

Protección de la Próxima Generación de TV-Paga

Amenazas de Seguridad de TV-Paga en Evolución

Todos los operadores de TV-paga comparten el mismo objetivo fundamental. Este es, asegurar la monetización del contenido y específicamente, proteger el contenido y los servicios contra la piratería. Se interesan particularmente en asegurar sus operaciones contra las amenazas de "fuga de ingresos", tal como el robo de servicios, pirateo de tarjetas inteligentes, etc. Mientras la TV-paga va cambiando hacia la entrega digital alrededor del mundo, los operadores tienen que estar preparados para responder a las amenazas de seguridad en evolución. Las nuevas tecnologías de entrega ofrecen oportunidades para crecimiento de suscriptores e ingresos, y a la vez, presentan retos nuevos de seguridad para el mundo TV-paga.

Mientras la seguridad para sistemas de TV cable analógico se enfocan en prevenir el robo de servicios, el reto es completamente diferente y más complicado en la transición a servicios de TV digital. Por lo tanto, cuando los operadores planifican una transición de TV analógica a digital, tienen que contender con cuestiones complicadas. La meta es asegurar que la trayectoria de seguridad que se toma, minimiza los costos sin sacrificar la capacidad de cumplir con los requisitos a largo plazo. La selección de tecnología de seguridad es esencial para la competitividad total y prosperidad del operador de TV-paga.

Consideraciones Para TV Digital

La evaluación de opciones de seguridad pone en juego un montón de consideraciones sobre formatos de video antiguos, la cantidad de suscriptores afectados por la transición a TV digital, la antigüedad y tipos de STBs existentes en el campo, como gestionar las logísticas infraestructurales, y las metas de negocio a largo plazo del operador.

Mientras los operadores de cable contemplan cambios significativos en el perfil de sus servicios, les conviene considerar en paralelo el valor aportado por los operadores de seguridad de TV digital. Estos cambios potenciales, vistos desde un panorama de alto nivel incluyen:

- La transición de analógico a digital
- Escoger entre formatos de video MPEG-2 o MPEG 4
- Ofrecer solamente servicios de definición estándar (SD), o incluir alta definición (HD) desde el principio
- Añadir soluciones híbridas basadas en IP a las redes de transmisión

Los operadores de TV-paga de cualquier tipo, y en cualquier etapa de desarrollo de la red, consideran que una arquitectura de seguridad flexible y efectiva, es esencial para habilitar modelos de negocio innovadores y mejorar su posición competitiva. Por lo tanto, la forma y flexibilidad de la solución de seguridad total, se ha convertido en una decisión de estrategia crítica. Esta consideración lleva la perspectiva de la tecnología de seguridad, más allá del concepto básico de protección de contenido, hacia el concepto amplio de seguridad de ingresos.

Hay muchos factores de seguridad para TV-paga que tienen que considerarse, no solamente los financieros. Entre ellos están:

- El costo inicial de compra (CAPEX)
- Costos operacionales (OPEX)
- Costos de fallos de seguridad no resueltos (pérdida de ingresos)
- Costos para superar los fallos de seguridad (reanudación de seguridad)
- Costos de certificación de STBs y tiempo de elaboración
- Selección y disponibilidad de STBs (competitividad entre vendedores de STBs)
- Habilidad de obtener licencias de contenido Premium (CA de confianza/vendedor DRM)



Preocupaciones de los Dueños de Contenido

Las licencias sobre el contenido son la piedra angular del negocio de TV-paga. Para los estudios y dueños de contenido, la amenaza de la piratería de gran escala, son una preocupación importante porque pueden socavar la vida de ingresos potencial de su producto. Los dueños de contenido se enfocan en derechos digitales por medio de procesos tecnológicos y legales para asegurar que un solo canal de distribución no impacte el ingreso potencial en otra área geográfica y ventanas de lanzamiento. Además los intereses comerciales para contenido HD son mucho más altos que para SD, y ahora se añade el contenido 3D a la mezcla.

