riscure

Broadband service providers – a security view

4 things you can do today for your device and network security

Broadband service providers (BBSP) are well-positioned in the upcoming age of IoT development for consumer devices, offering a multitude of services such as internet access, VoIP as well as media content. BBSPs are handling different technologies and rely on their partners when it comes to security. New security developments and threats for IoT and edge devices are taken seriously by the BBSPs.

In this whitepaper, we explore the current developments in the market concerning the device and network security with real-world examples. Additionally, we provide an overview of the current developments of legislative activities for consumer devices. Finally, we conclude with concrete tips that BBSPs can put into practice.

inforequest@riscure.com www.riscure.com

Introduction

According to Gartner, the number of connected devices in the world will reach 25 billion in 2021. Even though broadband service providers (BBSP) are best positioned when this impressive growth is considered, connectivity presents a double-edged sword. On one side, service providers have a great advantage of having a direct relationship with the consumers through infrastructure and deployed devices. On the other side, these infrastructures and devices may be the biggest threat to the offered value-added services and reputation.

Although most of the broadband service providers are very well aware of the network security threats and take continuous protection of their systems seriously, the security of devices never comes first, but always starts with the functionality. If the security is not part of the design process for a device, trying to plug holes and fight against ever-growing waves of attacks will be frustrating.

Service providers usually rely on supplier assurance regarding the security robustness of their devices. The globally accepted Common Criteria (CC) is an approach that attracts vendors due to its widespread acceptance and support from the government. However, as the certification process for even low-level EAL2 is quite expensive, smaller vendors and those with a tighter budget are not choosing this route. Additionally, while CC assures the company processes to a certain extent, security robustness for lower levels such as EAL2 is not well tested. Next to those common criteria does not provide continuity over multiple updates as the certificate holds only for one hardware and software version.

A compromise on the service providers' device and/or infrastructure can lead to very serious consequences. For example, a DDoS attack may significantly lower the quality of the services or even suspend the services. On the other hand, leakage of sensitive data most likely results in substantial financial impacts like fines, theft of trade secrets and intellectual property, loss of reputation, credibility, and customers.

Broadband service providers and security concerns for Devices

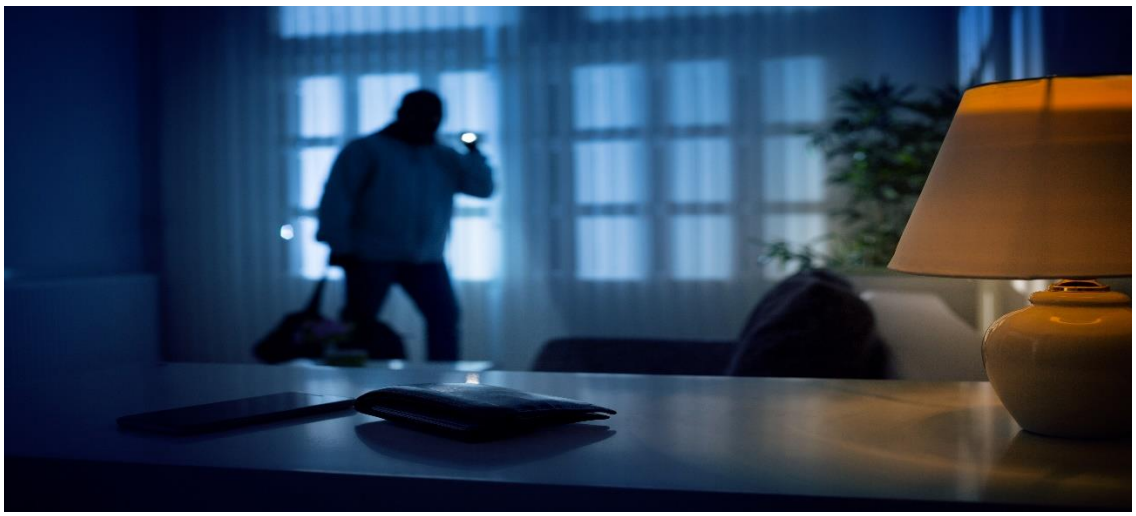
Broadband service providers undertake activities to increase the security level of their edge devices and networks, such as penetration testing of networks and devices, configuration as well as development. The main objective of such activities is to protect the assets and support the business's continuity. Depending on the complexity of services BBSP might offer, some of the notable assets that have to be protected are:

- the integrity of the device
- the integrity of the backend services,
- the exploitation of Broadband service provider's services such as the internet, VoIP or content delivery
- the confidentiality and authenticity of private and secret data

The device integrity assures that the device cannot be repurposed. The device deployment includes costs for the BBSP and repurposing of the device is a direct loss of revenue and potential brand damage. Repurposed devices could be used in botnets for DDoS, ransomware, cryptocurrency mining, attack on other devices in the network or simply used for other purposes such as a streaming platform.

