DSTAC SUMMARY REPORT

FINAL: 8/28/2015

Introduction

The STELA Reauthorization (STELAR) Act of 2014 directed the FCC Chairman to establish a working group of technical experts that represent the viewpoints of a wide range of stakeholders "to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system designed to promote the competitive availability of navigation devices in furtherance of Section 629 of the Communications Act."

The Commission in turn chartered the Downloadable Security Technology Advisory Committee (DSTAC) for this assignment.

The DSTAC undertook extensive surveys and studies (including 50 technical presentations from 33 industry experts) of various security systems, of the trust infrastructure used for the secure delivery of commercial content and multichannel services, the variation in current video providers' distribution technologies and platforms, and the capabilities of various original equipment manufacturers and retail devices used with video services[1].

Scope

One of the points of contention within the advisory committee is whether examination of non-security related issues is beyond the scope of the congressional mandate. STELAR gave the committee a very specific mission as stated in the Introduction. STELAR does not direct the committee to recommend just any performance objectives, technical capabilities, or technical standards, but only those related to designing a downloadable security system, and only to the extent that they are not unduly burdensome. Thus some committee members believe the analysis of Working Group 4 on non-security issues exceeds the scope of issues Congress intended the advisory committee to consider.

Additionally, the definition of what is meant by "MVPD service" (multichannel video programming distributor) is a point of disagreement in the group. Some members of the DSTAC consider MVPD service to include all the various functionalities and features that the MVPD provides to its customers, including the interactive features and the User Interface which they use in their retail offerings and consider protected by copyright, licensing, and other requirements determining how their service is distributed and presented; retaining these elements is also part of respecting the contractual and copyright terms between content providers and distributors for the commercial distribution of programming.

Other members consider "MVPD Service" to be primarily video transport, and consider the inclusion of the MVPD's User Interface and other features to prevent retail devices from innovating and differentiating their products, which they believe is essential for success in the

[1] In addition, material from interested parties was captured in FCC MB Docket No. 15-64, and in demonstrations of service offerings and in public comments made during advisory committee meetings.

marketplace. They also point out the current cable specific CableCARD system allows consumer electronics (CE) manufacturers to build such products today and are in use by consumers.

FCC staff instructed DSTAC to make recommendations concerning both approaches. Both approaches were pursued as options and have been documented in the Working Group Reports.

Organization of Working Groups

The DSTAC's work was conducted and is presented primarily within four Working Group Reports. The Working Group 1 Report presents the commercial requirements of content owners, multichannel video programming distributors (MVPDs), consumer electronics companies, system equipment manufacturers, and consumers. The Working Group 2 Report presents information on current video providers' distribution architectures, technologies and platforms.

The Working Group 3 Report covers two approaches for addressing the security elements of a downloadable security system, including performance objectives, technical capabilities, and industry standards. The Working Group 4 Report presents two proposals for handling non-security elements, as well as critiques of each approach by members of DSTAC.

The four reports produced by the Working Groups, in addition to this Summary document, comprise the whole of the DSTAC congressionally mandated technical report that will be submitted to the Commission on or before September 4, 2015.

Points of Agreement

Although DSTAC is not reporting a consensus recommendation, there were major points of agreement:

- Proposals acknowledge there is a wide diversity in delivery networks, conditional access systems, bi-directional communication paths, and other technology choices across MVPDs (and even within MVPDs of a similar type). It should not be necessary to disturb the potentially multiple present and future CA/DRM[2] system choices made by cable, DBS and IPTV systems, which effectively leaves in place several proprietary systems for delivering digital video programming and services across MVPDs.
- None of the proposals recommend a solution based on common reliance[3].
- Proposals acknowledge that it is unreasonable to expect that retail devices connect directly to all of the various MVPDs' access networks; rather they should connect via an IP (Internet Protocol) connection with specified APIs[4]/protocols, via the MVPD's cloud and/or from within the home.

[2] Conditional Access / Digital Rights Management
[3] Common reliance is the concept that operator supplied equipment use the same security solution as retail devices to receive MVPD services.
[4] Application Program Interface; a set of routines, protocols, and tools for building software applications.

- Proposals acknowledge that is unreasonable to expect that MVPDs will modify their access networks to converge on a single common security solution
- Proposals acknowledge that the downloaded security components need to remain in the control of the MVPD.
- It would not be a step forward or economically viable to require an environment in which a retail manufacturer would have to equip a device with RF tuners for cable and satellite, [and] varied semiconductor platforms, to support the dozen-plus proprietary CAS technologies that are currently in use.
- It is not reasonable to expect that all MVPDs will re-architect their networks in order to converge on a common solution.

