Securing Virtual Service Generation on the Network: Adapting Digital Rights Management to Cloud-Delivered Media

Alexandra Mikityuk
Security in Telecommunications
TU-Berlin, Germany
Email: alex@sec.t-labs.tu-berlin.de

Oliver Friedrich
New Media, T-Labs
Deutsche Telekom AG
Email: oliver.friedrich@telekom.de

ABSTRACT

This work introduces a novel content protection security framework within the virtual Set-Top Box (vSTB) concept. This concept presents a fundamental change in the creation and delivery of media services such as IP Television, by shifting most of the STB’s service execution environment to a network infrastructure. This shift enables a so-called cloud-based rendering of the User Interface and therefore poses new challenges for the classical IPTV security mechanism. After successful tests on the conventional network infrastructure (legacy network), the vSTB concept takes the consolidated and virtualized network approach as its target architecture for the implementation of the vSTB Security Framework. This work briefly introduces the vSTB concept, comparing overall system latency for locally- and cloud-rendered IPTV User Interface. It also presents the novel vSTB High Level Security Framework within the virtualized network infrastructure, analyzing potential system vulnerabilities and security threats. This work defines security challenges and open issues that may arise in the context of virtual service generation and its delivery to lightweight hardware. The paper herewith provides a review of this new research topic, on which research has not yet been published.

I INTRODUCTION

The ongoing shift of media content to the cloud is currently gaining in interest for different media services, such as IP Television (IPTV). Above all, the storage of movies in and the transfer of television channels out of the central cloud infrastructure is already being implemented on a large scale. This poses new demands on the available transmission capacities of the Internet and encryption techniques, due to the bandwidth required and more advanced content protection mechanisms. Subsequently, the shift of execution of services and applications will gain in importance for media service providers.

The Virtual Set-Top Box project, initiated by our team, addresses the complexity and limited lifetime of Set-Top Boxes located on a subscriber’s premises in current IPTV/ Hybrid TV (Broadcast TV and Internet TV) deployments. This project analyzes the effects of a partial shift of STB functionality. In contrast to previous content-streaming solutions, part of the STBs functionality must instead be realized in the cloud infrastructure. This includes the generation of the user interface, execution of user applications as well as service and subscription management.

The vSTB Approach might therefore help reduce costs through a simplified centralized management of services, as well as helping increase the lifetime of STBs in the field through simpler end devices with a longer lifetime by locating STB functionalities in the operator network. This shift from the local terminal (computer, TV, phone) into the cloud requires, as it did for the classic devices, a safe, secure and standardized execution environment for new cloud-based technologies to be accepted.

The server-side execution of services raises a number of open security-related issues, such as:

- currently nonexistent protected environments for the execution of services in the cloud,
- a demand for new advanced forms of content protection mechanisms that take into account new service execution scenarios in the cloud.

It is worth mentioning at this point that content piracy remains a major threat for content providers. Video and music content has always been subject to extensive piracy. Providers such as Premiere/Sky have struggled to eliminate unauthorized free access to premium content. For this reason security and content protection issues are extremely important for the cloud-based execution of media services. This work focuses on a first definition of a High Level Security Framework for secure service generation, execution and composition in the cloud, also known as a cloud-rendered user interface, as well as the necessary
content security while streaming the protected content to the terminal.

The security issues within the new vSTB landscape have not been yet researched. However, they create a cross-domain complexity for both software- and hardware development. The current security solutions for IPTV and Hybrid TV are made up of a combination of software and dedicated hardware on the STB, which has not always been the case with the advent of new lightweight clients. One of the biggest challenges will be the integration of security mechanisms for content protection into vSTB functionalities. This will provide security of content and applications, and also support secure service generation and composition on both the network and service planes.

This work also defines a network architecture that will be used for the implementation of the security framework. The target architecture uses a consolidated and virtualized network approach with Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies, which virtualize the network control plane, for management of network resources. The architecture also uses the NFV Approach as a basis for facilitating the virtualization of home STBs. NFV supports the network centralization of the computation power of the STBs, formerly distributed within user home premises.

The main contributions of this paper are:

**Security of virtual service generation**
An exploration and analyses of server- and client-side security in the context of virtual service generation and delivery to lightweight hardware

**Security Framework**
A novel vSTB High Level Security Framework for cloud-delivered media

**Network Architecture**
Conceptual architecture of the security framework presented for a future implementation on SDN- and NFV-based networks

II RELATED WORK

Security frameworks for the vSTB Approach represent a relatively new area of research, which has yet to be investigated in detail. Nevertheless, there are a number of publications related to this subject. Given that the computation power in this approach resides in the cloud, an overview of general and potential new security issues in the cloud are presented below. With regard to content protection and content securing mechanisms, the cloud-based content protection mechanisms and the client-side STB secure mechanisms are taken into account and presented in this section.