For broadband service providers, the integrity of the backend services is directly related to the potential costs and legal obligation towards content owners for media services. Additionally, exploitation of BBSP services such as the internet, VoIP, or content delivery could lead to costs, loss of customers, and brand damage.

Finally, protection of user data is always in the scope of the BBSP security considerations as a leak of user data such as Parental PIN Code, Wi-Fi password, credit card numbers can cause financial losses and brand damage, as much as the security of BBSP keys and certificates.



When the security robustness efforts are exercised, the focus is always on scalable and remote attacks as they are the most devastating, especially with the introduction of IPv6.

From many years of experience with 800 edge and media devices, Riscure observed that the vulnerabilities are present in all parts of the software including bootloader, middleware, open-source libraries, and OSs. Vulnerabilities differ among gaining runtime control of the device, compromising the confidentiality of data, or compromising the availability of (security) services. Next to the vulnerable devices, an attacker can use a compromised device as a gateway to access and compromise backend servers or user devices on the same network if BBSP's network is not securely configured.

In the past two years, there has been a surge of government regulations for devices and the IoT market in general. These regulations are attempting to address consumer rights on devices and continuous service as well as to protect general internet infrastructure from botnets caused by vulnerable devices. A well-known example of such legislative activities is the Californian bill (SB-327) and European Cyber Security Act (CSA). There are several government initiatives to provide guidance and recommendations for users as the first step towards legal regulations in the UK, Australia, Japan, and Sweden.

In this paper, we will address primarily the security aspects of home devices for BBSPs and only lightly touch upon existing and upcoming regulations.

Device configuration

The home gateways and media devices are configured insecurely due to lack of security focus in device development and deployment phases. Default factory settings are the most common security problem. IP configuration is common for the entire series of devices as well as for administrators' user names and passwords. Similarly, some enabled services increase usability at the expense of security with examples of UPnP, Telnet, a remote management protocol, and WPS (Wi-Fi Protected Setup). Aside from network misconfiguration, misconfigured separation of privileges in the OS is also a prominent issue.

A good illustration of how a misconfiguration of a device could lead to devastating outcomes is the MIRAI attack from 2016. All the devices were compromised remotely only based on the misconfiguration of network services as well as lack of separation. No software (code) vulnerabilities in the classical sense have been used. The botnet simply connected to the available service on the external interface and went through 60 pairs of default/standard username and password.

Newer generations of botnets based on MIRAI use Android ADB over Ethernet which is configured with standard login username and password affecting mostly STB and TV devices.

The BBSPs use SNMP as well as CWMP protocols to manage the devices on their networks and misconfiguration of the firewall rules enables anybody on the network to access the devices from other users in

the network. Due to a lack of restrictive configuration, with a vulnerable CWMP implementation, an attacker could have full access to the device from reconfiguration (DNS) to reboot. Changing DNS addresses to the attacker website which does not use HTTPS, enables an attacker to extract critical user information such as credit card data.

Sometimes manufacturers deliberately implement backdoors in their equipment in order to improve the technical capabilities of the device. However, these backdoors can be used by the attackers to receive remote commands or extract data from the device.

Real world example – Mirai attack
Mirai means future in Japanese and it is the name of an IoT based botnet constructed by students Paras Jha, Josiah White, and Dalton Norman in 2016. The botnet was built to attacking Minecraft servers and gain profit for the attackers. However, it was used in a massive distributed denial-of-service (DDoS) attack that brought down a major U.S. dynamic DNS provider, Dyn DNS, with unprecedented force, triggering widespread internet outages in the U.S. and Europe.