Security

WG3 "HTML5 Security APIs" Proposal

The WG3 (Working Group 3) HTML5 Security APIs proposal recommends that MVPD/OVDs (online video distributor[5]) and CE/CPE (customer premise equipment) companies adopt the security APIs in HTML5 as a non-exclusive security system interface between MVPD/OVD services and consumer electronic devices. According to its proponents, this proposal has the following characteristics:

HTML5 is the new standard defined in 2014 by the World Wide Web Consortium (W3C) as a common and open approach to deliver IP streaming media based on Internet protocols. HTML5 is a full application foundation, supporting both security elements and non-security elements. HTML5 and its Encrypted Media Extensions (EME), Media Source Extensions (MSE) and Web Cryptography (WebCrypto) extensions are being deployed across the Web today by multiple vendors on hundreds of millions of devices, and are widely supported by all major browsers.

The EME extension defines standard APIs (software programming interfaces) that permit HTML5 to support media under common encryption[6], even while protected by a variety of DRMs. EME operates as a bridge that permits competing DRM security systems to operate on a variety of platforms, including platforms that offer hardware roots of trust[7] and platforms that do not. EME enables device manufacturers and service providers to choose from a competitive market of commercial content protection technologies and enables security systems to advance ahead of, or in response to, the growing sophistication of attacks. By not mandating a single security system, it avoids creating a single point of attack for hackers.

---

[5] In the Working Group reports, OVD is sometimes referred to as OTT.

[6] "Common Encryption (AKA key-sharing or simulcrypt) allows multiple security systems of potentially diverse and divergent design to simultaneously operate on the same content stream or file." Source: Working Group 3 Report.

[7] "Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide." Source: Working Group 3 Report.

Almost all content protection companies surveyed and discussed in WG3 now support or plan to support EME. These W3C APIs are used in Web browsers but can also be used outside of a browser on other device platforms. This approach makes for a competitive market for security systems, and is technology- and platform-neutral. It is royalty free and open source.

WG3 "Virtual Headend System" Proposal

The WG3 Virtual Headend System proposal recommends that network security and conditional access are performed in the cloud, and the security between the cloud and retail navigation devices be a well-defined, widely used link protection mechanism such as DTCP-IP. According to its proponents, this proposal has the following characteristics:

An MVPD may choose a system architecture for a Virtual Headend System that includes a device located at a consumer's home, which provides a "local cloud" which has security system components downloaded to it as necessary, or the entire solution may be in their network "cloud" and offered as IP services directly to devices in the home. Because the interface to the home network (and retail devices) is standardized across MVPDs at the link protection, this enables nationally portable retail navigation devices.

Current efforts from MVPDs are cited as demonstrating that operators are working towards Virtual Headend System technology that defines a new set of interfaces to legacy network systems under a common set of IP network protocols, served from devices in the home or from the MVPD's cloud that can serve a variety of navigation devices.

Proponents have indicated that an existing link protection mechanism such as DTCP-IP would need to be modified to protect certain kinds of content (such as 4K) and for cloud-to-ground delivery.

Non-security

WG4 "Application-Based Service with Operator Provided User-Interface" Proposal

The Working Group 4 (WG4) "Application-Based" proposal is based on the downloadable apps that MVPDs and OVD providers use today to provide video and other services on CE devices such as PCs/Macs, iOS & Android tablets and smartphones, game stations, Roku, and Smart TVs. Apps are widely adopted, and MVPDs are beginning to extend this apps approach beyond large platforms by using new W3C HTML5 standards to reach more retail devices. According to its proponents, this proposal has the following characteristics:

In this System, the retail device manufacturer can choose one or more methods to enable the MVPD's services through a downloaded MVPD issued app and remote user interface.

- Device Specific Apps (e.g. iOS, Android, Samsung, LG, Xbox, PlayStation, Roku).
- HTML5 Web Apps, using W3C HTML5 standards to reach retail devices that include an HTML5 browser or components with multiple DRM support.
- DLNA VidiPath, as developed by the Digital Living Network Alliance (DLNA) and major CE manufacturers, chip manufacturers, and MVPDs. DLNA-certified retail devices on the home network receive an HTML5 Web app enabling video services to be delivered via a home server and/or via the cloud/network.