With regard to cloud security in general, numerous security issues arise, categorized in [1] by Chow et al. as: traditional security, availability and third-party data control. Moreover, the work presents an overview of potential access management problems in cloud environments. Noteworthy problems include increased authentication demands and a mash-up authorization (an authorization against the services, which perform data mash-ups). The authors of the paper recognize advantages in the advent of thin clients (clients, where the computation mostly happens on the server-side). This will make software piracy more difficult and centralize user monitoring for content providers. In this case, authentication must be secured to avoid the stealing of authentication credentials by phishing and other technologies. With regard to increasing data mash-ups, it is obvious that their authorization mechanisms must be improved in order to avoid data leaks. The authors propose information-centric security, where the data will be protected not from the outside, but from within, which will be achieved by putting intelligence in the data itself. Chen et al. introduce in [2] an idea of new unexpected side channels and covert channels created in the shared resource environment of the cloud. Schoo et al. demonstrate [3], in which the main threats of virtual networking and virtualization environments are identified and the preliminary version of an attacking model is presented, where an external attacker tries to exploit system vulnerabilities.

Cloud-based content protection mechanisms are addressed in [3], [4]. In their work, Zou et al. present a mobile Digital Rights Management (DRM) system which utilizes a sim card on the mobile device for key storage and a cloud-based DRM back-end for managing unstructured DRM data. This can be interpreted as a motivation for a content protection back-end within the Security Architecture of the vSTB Approach in a future work. Petrovic, in turn, describes in [4] a scheme for cloud-based DRM based on extended proxy re-encryption, in order to provide anonymity and reduce the possibility of profile building for different parties. Villegas and Perez in [5] analyze new network scenarios for Conditional Access System (CAS) with permanent bidirectional connectivity and propose a new architecture for content
protection, in which parts of the currently existing CAS system are connected with network functionalities forming the new network-assisted CAS.

However, the scientific works that describe secure generation of UI in the cloud have not yet been published. Nonetheless, there are client-side secure mechanisms and countermeasures available for existing TV delivery systems. The “Secure Digital Video Broadcasting (DVB) Set-Top Box” approach presented by Acicmez et al. [6] is based on off-the-shelf Trusted Computing technologies and provides service providers and users with secure scenarios for the consumption of protected content.

III BACKGROUND

Through the rapid development of the World Wide Web (WWW) and corresponding web technologies in recent years, service development paradigms have changed. In combination with the rise of mobile and TV platforms, these paradigms have also reached the embedded domain. In this context, web browsers have also become standard in embedded devices, and trends for the centralization of services in the cloud have yielded new approaches for reaching TV and mobiles as well. Taking this into account, two new approaches to concepts for building IPTV and Hybrid TV STBs using web-based resources have been developed in our vSTB project.

These approaches are the so-called Thin and Zero Client Approaches, both of which use web-browser technology for service execution. However, the first concept involves client-side execution of services, whereas execution in the cloud is called for in the second concept. The Thin Client Approach, which uses browser technology as the STBs middleware layer and is supported by various standardization organizations, represents the current state-of-the-art in STB middleware technology and is not considered in the project.

The Zero Client Approach is a potential target solution for the Virtual STB project because this approach is the closest to the idea of remote UI execution: outsourcing as much as possible to the cloud, thus ensuring maximum simplification on the client side. Here, making customer hardware lightweight goes even further than the one in Thin Client Approach and locates not only the application layer in the virtualized environment but also the middleware layer. In the ideal case, only video decoding is done on the client. Therefore, in this approach, middleware is decoupled from hardware due to a virtualization (remote execution) that resolves hardware dependencies, completely decoupling Customer Premises Equipment (CPE) and middleware, and making the system highly adaptive and flexible, providing a variety of application environments. This approach also solves the limitations of CPE capabilities and thus enables the operator to deliver new rich multimedia services to legacy STBs and in general to any device owned by the end user, providing thereby built-in multi-screen and companion device support.