The botnet is self-propagating by connecting to telnet port. After it attacks a device it configures the device securely to protect the device from other security attackers and botnets. Additionally the botnet payload (scripts) has a particular list of do-not-attack devices mostly related to US government. Before the original developers of MIRAI were arrested, they have released the source code of Mirai. This caused development of new variants based on Mirai, with at least 63 Mirai variants observed in 2019.

Beyond MIRAI
In September 2018, researchers observed the Hide and Seek (HNS) IoT botnet targeting Android devices with ADB option enabled. In June, Trend Micro discovered an Android crypto-currency mining botnet that can spread via open ADB (Android Debug Bridge) ports and Secure Shell (SSH).

Since then, malware is mostly focused on enslaving consumer-based devices to build botnets and perform nefarious tasks, which mostly consist of DDoS attacks and illicit cryptocurrency coin mining. Potential impact to back-end is also recognized in the community as IoT devices connected to cloud architecture could allow Mirai adversaries to gain access to cloud servers.

For devices that have Android, the issues become even more difficult as Android is by design an open platform. The internet is full of various advice on how to install and repurposing the device for streaming applications that compromise content protection such as XBMC / Kodi.

Real world example – website with hacking instructions
TVHacking is an instructional website on "How to install XBMC/Kodi players" and access the content online. Various devices can be modified to allow running of the player such as Amazon FireTV and AppleTV. Android installing is performed through enabling ADB network debugging feature.
https://tvhacking.com/

The recent attacks that use misconfiguration to access the routers/modems and edge devices are directly linked to the most devastating event in recent history COVID-19.

Real world example – COVID-19 themed attacks
Recent attacks on **routers** include brute forcing **remote management credentials**. After the control is established over the router, the DNS settings are changed to point users to hacker's websites. The malicious website appears to be a legitimate website and it prompts the user to install malware on the home computers that is then stealing credentials and credit card data.
https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

Typical issues in the configuration of the home routers and media devices.

Re-use of passwords and default passwords
For the devices delivered to users, default passwords are frequently used. Due to lack of knowledge, home users are not changing these passwords, which enables attackers' access to data. More worrisome is that same passwords are used for administration of devices as well as for accessing the services in the back-end system.

Misconfigured Telnet/ssh/SNMP
Frequently either device vendor or the broadband service provider is enabling telnet, ssh or Simple Network Management Protocols (SNMP), which are used to control and configure the device. Next to the standard passwords and re-use of passwords on these open ports, they are configured very openly with large impact on the device. SNMPv1, can cause security related risk as it sends the configuration file containing authentication strings in plain text. SNMP can create severe security related issues when operating in Read-Write mode.

Open ports with other services
Various other services or proprietary protocols are frequently used for diagnostics. Security is never achieved through obscurity, and many attackers possess skills to reverse engineer protocols and firmware to discover how the protocol works and what the weak points are. UPnP is one of the protocols that is very difficult to configure correctly. Defenscode identified over 80 million hosts that responded to a standard UPnP request on WAN port. One in five of them supported SOAP (Simple Object Access Protocol) service, while 23 million allowed to execute any code without authorization.

Firewall rules
Firewalls are by default available on Linux OS, however they are rarely used and configured. And when they are configured, very permissive rules are used which enable attackers to compromise the device. An example of a port that should be blocked is UPNP port 1900 on WAN interface or completely disable UPnP in WAN interfaces.

Linux privileges separation issues
Linux is the base system for many embedded devices due to its modularity and efficiency as well as security. However, the security features are not frequently used and what can be observed is that root privileges are provided to services listening on external ports and using no or poor authentication. Further technologies such as SELinux and jailing of processes using chroot are not frequently used.

Certificates misconfiguration
Certificates that are used for accessing websites from the device are stored on the device. The rules to use the certificate can be configured to allow for security inferior options such as self-signed certificate or wild card certificates.

Open debug facilities through USB, UART, JTAG
Although debug facilities are useful during development, when the device is deployed, it can cause problems if left unprotected. When attackers are planning an attack on a device, they usually learn as much as possible about the device by reverse-engineering. If it is possible to buy a device and access its debug facilities, the attack can quickly access firmware for reverse engineering or even have runtime access to find the secrets such as keys or certificates. Note that downloading firmware is still possible even if the debug facilities are not open by desoldering the chip, however it is more difficult and might contain further protections such as encryption.