Los dueños de contenido e igualmente los operadores, dan por hecho que los vendedores de seguridad de TV digital se enfrenten a los retos en evolución, por medio de las tecnologías y herramientas que abarcan la seguridad de ingresos completa, ya sea durante la creación de contenido, el almacenaje, la entrega, el consumo, y más.

En este respecto, el operador que está considerando una transición digital, se beneficiara si escoge un vendedor de seguridad reconocido y respetado por los proveedores de contenido. Hay sólo un criterio que importa: un historial comprobado de despliegues de operadores de TV-paga alrededor del mundo.

Sistemas CA Antiguos

Cuando la TV digital fue introducida por primera vez en mediados de la década de 1990, todas las redes de transmisión eran unidireccionales, es decir, no había canal de retorno desde el STB hacia la cabecera. El acercamiento tecnológico que se tomaba, que parecía buena idea en su tiempo, era proteger los "secretos de TV-paga", tal como las autorizaciones del suscriptor y claves de decodificación, en una "tarjeta inteligente", que se proporcionaba al suscriptor junto con el STB. Los proveedores de servicios requerían una solución de seguridad robusta que no dependía en una conexión física entre la red y los STBs, bien adecuada para sistemas de "acceso condicional" basados en tarjetas inteligentes.

Desafortunadamente, la piratería surgió pronto y evolucionó en un negocio sofisticado, donde el análisis e ingeniería inversa de tarjetas inteligentes, y también la decodificación de las comunicaciones con el CPU del STB, se hicieron comunes. Todos los sistemas CA antiguos sufrieron la piratería, de una manera u otra.

Este es el inconveniente de los sistemas anticuados: si la seguridad es comprometida, todas las tarjetas inteligentes tienen que ser revocadas y reexpedidas. Por lo tanto, es una práctica común entre los vendedores de sistemas anticuados y operadores, cambiar las tarjetas más o menos cada tres años.

La Evolución de los STBs

Avancemos nuestro reloj al día de hoy y el entorno de video cambia completamente. Los proveedores de cable y satélite todavía usan los STBs por supuesto, pero estas cajas tienen mucha más inteligencia y frecuentemente mucha mejor conectividad que las del pasado. Los STBs de hoy, típicamente tienen conectividad de doble sentido, y los operadores van añadiendo video bajo demanda (VoD) y servicios interactivos.

Los STBs modernos pueden hacer mucho más que sus predecesores. Su poder procesador (para decodificación y descompresión de video, y también para exponer guías electrónicas de programación y la ejecución de aplicaciones interactivas sofisticadas), rivaliza con las computadoras personales. Pueden hacer con el software, lo que antes requería hardware dedicado, y es este poder el que mueve la balanza a favor de seguridad basada en software para los STBs.



La mayoría de los STBs son perfectamente capaces de manejar funciones de seguridad usando una combinación de software y características de seguridad integradas en el CPU, así se puede evitar el costo de las tarjetas inteligentes y las logísticas de distribución asociadas.

Seguridad Sin Tarjeta

La seguridad sin tarjeta de los STBs modernos puede consistir de una caja de muy bajo costo, que contiene un módulo de seguridad con alta ofuscación basada en software, o un sofisticado sistema en el chip (SOC), con características de seguridad integradas, que permiten la más robusta e impenetrable seguridad de TV-paga posible hoy en día. El módulo está basado en software pero reside en un entorno de seguridad alta que no puede ser penetrada por las herramientas tradicionales de los piratas de tarjetas inteligentes. La gran diferencia es que mientras una tarjeta inteligente se puede quitar de la caja, analizar con gran detalle y hasta clonada, el SOC impide este tipo de análisis al estar integrado dentro del CPU de la caja.

