cause serious harms. The main reasons are as follows:

1) The practical development of client-side software and hardware lags behind the international equivalent IoT product standards
2) The client-side devices lack security protection, and exploitations of vulnerabilities are hardly blocked
3) Lack of front-end and back-end security protection cooperation which results in no resistance to penetration.

Next, based on the current situation of the radio and television network and the results of the security tests, a security protection scheme for the client-side devices of smart TV network is designed.The protection scheme for smart TV network client-side devices is shown in the figure 12.

Set-top box security solutions adopt a security model of detection, protection, monitoring and response. Before putting online, conduct security inspections on the compliance and application vulnerabilities of the set-top boxes to achieve early detection and early treatment. In production environment, continuous security monitoring of the operating environment in order to detect attacks and sensitive operations, and timely take actions based on the monitoring results. After an incident, log records and monitored behaviors are used to conduct operational audits and perform root cause analysis. Through pre-event security detection, in-event monitoring response protection and post-event audit traceability, a set-top box security protection system integrating equipment, applications and data is constructed.

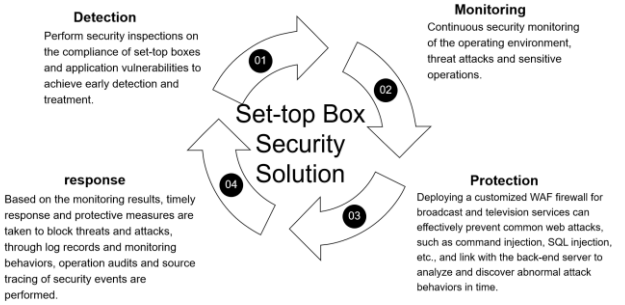



Figure 12. Protection scheme for smart TV network client-side devices

1) For the software development of client-side devices, full life cycle security development standard (SDL) should be followed, and the universal OWASP security coding and other international security development guidelines should also be referred. Source code and firmware must be tested and evaluated to ensure system security;
2) For client-side device hardware, the IoT security threat model should be applied. Before putting it into use, it should undergo professional security analysis to resolve security risks, and penetration tests and security assessments should be periodically carried out to ensure the security of the device hardware architecture.
3) Deploying a customized WAF for broadcast and television services can effectively prevent common web attacks, such as command injection, SQL injection, etc., and cooperate with the back-end server in order to analyze and discover abnormal behaviors in time.
4) For the TVOS of client-side devices, EDR protection system should be deployed. By adopting TrustZone technology for the underlying hardware system, the system critical behaviors and abnormal event logs are encrypted and stored, and the warning logs are sent to the back-end server to discover the abnormal behaviors in time, then forming a closed loop of "defense-detect-response".

## VI. CONCLUSION

This paper conducts a full-dimensional security test analysis for client-side devices of smart TV network. Tests found that EOC cable bridge gateways and smart set-top boxes have vulnerabilities such as command injection and

system debugging interface opening, allowing unauthorized users to use the vulnerabilities to obtain system shells. Then, the smart TV network client-side security solutions are proposed, including: implementing a full life cycle security development standard (SDL) for the development software, applying IoT security threat models for devices, deploy a customized WAF firewall for broadcast and television services; and apply an EDR protection system for the smart TVOS, etc.

## ACKNOWLEDGMENT

This work was supported by the Shanghai Science and Technology Committee Research Program (C20351).

## REFERENCES

[1] Huo Xiangwei. Talking about the threats and protection of radio and television network information security[J]. Jiangsu Communication ,2019,35(06):74-77.

[2] Kim H. Secure communication in digital TV broadcasting[J]. International Journal of Computer Science and Network Security, 2008, 8(9): 1-5.

[3] Bachy Y, Basse F, Nicomette V, et al. Smart-TV security analysis: practical experiments[C]//2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. IEEE, 2015: 497-504.

[4] User-side network security risk analysis and construction ideas of radio and television networks, "Cable TV Technology", Issue 5, 2019

[5] Shen Yuhang. Analysis of the current situation of information security of radio and television network integration terminals and research on development countermeasures [J]. Radio and television technology, 2016,43(04):77-80.

[6] [7] Mao Zejie, Wu Weihua. Security analysis and research of Android smart set-top box［J］. TV technology, 2016，40( 3) : 79－82.

[7] Michéle B, Karpow A. Watch and be watched: Compromising all smart tv generations[C]//2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). IEEE, 2014: 351-356.

[8] Michele B, Karpow A. Using malicious media files to compromise the security and privacy of smart TVs[C]//2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). IEEE, 2014: 1144-1145.

[9] Shu Yun, Wang Ruiying. Development of China's Cable Television (CATV) [J]. International Broadcasting and Television Technology, 1990, 004(006):2-7.