Historically BBSPs receive the devices for deployment and have little or no influence on the configuration and SW running on the device. Additional penetration testing of the device is usually required and executed by the company's Red teams or subcontractor. It is very important to address the basic configuration issues ***before*** the

device is purchased to minimize the risk and prevent later interventions. While BBSPs Red teams and most of the subcontractors are very experienced in network penetration testing, an additional focus that Riscure provides in the mix is the embedded device knowledge, which can point towards unexpected vulnerabilities in the configurations.

Code vulnerabilities

Next to the misconfigurations of the system, a large issue with security lies in the SW or code vulnerabilities in the implementation software. Devices come in a multitude of forms and software is present. Anything from Linux, RDK, or Android is available and used. On top of the variety of operating systems, the middleware developed by third parties interacts with various systems including backend. In such a varied eco-system, it is difficult to set and keep the security development requirements clear and verified.

Developers and security specialists are quite familiar with code vulnerabilities such as buffer overflows. The memory corruptions are at the core of most code vulnerabilities. While insecure configuration is frequently motivated by a lack of understanding of security or demand for features, code vulnerabilities are commonly introduced during the development by accident. Input sanitation is a very important measure against buffer overflows as well as SQL and command injection, path traversals, etc.

For the open-source software, most of the vulnerabilities are widely known and published on the CVE website. Next to that exploits for those vulnerabilities are available which makes exploiting old software versions easier. In that context anti-rollback feature which allows users to downgrade the SW version on a device can lead to exploitation of the device.

The most common way of finding the vulnerabilities in the wild is by reverse engineering the firmware running on the device. The firmware is usually extracted either from the manufacturer update-servers, through open debug access or by desoldering flash and dumping firmware. Firmware is then reverse engineered and the attacker gains a better understanding of the attack surface, such as vulnerable services exposed, issues with configuration and plain text passwords and usernames. Out of all consumer devices, the attackers are most interested in routers and modems and a lot of research and hacking activity is revolving around router and modems.

Real world example - public attack
Memory corruptions are the most common vulnerabilities used in different attacks. Some of the real world examples include:

- Over 10 bugs discovered in routers, among others stack overflow - *Presentation on BlackHat: Lecture: Don't Ruck Us Too Hard - Owning Ruckus AP Devices*
- Vulnerabilities in UPnP stack for older versions of libupnp

Website tracking different vulnerabilities in router firmware:
https://routersecurity.org/bugs.php

Complete attack on a connected device
A good illustration of full attack on a device is illustrated by Adam Gowdiak attack on a STB gateway that included: javascript exploit, use of code vulnerabilities and misconfiguration to reach higher privilege level and finally abuse of hardware security features.

Adam Gowdiak attacks on Digital Satellite STB
#HITB2012AMS D1T2 - Adam Gowdiak - Part 1 - Security Threats in The World of Digital Sat TV

Riscure is a security evaluation laboratory with experience of over 19 years, and we have encountered various issues in home gateways and media devices such as old libraries with known security vulnerabilities, java scripting issues in browsers as well as input processing issues for USB devices attached to the gateway.

Old libraries with known vulnerabilities
In general, it is quite difficult to make sure the embedded device SW is up to date. Changing the libraries during development increases compatibility risks. For that reason, a lot of devices are suffering from this issue.

Vulnerabilities during boot or remote update
Even in cases where firmware update is properly configured with appropriate authentication on the device, vulnerabilities in the update process can lead to weak devices.

Vulnerabilities in browser script executions
The most common way to attack a device that is securely configured is through the browser interface. If there are vulnerabilities in the browser or virtual machine – this can be abused to access the device.

Lack of input parsing
Input coming from the network, USB or user input on screen should be carefully parsed to protect from standard attacks such as path traversal, misconfiguration of the buffer for the input, command injection. Or simple buffer and stack overflows caused with incomplete parsing.

During management of the device, input is received through an unauthenticated channel. Additionally, this input is also unauthenticated which means that anybody can modify the input and either exploit the service processing it or use a vulnerability to reach other services on the device.

Use of vulnerable POSIX functions
Use of insecure POSIX functions such as gets() support the introduction of these vulnerabilities. With gets(), the size of the destination buffer is unknown. Consequently, any program that reads input using gets() has a buffer overflow vulnerability. Other vulnerable functions include strcpy(), sprint() and strcat() etc.