La solución segura del SOC también resuelve el temido problema de piratería donde se comparten las claves de acceso, conocido como "control word sharing". En algunos sistemas anticuados, la clave de acceso se transmite sin encriptación entre la tarjeta inteligente y el decodificador del STB. Los piratas han encontrado la manera de interceptar la clave y compartirla con otros suscriptores (que no han pagado) a través de Internet. De esta manera, la caja que ha sido decodificada, puede ser usada para ayudar a otros a robar servicios. En el entorno seguro del SOC, la clave nunca está expuesta sin codificar fuera del área segura, y por lo tanto, la amenaza de claves compartidas es superada.

Ventajas de Seguridad Basada en Software

Como hemos dicho, el costo y el tiempo requerido para remplazar un sistema de seguridad basado en hardware pueden ser importantes. Por lo tanto, la renovabilidad de subsistemas de seguridad, es una ventaja clara en un entorno de amenazas y oportunidades para un negocio que cambia con rapidez, haciendo la seguridad basada en software una opción atractiva. La seguridad de contenido es una guerra de armas contra los piratas y defraudadores, y por eso la seguridad tiene que ser renovable. La seguridad basada en software, en combinación con la tecnología SOC de última generación, ofrece opciones flexibles y renovables que permiten a los operadores mantenerse un paso adelante.

La seguridad basada en software combina costos CAPEX y OPEX más bajos en una ecuación de Costo Total de Propiedad más favorable que la de los sistemas basados en hardware. Las amenazas pueden ser contrarrestadas por medio de actualizaciones OTT, evitando los temidos reemplazos de tarjetas.

Tomando la Decisión Correcta Para la Seguridad de TV Digital

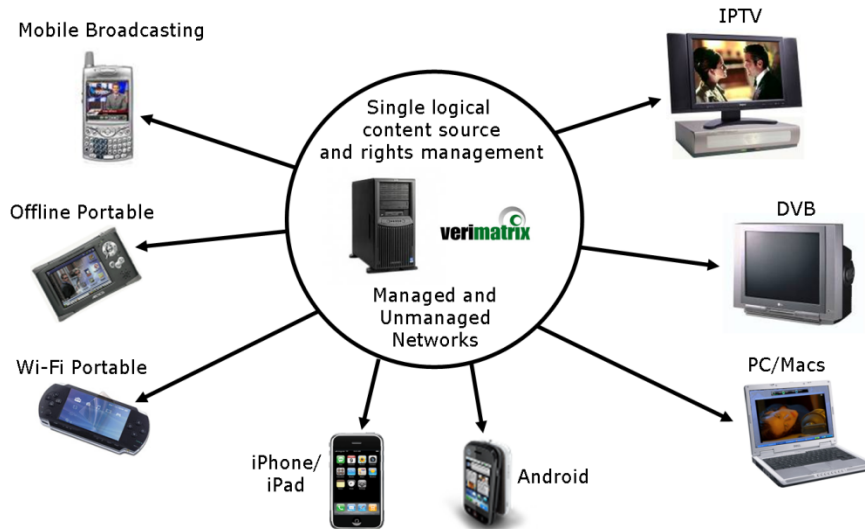
Aún si un operador de cable analógico está simplemente contemplando la transición inicial al entorno digital, es imperativo escoger una arquitectura de seguridad con soporte para los requisitos inmediatos y a la vez sentar las bases para el futuro, un futuro que puede incluir entrega a PCs y Macs, consolas de juego, teléfonos inteligentes, tabletas Web y otros dispositivos móviles.

En última instancia, los proveedores de servicios desean implementar un sistema de seguridad que pueda servir como plataforma de seguridad de ingresos con una sola fuente, para servicios diseñados para alcanzar pantallas múltiples a través de redes múltiples. Ellos desean una solución que combina lo mejor de la encriptación, el acceso condicional, la gestión de derechos, y las técnicas de marca de agua, para aplicar cualquier tipo de seguridad apropiado para cada servicio. No importa que red de entrega sea utilizada, ni que tipo de dispositivo el suscriptor use para acceder al contenido.