Compared to traditional Internet-based television (IPTV), certain STB functionalities within the Zero Client vSTB Approach are performed on a network server and then converted into a video stream (see Figure 1). These functionalities are the service and application execution, as well as the generation of the user interface and its composition with media content (TV, video, applications). The video stream is decoded and displayed by the lightweight STB. The STB functions, which are now executed on a network server, form a so-called “virtual Set-Top Box” in the cloud. In the course of this, separate local UI generation and a corresponding execution environment is not required on the end client (STB) anymore, which reduces the complexity of the terminal compared to IPTV. Similarly, the server-side complexity will be increased.

IV CLASSICAL CONTENT PROTECTION

In order to secure valuable content while distributing it on a network, content protection mechanisms have been developed in the past. These content protection mechanisms address different video standards and underlying transmitting technologies. They also differ in their scope of implementation.
Conditional Access (CA) [7] was introduced by DVB as standard for digital TV [8] and focuses on the definition of access conditions, which are used to decide whether access to the video content can be granted to a digital receiver or not. The encryption algorithm used in CA is Common Scrambling Algorithm (DVB-CSA). Multiple pirate attacks have been made in the past against this encryption algorithm with some success [9]. This in turn, has stimulated research in this field where new improved CA mechanisms have been introduced: e.g. an advanced CA system using metadata in [10] and countermeasures against card sharing attack by measuring the response time of a smart card used in CAS [11]. With the advent of IPTV, Conditional Access Systems have also become relevant for the IPTV domain.

Another content protection mechanism, Digital Rights Management (DRM) protects digital media assets distributed on the internet, and is more suitable for content which is copied when stored. With DRM the owner of the content has full control over accessing the content beginning at its creation and stretching until the content would be used. There are multiple proprietary DRM schemes used in the field, which are either device or smart/sim card based and implement different cryptographic mechanisms [12]. In [3] Peng Zou introduces a sim card-based implementation of a DRM Scheme with a cloud-based back-end for managing unstructured data. With regard to the protocol level, the HDCP protocol was created by Intel to protect the digital video content transmitted over the DVI bus between a DVD player and a video monitor, which was hacked through a key recovery attack in [13].

The high-level overview of CAS and DRM architectures and general encryption/decryption logic [5] is described in Figure 2. The end-to-end content protection (CP) chain of both technologies involves four steps: scrambling (encrypting), the transmission of encrypted content over networks, descrambling (decrypting) and license exchange. The Video Head-End scrambles (encrypts) the content with the key $K_{sec}$. This key is provided to the Scrambler from either the CAS or DRM Back-end for CAS or DRM respectively. After the encrypted content and the licenses have been transmitted over the network, the Secure Client extracts the $K_{descr}$ with the key $K_{client}$ out of the license. The licenses are transmitted only to authorized users. The $K_{descr}$ is then sent to the Descrambler for the descrambling of content. $K_{client}$ can be equal to the key $K_{sec}$ or not depending on the cryptographic mechanism used (symmetrical/ asymmetrical). The licenses for CA and DRM differ in a way that the CA licenses define whether the content can be accessed and the DRM licenses define the terms of usage for the distributed content. However, the back channel from the end-client to the CP back-end does not exist within CAS.

V SECURITY FRAMEWORK REQUIREMENTS

As previously mentioned with regard to content protection, current runtime environments for interactive services and security solutions for TVs are based on a combination of software and dedicated hardware, which is integrated directly into TVs or STBs. Within the vSTB Approach, the current STB is shifted into the network, which changes the existing structure of encryption through putting the content protection back-end and decryption of the content on the device. This is due to the fact that the vSTB already has to insert the interactive services and graphical control elements into the media stream on the network-side. Therefore, the paradigm shift of service execution results in security vulnerabilities in the following system elements: the content protection back-end, the network-based vSTB and the client-side lightweight STB.
The most important security issues for each of the elements are listed below. The Req. 2 and the Req. 4 will be addressed in this paper.

Content Protection Back-end
Due to the fact that each client entity will be virtually doubled within the network on the vSTB, the complexity of key handling on the CP back-end will increase. Therefore, advanced protection mechanisms are required to analyze the integrity of the data and prevent the usage of false keys.

Req. 1.: Advanced Data Integrity Analyses

Network-based vSTB
Apart from the data integrity analysis which is also required in this case, the media content will have to be decrypted on the input of the vSTB and encrypted on the output for multiple-user environments with multiple content streams per user. This process must be highly managed in order to identify possible malicious data. Moreover, the vSTB Approach creates an access point on the network, where the content is not decrypted for a certain amount of time and can be accessed by attackers.