Lack of SW protection features
Next to decreasing the number of SW vulnerabilities, it is very important to also introduce software attack mitigation techniques such as ASLR, stack canaries, Control-flow integrity, non-executable stack and heap (NX), guard pages etc. These mitigation techniques are not always present in devices.

Devices on BBSPs network

A compromised device is a gateway for the backend system as well as for the other devices in the network. With a proper authentication of each device by the backend system, some attacks could be remediated. If the credentials to authenticate the device are extracted, the device can still be used to attack your backend system or other devices on your network.

In the DOC-SIS standard, there are several intrinsic vulnerabilities in how the network configuration is set. For example, cable modems require a configuration – provisioning file to configure the network. The provisioning file contains a user name and password for administrative access to all devices in the network. Similarly, VoIP services can be vulnerable to the same provisioning file attacks. An attacker could force other user devices to call pay-service-numbers or even listen to the conversation of other users in the network. In case of open

access provided to vulnerable home devices, any vulnerability in the backend system is directly exposed to the attacker.

Example of a public attack
A research presented in 32C3 conference, showed devastating effects of having a compromised device on a cable network with permissive network configuration.

In this particular case, DOC-SIS interface provided users with 3 lines from the device through CMTS to the back bone, among which Admin line is used for configuration files for provisioning and VoIP line is used for configuration of calls.

The provisioning file contained passwords for SNMP, telnet as well as insecure SSH hash. As the provisioning file contained the user name and password, the attackers was able to access modems of other users in the network and have a root shell. The VoIP service for the same provider was vulnerable to the same configuration attacks. Attacker could force other rooters to call pay-service-numbers or even listen to the conversation of over 3 million users in the vulnerable network.

The backend system allowed for devices to interact with each other, and used the same login credentials for all the devices and firewalls were not configured properly.

At CCC 32C3, in a presentation titled "Beyond your cable modem. How not to do DOC-SIS networks",

Thermostat connecting to the back-end
Riscure has researched the implications of smart thermostat with back-end server that supports the connectivity for computer thermostat applications. Once the thermostat is installed in a consumer network, the server provided an SSH tunnel (SSH relay) to the device. If it is not done securely, it essential creates a massive security hole in the consumer home network.

We were able to obtain the login credentials for the back-end server through a standard request that thermostat devices perform. The server was running an old image for which known exploits exist that can enable root access on the server. From the server it could be possible to reach thermostats in consumer houses.

https://www.riscure.com/blog/on-the-security-or-lack-thereof-of-the-connected-iot-thermostat/

Penetration testing of the backend and network tends to miss vulnerabilities that can enable hacking of the devices as they are assumed by the network provider to be functional enablers.

Security standards development

In recent years, motivated by the appearance of attacks on IoT and embedded devices such as MIRAI and derivatives, several legislation activities took place all around the world. The most prominent being Californian bill (SB-327), "Security of Connected Devices", which prescribes the basic level of security of the connected device. Within the law that became active on January 1st 2020, the responsibility for the device lays on the device vendor. It is unclear how the law will address the devices that are provided by BBSPs. Following the Californian activity, several other states have started on the same path, namely Oregon and Virginia (HB 2395 and HB2793). Next to that, the USA congress is working on the IoT improvement act and cyber shield act. Europe is following in the domain of certification with the Cyber Security Act that became active in 2019. Although the Cyber Security Act at this point leaves security evaluations and testing optional, there are plans to enforce security levels in the next couple of years.

Before legislators focused on the connected embedded devices, Europe has enforced and worked with GDPR legislation for years. With insecure embedded devices the, potential leakage of information or collection of

information without the awareness of the user is possible. The party that is collecting the information from the device is responsible to implement GDPR requirements.

Real world example – leaking information from advertisements on embedded devices
The advertisement market for home appliances such as SmartTV sets and other media devices is developing fast. As any new and disruptive technology, the security and especially customer consent GDPR requirements do not receive sufficient attention. Several academic research paper have been published on the topic of consumer rights with respect to personal data tracking (online activity identifiers and data) in the scope of GDPR:

- *Watching YouWatch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices*
- *Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach*

These legislations can affect unprepared BBSPs as the deployed devices at users' premises could be evaluated as insecure or could leak user data that is covered by GDPR. The BBSPs would have to remove them, which could lead to significant losses on the side of BBSP.