Afortunadamente, los sistemas de seguridad basados en software proporcionan la flexibilidad para eludir las restricciones de los sistemas tradicionales de acceso condicional (CA), sin comprometer la seguridad

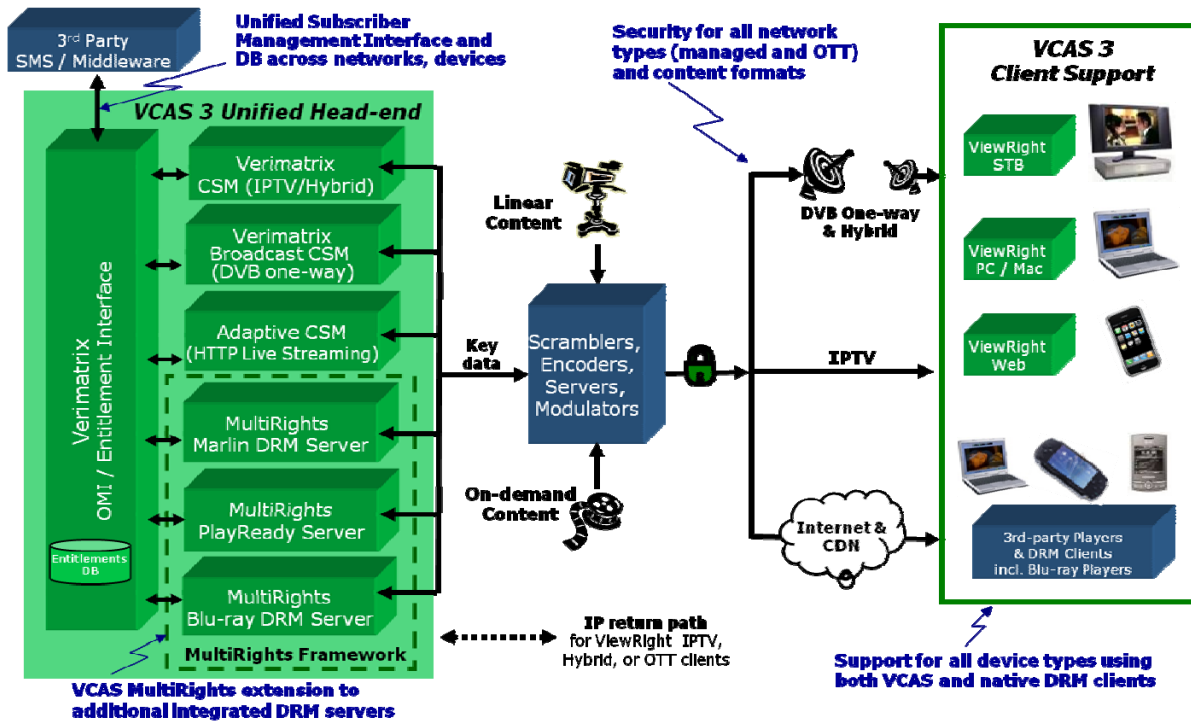


ni añadir complicaciones a la experiencia del consumidor. De hecho, los sistemas de seguridad basados en software proporcionan nuevos niveles de seguridad, esencial para los nuevos modelos de servicio con dispositivos múltiples, que serían imposibles de lograr con sistemas anticuados.



Un sistema de seguridad unificada para TV-paga es un ingrediente integral para los operadores que desean ampliar el perfil de sus servicios. Así podrán lograr las obligaciones de sus contratos y la protección de sus servicios. Pero más importante aún, un sistema de seguridad unificado, basado en software, ofrece capas de protección múltiples, permitiendo que los nuevos modelos de negocio surjan y florezcan.

VCAS 3 High-level Architecture



© 2006-2011 Verimatrix, Inc.

1