Req. 2.: Highly-managed Multiple Key Handling

Req. 3.: Protection of Decrypted Content

Client-side lightweight STB
Current generations of STBs have strong hardware-software security architectures, which are there to prevent the propagation of unauthorized video content copies. The shift of the UI execution to the network makes the client-side hardware more lightweight. This lightweight hardware could be a minimum functional unit for the receiving of digital television signals, such as a simple hardware decoder or a lightweight client application running on a mini-PC. Nevertheless, making the client hardware lightweight must not affect the security of the system and the security mechanisms must not affect the overall system latency.

Req. 4.: Low-latency Client-Side Security Framework

VI HIGH LEVEL SECURITY FRAMEWORK ARCHITECTURE

1 SECURE VSTB

The Zero Client Approach enables UI rendering and application execution on the network, where the virtual Set-Top Box Enabler (vSTB) takes over these tasks and combines the UI and the video into the H.264/MPEG-2 stream on a server. The H.264/MPEG-2 stream is then delivered to the client, which in turn only needs to perform stream decoding. Nevertheless, the degree of service composition complexity on the operator side and network load increases when moving to the Zero Client. With regard to the drawbacks of such an approach, it is obvious that the additional network traffic caused by service delivery out of the cloud has a significant impact on the network. In order to decrease the network load, we have sub-divided the Zero Client Approach into two different sub-approaches (see Figure 3):

- the Single Stream Approach: the server combines both the video stream and the UI/Apps into one single video stream that’s delivered to the client;
- the Double Stream Approach: the server only renders the UI with applications, thereby the video and UI/Apps streams are delivered separately to the client which then has to combine both these streams itself to present it as one to the end user.

The Single Stream Approach can be realized in a way in which the H.264/MPEG-2 Hardware (HW) decoder is used on a client. However, the access management issues, service quality monitoring and content protection still require a lightweight client application running on a client HW, e.g. a HDMI-Dongle. The Double Stream Approach requires more logic and computing power on the client side since the two streams have to be overlaid and the client has to know which content stream it needs to receive. Within the exist-
(UC) Infrastructure, in which individual traffic is delivered to the end customer. Accordingly, the combined vSTB Approach is required, in which MC traffic can still be delivered over the existing MC infrastructure via the Double Stream and the individual traffic is delivered via the Single Stream Approach. The combined approach was implemented with a vendor, the implemented stack of lightweight client application is presented in Figure 4.

The application has interfaces with a session manager and an HTTP/UDP player for UC and MC correspondingly. The IGMP handling is also performed by the application, assuming that the client has to deal with MC. After the MC or UC encrypted stream is received by the end-client, the Secure Client generates a key from the MPEG-TS and sends it to the Descrambler. The Descrambler descrambles the stream and redirects it to the decoder; the HTTP/UDP Player gets the decoded stream for play out. To implement user control over the delivered service, commands from a remote control are sent back to the server to render the user interface appropriately. Considering the vSTB functionalities, the vSTB Platform architecture can be described through the four main layers depicted in Figure 5. The service/ application layer is mainly responsible for application execution and service composition (or UI Generation), which comprises its discovery, execution and composition. The functional layer executes near-hardware functions, such as different Video and UI operations, transcoding and content protection. Nevertheless, content protection mechanisms are not supported in the current implementation, which is described in Section 4 and will be part of future implementations. The session/ control layer performs the management of sessions/ users (sessions regarding an interface to the client: vSTB Client STB), to which the client STBs are assigned, including resource management for hardware assignment tasks as well. The session manager is also in charge of interfacing with the Internet and managing vSTB sessions with service/ content providers. The network manager coordinates the transport layer, controlling physical links, and handling MC requests and session handovers. To address the functional and service/ application layers in detail, the execution and composition engine accomplishes the complete service generation by running in separate virtual machines on the server, therefore making up the final UI (see Figure 6). The incoming content, as previously mentioned, will be descrambled on input, decoded and sent to the graphics pipeline. After the UI is composed, it will be sent to the encoder and then scrambled again to stream it down to the client. The final 720p UI drawing commands are sent from this engine over a direct interface to the virtual CPU (vCPU), which, in turn, utilizes the power of real hardware resources and thereby partly uses CPU. The graphical operations for the UI are then saved in the buffer from which the UI frames are captured by the frame grabber and sent to the H.264/ MPEG2 encoder. The encoder then delivers the video stream to the lightweight STB.
2 SERVER-SIDE VSTB SCENARIOS

An essential part of TV services is the provisioning of Program Guides or Electronic Program Guides (EPGs) to the end-user. The complexity of the EPGs currently available on the market poses strong requirements on the vSTB Approach, which has to be taken into account. Variations of the EPGs include Mosaic EPG and Picture-in-Picture EPG (PiP EPG), where the former presents the combination of a live channel preview in a matrix view and the latter presents a preview of a selected channel in a small window on an EPG screen. These types of scenarios can be handled only in the Single Stream Approach, they are otherwise too complex for the lightweight client to manage due to video scaling tasks in the Double Stream Approach.

