

[Advanced Search](#)[ABOUT](#) [MEMBERS](#) [SPONSORS](#) [SUBCOMMITTEES](#) [TECHNICAL DOCUMENTS](#) [NEWS](#) [EVENTS](#)[SPOTLIGHT ATSC 3.0](#) [CONTACT US](#)

SECURITY, CONTENT PROTECTION HIGH PRIORITIES FOR NEXTGEN TV

Posted on March 5, 2020 in [ATSC News](#)

Reprinted with permission from TVTechnology

By LYNN CLAUDY

WASHINGTON—Early in the ATSC 3.0 development process it became readily apparent that for prevention of content piracy or unsanctioned signal retransmission, and to enable the capability to run auxiliary subscription services, the broadcast signal would need to be encrypted.

Within today's completed set of ATSC 3.0 standards, encryption is indeed a fundamental part of the overall system. This includes cryptographic signing of signaling and applications, secure protocols in the Studio-to-Transmitter (STL) link and protection of broadcast content through encryption. All three of these areas need to be protected in order to thwart security attacks on ATSC 3.0 broadcast transmissions.

THE BACKSTORY

As a brief aside, here's a little history: While it's theoretically possible to achieve the above goals of content protection without encryption, the practical challenges make it quite difficult. Arguably, this mistake was made with the original ATSC digital TV service (now retrospectively referred to as "ATSC-1"), which was standardized in the mid-1990s, then launched as a totally in-the-clear service in the late 1990s (and remains so today). The idea of encryption really wasn't investigated rigorously or pursued intently during ATSC-1's development and deployment, because back then, free over-the-air television was considered synonymous with unencrypted, in-the-clear transmission.

By the time the advantages of encryption (even for the free broadcasting service) became appreciated, ATSC-1 service had already been in place for awhile, and it was too late to add encryption at that

point. Too many TV sets had already been sold and the thought of disenfranchising them was essentially unthinkable.

So the industry came up with the “broadcast flag” concept in the early 2000’s whereby broadcasters would set a “flag” in their transmissions (the specification for the Redistribution Control Descriptor is still included in the ATSC A/65 PSIP standard) that indicated content protection was asserted. Receiver manufacturers would then be required by FCC regulations to look for such flagged content and allow their devices to output signals only to “protected outputs” such as HDMI ports with HDCP encryption, or in lower resolution to other digital or analog outputs.

Near the end of 2003, the FCC adopted the broadcast flag rules, which required TV sets manufactured after July 1, 2005, to comply with its receiver rules for output signals. This FCC decision was controversial, however, and a lawsuit filed with a U.S. Appeals Court resulted in striking down the broadcast flag regulations in May 2005, with the court ruling that the FCC did not have jurisdiction to regulate receivers in that way. That ruling essentially ended the broadcast flag program.

The broadcast flag was not the television broadcast industry’s first experience with content protection, which goes back to the analog television days. Anyone remember SuperTV? I remember it because it was an evening-only subscription television service provided on broadcast Channel 50 (then WFTY) in the Washington, D.C. market, which ran from 1981 to 1986.

Several other cities had similar formats with names like OnTV, Spectrum and SelecTV. Subscribers needed a set-top box (this was back when TV sets were deep enough that they actually had tops on which boxes could sit), and the system used the Zenith SSAVI (Sync Suppression And Video Inversion) system for decoding, which is pretty self-descriptive as to how the encryption worked: The amplitude of the analog sync pulses were changed and the video of some of the horizontal TV lines were inverted so that the picture looked jumbled, even if the TV achieved sync. Audio for the encrypted service was delivered on a subcarrier, and the station’s standard audio channel carried a barker loop telling viewers they were tuned to a subscription channel. It was an innovative system but ultimately destined for failure with the rise of cable TV and other market factors.

Coming back to the present and the current ATSC 3.0 solution for content protection, it goes without saying that effective encryption and decryption of television signals have come a long way in the digital age and are now quite complex operations. For those that really want to understand how it’s done and are willing to put in the time (you don’t have to be a rocket scientist, but it might help), most of the details are available in excruciating detail in a few relevant, publicly available ATSC and CTA documents.

For those that attended the recent IEEE Broadcast Symposium in Hartford, Conn., the general principles of content protection, signaling/application signing and STL security in ATSC 3.0 were explained in plain language to the symposium audience by consultant Pete Van Peenen, Sony’s Adam Goldberg and consultant Merrill Weiss, respectively. To whet your appetite for the subject, a few of the basic concepts are described below.

CONTENT PROTECTION

For content encryption/decryption, Figure c.1.1 from the ATSC Technology Group Report on Digital Rights Management (DRM) Guidelines (left) shows the workflow for how a broadcast TV set with internet access is expected to handle encrypted content, which in this example is a Scalable HEVC service with an encrypted enhancement layer. You can follow the numbered steps in the diagram to get a feel for how the requests and permissions flow. There is a similar diagram for TV sets that are not connected to the internet.

SIGNALING SECURITY

In the ATSC 3.0 protocol, signaling tells the receiver information about the content and how to tune and retrieve it, which is described in the ATSC A/331 Standard on Signaling, Delivery, Synchronization and Error Protection (available [here](#)). In a so-called “man-in-the-middle attack” (in which a receiving/re-transmitting entity interposes itself between the broadcast transmitter and consumer receiver), an attacker could potentially alter the signaling associated with how to tune and retrieve content and redirect the receiver to change the content displayed.

To avoid this kind of mischief, cryptographic signing is applied to signaling in ATSC 3.0, described in the ATSC A/360 standard (available [here](#)). Cryptographic signing is a technique using public and private keys and a public key infrastructure, whereby an independent certificate authority can provide verification of public keys.

APPLICATION SECURITY

The ATSC 3.0 system includes an application execution environment for downloading applications. Cryptographic signing is also required to be applied to applications to avoid bogus or unauthorized executable code in the broadcast content. CTA Recommended Practice CTA-CEB 32.9 for ATSC 3.0 Television Sets, Security and Protected Services recommends that receivers should refuse to execute any apps without signatures, or whose signatures are not verified.

STL SECURITY

Another point of possible attack in the ATSC 3.0 system is the Studio-to-Transmitter (STL) link, where at least in theory, if no security measures were taken, a man-in-the-middle attack could replace the content intended to be transmitted. The ATSC security protocol for the STL link is described in ATSC Candidate Standard A/324. Security measures include a signing function that can authenticate the data and content of the stream, as well as a system function that securely generates and delivers the keys used by the signing function.

CONFORMANCE TESTING

In late September 2019, at the Consumer Technology Association (CTA) Technology & Standards Fall Forum, the NextGen TV logo was unveiled for consumer devices to use to show that they are ATSC 3.0 compliant. To ascertain compliance and obtain use of the logo by CTA, devices must pass a conformance test suite developed by ATSC and industry partners that exercises the functionality of the receiving device when presented with various ATSC 3.0 usage scenarios. Integrated by reference into the conformance test program, and managed separately by an independent third party organization (currently being formed), are conformance tests associated with cryptographic signing of signaling/applications and content encryption. The NextGen TV logo on consumer products will assure that they can process and present encrypted ATSC 3.0 programs and services reliably and are protected from security attacks.

We've certainly come a long way from SuperTV!

Lynn Claudy is senior vice president of technology for NAB and chairman of the ATSC Board of Directors. Reprinted with permission from TV Technology. For a comprehensive source of NextGen TV coverage, see TV Technology's [NextGen TV silo](#).

Posted in [ATSC News](#)