- RVU, as developed by the RVU Alliance, a technology standards alliance of service providers, consumer electronics manufacturers and technology providers. The protocol enables retail devices on the home network to receive full-featured service while leaving most of the "hard work" to the in-home "server".
- DISH Virtual Joey enables navigation of DISH's broadcast system and Hopper DVR recordings using HTML5.
- Sling Media Technology Clients enables retail devices to receive and navigate service.

All six app approaches enable MVPD supported retail devices to receive multiple MVPD and OVD video services with the CE user interface controlling the device, and the MVPD/OVD video provider's user interface controlling the service. The app model allows the applications to connect to the many different parts of each network involved in delivering service and still take advantage of each networks' efficiencies, which vary based on architectures optimized for their different physical natures (RF over coax, twisted pair copper, light signals over fiber, wireless RF). This system hides the diversity and complexity of service providers' access network technologies and customer-owned IP devices and accommodates rapid change and innovation by both service providers and consumer electronics manufacturers.

The apps deliver the MVPD service that includes modern features such as interactivity, on-screen caller ID, the ability to navigate, see recent tuning history and pause/resume on different devices in the home, regardless of which device was used. Consumers receive service as advertised and as intended by the service provider, including a user interface designed for interacting with the MVPD's experience.

Consumers receive automatic service and feature upgrades from the MVPD as service evolves via app updates, without awaiting industry consensus, standards, or rule changes.

Apps permit MVPDs to offer their services consistent with the copyright law, content licenses, and requirements under which they acquire distribution rights, such as terms governing the geographic area for delivery, provisions related to copying or redistribution, specifications for how content is displayed, requirements that particular advertising, branding, polling or other interactive material be associated with their content, and/or restricting certain types of ads or overlays from being shown with content. Apps also give MVPDs the tools to support the advertising that funds the dual-revenue MVPD business.

Apps support all regulatory requirements, including delivery of the Emergency Alert System (EAS), privacy requirements, and restrictions on the display of commercial web links in association with programming directed to children.

WG4 "Competitive Navigation" System

The WG4 "Competitive Navigation" proposal is based on proposed protocols and APIs derived from CableCARD specifications, and some based on cable TV broadcast TV or Internet APIs and protocols. According to its proponents, this proposal has the following characteristics:

In this System, MVPDs would provide a new set of interfaces to their service to allow the user interface (UI) on a retail device to differentiate itself from the UI provided by the MVPD and enable new innovation.

Three new main interfaces would be created:

- a Service Discovery Interface, providing information about available services and messaging from the MVPD
- an Entitlement Information Interface, providing information on the rights associated with the services
- a Content Delivery Interface, delivering Live, Linear, VOD, and network DVR content streams, the content protection mechanism, and the secure transfer of metadata such as entitlement and copy control information

This system would terminate the MVPD's content protection system and protect it using a single common format like DTCP-IP or similar link protection. A Digital Rights Management system (DRM), such as PlayReady, or an enhanced link protection system such as DTCP+, would be suitable for Cloud based delivery.

Additional service features could be supported by widgets[8] to be developed by all MVPDs and delivered through an enhanced Man Machine Interface (MMI). These could support unique consumer interactions, communication with MVPD network "back office" components, billing, and certain service features. Hyperlinks inside an expanded MMI widget could support targets on the greater Internet to communicate directly with an MVPD web service. Display of widgets on the device must be optional, based on user input, regulatory requirements (e.g., EAS would not be optional), and user actions. Widget requirements would need analysis to determine the level of HTML that the MMI should support.

Under this system, obligations of devices should be established by the Commission, rather than by the terms of MVPDs' regulatory and contractual obligations.

This system would require standardization from a number of different standards and the development and implementation of some new protocols and standards.

Relationship of System Proposals

DSTAC considered how the various proposals might work or not work with each other. The WG3 HTML5 Security APIs proposal can support the WG4 "Application-Based" proposal, and the WG3 "Virtual Headend" Proposal can work with the WG4 "Competitive Navigation" proposal. The WG3 HTML5 Security APIs proposal also supports the security elements mentioned in the WG4 "Competitive Navigation" proposal, but there was insufficient time and insufficient detail about other combinations to assess the likely amount of interoperability in the time allotted to the committee.

[8] Reference: http://www.w3.org/TR/widgets-apis/