The whole EPG - the bitmap matrix with \( i \) from 1 to \( l \) and \( j \) from 1 to \( l \) is then scrambled with the \( K_{en} \) and streamed to the end-user.

The same has to be performed for the Mosaic EPG presented in Figure 8, where multiple channels (e.g. 4 channels) have to be descrambled with the keys \( K_{de1}, K_{de2}, K_{de3} \) and \( K_{de4} \), scaled down, inserted into the final bitmap and then scrambled with the \( K_{en} \).

3 HIGH LEVEL SECURITY FRAMEWORK

With regard to the EPG scenarios, the High Level Security Framework for the Single Stream vSTB Approach presented in Figure 9 differs from the classical CAS and DRM architectures and presents a more complex end-to-end CP chain. This chain comprises: CP Back-End Scrambling (Encrypting), the Transmission of encrypted content over networks, vSTB Descrambling (Decrypting), vSTB Scrambling (Encrypting), Client-side Descrambling (Decrypting) and License Exchange. The Req. 2.: Highly-managed Multiple Key Handling mentioned in Section IV is addressed by the Secure Multi-Key Handler Client in vSTB, which is synchronized with the Secure Multi-Key Handler Server within the CP Back-End to manage multiple keys for multiple users and analyze data integrity.

The content in this approach is scrambled by the CP Back-End and sent over the network to the vSTB, where the vSTB Secure Framework decodes and descrambles the content, adjusts the content to that requested by the client UI and scrambles and encodes the content again.

After the processing within the vSTB, the content is sent to the end client, where the client decodes and descrambles the content. The way the streams are processed within the vSTB was described in Section 2. The license exchange takes place not only between the CP back-end and the client, but also between the CP back-end and the vSTB secure framework.

It is important to mention that with the advent of HTML5 technology, Encrypted Media Extensions (EME) can also gain in importance, assuming that the composition engine will remain a browser. Nevertheless, well-known browser security issues must be also addressed within this concept to prevent attacks on the browser. The potential virtualizations of existing CA/DRM solutions can also become an issue, as well as secure mechanisms for translation between DRM and CAS on the network.
Last but not least, the security required for multiple vSTB sessions running on the same vSTB for different users will also have to be addressed either through virtualization (which also proved to be not always secure in \cite{14}) or other advanced techniques.

\section{VII EVALUATION}

\subsection{1 VSTB APPROACH: LEGACY NETWORK IMPLEMENTATION}

For the Single and Double Stream Approach (as of now implemented without the security framework), the AGS (Aggregation Switch) network level in the metro network was chosen (see Figure \ref{fig:12}). The vSTB component was connected to the Broadband Remote Access Server (BRAS), taking into account that a PPPoE session with the BRAS has to be built up first for Internet access and that delivery of LiveTV channels is made via the existing MC infrastructure (no additional LiveTV traffic). The vSTB Clients are connected to the DSL Router via copper twin wire (50 Mbit/s Internet access), which has a connection to the access node Ethernet-DSLAM (Digital Subscriber Line Access Multiplexer). The test network leads the connection to the test aggregation environment, which aggregates the traffic coming from the access nodes to the BRAS. The backbone in this set up is simulated via Test IP Network and connects the BRAS over LER (Label Edge Router) with the vSTB Middleware Server (HTML5 Webserver) and the vSTB Content Server (Live TV/ VoD Content).

The virtualization technology used for the functional layer of the vSTB (see Figure \ref{fig:6}) is VMware ESXi 5. The machines are deployed on a single physical host. The physical host is a Cisco UCS C200 with 2x 2,4Ghz Intel Xeon E5620 CPUs, 96 GB DDR3 1333-Mhz RAM and 2x 500GB SATA 7200 RPM HDDs in Raid0. The future implementations would use a bare-material implementation rather than the virtualized environment. The client STB is the Linux-based DuneHD TV-102-T2 STB \cite{15}.