The governments are entering the domain consumer embedded device security all over the world. Excluding GDPR, most of the governments are starting with recommendations; due to the concern that introduction of security requirements would have impact on business development. But a few legislators have decided to enforce the regulations from start.

GDPR - General Data Protection Regulation
GDPR is an EU regulation from 2018 that aims to protect and expand EU citizens' rights to have their data processed safely and only when needed. GDPR affects all the companies that have business on the territory of European Union that plan to process or order processing of EU citizens' data. GDPR is quite broad in the sense of person's identity, and so personal data include data that describe the person's economic, mental, or physical status, online identifiers and location data, data on ethnicity, political opinion, religious beliefs, health, and genetic and biometric data.
https://iotbusinessnews.com/2018/02/26/79400-gdpr-iot-problem-consent/

NIST – NISTIR 8259 - Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers
NISTIR 8259 (DRAFT) is intended to help Internet of Things (IoT) device manufacturers understand the cybersecurity risks their customers face. The publication defines a core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce.

ETSI TS 103.645 - Cyber security for consumer IoT
The recommendation document brings together widely considered good practice in security for internet-connected consumer devices in a set of high-level outcome-focused recommendations. The publication defines a core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce.

UK recommendation - code of practice for consumer IoT
The aim of this Code of Practice is to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design. The publication defines a core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce. It has been developed by the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), and follows engagement with industry, consumer associations and academia.

Singapore scheme - Cybersecurity Labelling Scheme (CLS)
The CLS is an initiative under the government Safer Cyberspace Masterplan, which is a plan aiming to create a safer cyberspace and protect the public and enterprises against cyber threats. The CLS is constructed as a voluntary scheme to allow time for the market and developers to understand how the scheme benefits them and it is based on several aforementioned publications.
https://www.csa.gov.sg/programmes/cybersecurity-labelling

Security Solutions for BBSPs

The BBSPs are navigating a complex ecosystem with strong needs to achieve a sufficient level of security robustness. The products stay on the market for up to 10 years and network penetration testing is not sufficient. The internationally accepted CC certification is expensive for vendors and only captures some attacks and for some versions of device SW and HW. The devices are developed and deployed with functionality in mind at the expense of security and that makes internal Red Teams inherently blind to some serious security issues.

While some BBSPs have in house red teams and perform independent penetration testing activities, in the face of new challenges for embedded devices this might not be sufficient. Here is what can a BBSP do today and how can a BBSP reach the satisfactory security robustness in the face of business challenges and governmental requirements for today and tomorrow.

There are many things that BBSPs can do today starting from simple steps.

Introduce secure development process for SW or request from your suppliers to follow one
Introduce development practices that support security in all SW components from bootloader, Linux or Android OS and middleware by requesting this from suppliers next to the requirements for functional testing.

Select your suppliers based on relevant security assessments
Make sure your supplier is providing you with up to date secure device without back doors, insecure configurations and unpatched libraries with known vulnerabilities. The basic security robustness assessment of a device can be done in a relatively short time and on a tight budget. A request for independent security robustness assessment towards your vendors could provide you with an initial assurance.

Use only needed services on the device and secure them
Reducing services to only necessary ones will significantly reduce the attack surface. With introduction of proper authentication and removal of password re-use; additional level of security can be reached. All services should be available only through encrypted and authenticated tunnels. By enabling firewall and having restrictive configuration, broadband service provider can significantly reduce the risk of the device compromise and service obstruction.

Configuration of OS security and device hardware security
The OS should be configured securely with the use of available open source or commercial tools. Next to the configuration of OS, debug ports should be protected to increase the effort attacker needs to dedicate to finding and reverse engineering the firmware.

The red team in house

Many larger BBSPs have a red team in house that are usually busy with the network operations and frequently do not have time to address the device penetration testing. The testing is frequently executed using automated SW testing tools, which have to be up to date but cannot substitute a thinking tester.

The second problem for internal red teams is the sheer amount of security challenges that are posed in front of them and expertise that touches upon many different fields. With appropriate trainings the knowledge level can be increased, however, only security laboratories have the knowledge that is up to date with current security problems from all the relevant security fields.

Finally, having a red team in-house could be expensive for some BBSPs and that is when BBSPs use independent penetration testing companies.