Figure \ref{fig:10} presents overall latency measurement data for comparison between locally- and cloud-rendered IPTV User Interfaces. It is important to note that both systems are not identical due to their architectural differences and cannot be compared directly. Therefore, the measurement data provided prove the feasibility of the vSTB Approach and show that the new solution can serve as a substitute for existing infrastructures. The Witbe system used for the measurements is a default system for quality reports for the IPTV solution \cite{16} currently implemented by Deutsche Telekom AG. The external probe - Witbe agent - is connected to the STB over the network bridge to analyze network traffic. The agent controls the STB through Infrared (IR) Remote control (RC). This communication is supported via the IR module of the Witbe agent. Interaction is based on preconfigured test scenarios, which are automatically executed through Python scripts. The lightweight DuneHD STB (cloud-rendered IPTV UI) was connected to the DSL Router (Speedport W722V VDSL2) via a 50 Mbit/s Internet access line to execute the test. Then the T-Home Media Receiver 303 Type A (locally-rendered IPTV UI) was connected to the same port in the same test environment to ensure a fair comparison.

As can be seen in the boxplots in Figure \ref{fig:10}, the cloud-rendered UI provides constant values for navigation with regard to Single Stream implementation. The cloud-rendered UI shows even shorter system delay times for the booting of the VoD portal due to an implementation with HTML5 technology, which cannot be implemented for the current solution due to the fact that the system interfaces are not open.
2 VSTB SECURITY FRAMEWORK: TARGET NETWORK ARCHITECTURE

The target architecture for the implementation of the High Level Security Framework presented here, is displayed in Figure 11. Considering the new network architecture, which is simplified due to the SDN and NFV technologies within the Data Centre and on the Rn, the Access, the Metro Network and the IP Backbone will fuse together. This will make the decision about the physical mapping of the vSTB component on the network easier and allow for locating the vSTB component within the SDN Infrastructure Rack.

The client-side Security Framework will be introduced to the IPv6 enabled clients. The virtualization of the clients is a part of the NFV Approach [17] [18], which supports computation centralization on the network. The clusters of the hardware resources like STBs, routers and switches form a so-called "NFV Infrastructure", which includes the Virtualization Layer and forms a basis for NFV Functions. The SDN-technologies also enable a fusion of control over the network resources (Switch 1 to N) and vSTB instances (vSTB 1 to N), to provide the load balancing mechanisms. The vSTB functionalities are spread over the network elements. The security framework interfaces the NFV functions, the SDN infrastructure rack and the vSTB middleware.

3 VSTB SECURITY FRAMEWORK: CLIENT-SIDE CHALLENGES

The lightweight hardware platforms do not necessarily have secure chips. Considering the client-side secure client presented in Figure 9, there are two different ways to make the content decryption on a lightweight hardware secure: software-based and hardware assisted CP client (Req. 4).

Software-based CP

In order to make the purely software-based CP client secure, the client software must be obfuscated and the keys must be stored in a secure storage. These keys can only be accessed by the CP client within the secure storage and internal memory.

Hardware-assisted CP

To increase the level of security of client-side decryption, Trustzone technology [19] can be used. This will enable execution of tasks related to the valuable content within the secure world of the chip that won’t require an additional secure chip, therefore requiring less hardware on the client-side. Thereby, the Secure Client itself, the Descrambler, the Renderer and the lightweight application can run within the Secure World. The challenge will remain in the creation of a client-side security framework that will support low-latency interactions with the vSTB server.

Figure 10: Overall Latency: System Response vSTB Single Stream vs. local execution

Figure 11: vSTB Security Framework: Target Architecture
VIII CONCLUSION

This paper introduced the novel content protection High Level Security Framework within the innovative virtual Set-Top Box (vSTB) concept, focusing on a SDN- and NFV-based network architecture which will become a target architecture for the implementation of the presented Security Framework in the near future. The encryption and decryption logic for classical content protection systems was presented and compared with required content protection schemes within the vSTB. The system vulnerabilities have been analyzed, and the security requirements has been defined and partly addressed in the paper. Server-side complications were addressed in detail, as well as the definition of challenges for the end-client regarding the implementation of content protection. Finally, a research topic was reviewed, which involved defining open issues in security of the vSTB concept, which enables virtual service generation and service delivery to lightweight hardware. Future work will address the detailed definition of the security framework presented here, provide a more detailed study of challenges and complications and finally present the implementation of the High Level Security Framework on next generation network infrastructures.

References