Independent penetration testing

Independent penetration testing companies are focused on network penetration testing of servers. They use automated tools and professional expertise for such testing, but they frequently lack testing knowledge and capabilities for embedded devices. Further, these penetration testing companies are working mostly on the general-purpose servers and do not have highly specified knowledge needed in content protection services such as watermarking. Rare are the companies that can provide security testing and assessment from end-to-end including devices, networks, and dedicated backend services.

Addressing challenges with your working partner

Riscure sees itself as an extension or substitute for your red team. A security partner can support you in your different security activities including but not limited to:

- Security testing of devices and network
- Selection of vendors based on fulfilling security requirements
- Independent security testing of the supplier equipment
- Security of supply chain
- Consulting on how to build a secure infrastructure

Riscure can perform extensive testing of the devices using methods known to a typical adversary, but also with new types of attacks on hardware and techniques that are used to reverse-engineer firmware and find credentials. Riscure can provide a comprehensive report on the device security state, with experience from the PayTV and Mobile Payment industry and certification. Riscure BBSPs can understand the security implications of new potential consumer equipment before deployment.

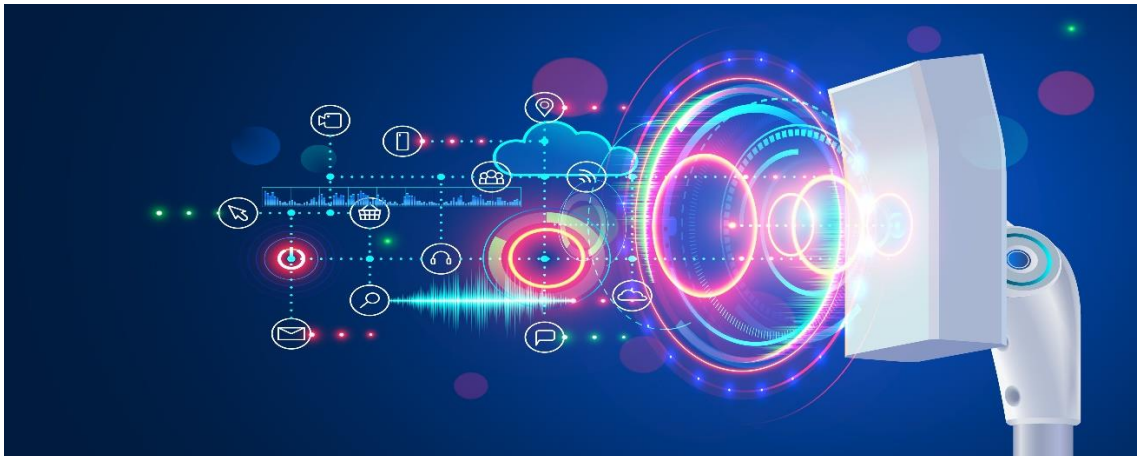
Use a one-stop shop with significant experience in the domain of security of embedded devices, media and entertainment, and payment for all your needs.

Conclusion and next steps

The new challenges posed in front of BBSPs will only grow in volume with various disruptive technologies continuing to gain traction in the coming years and legislative initiatives.

Even though there are security options currently available to BBSPs, without a security-focused partner the challenges include complex ecosystem interactions and require proper design, integration, and configuration in order to result in a secure solution.

For BBSPs, interested in improving the security of their devices and networks and reducing brand name damage and cost, the best way to ensure the security of the systems is to utilize the expertise of an independent partner with expertise in security and used technology.



How Riscure Can Help

Riscure is an international security laboratory, well recognized and respected for its media and entertainment and payment expertise. Riscure is recognized by many CAS, DRM vendors, and BBSPs to perform security assessments of a wide variety of devices and related backend applications.

Working with all involved stakeholders, from chipset and device developers as well as BBSPs, Riscure is perfectly positioned to support its clients and partners in their secure deployment and development process.

Riscure offers a broad, efficient, and flexible offering for BBSPs aiming to secure and protect their networks. With our services and expertise, we actively support our customers to reduce risks of monetary, legal, and reputational damage and delayed time-to-market.

More information about our services for BBSPs can be found here:
Network Operators service from Riscure

Interested to learn more about our offering and how to secure your device and network?
Visit our website at www.riscure.com or contact us at inforequest@riscure.com.

riscure

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road, Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com