

IN-DEPTH CONTENT PROTECTION

SECURITY | from 25

falling into the "analog hole"—the link in home networks where a DVR or other digital device employs an analog output to an analog TV—will lack the protections offered by closed IPTV systems has increased Hollywood's desire to see additional content protections like digital watermarking

applied. Some in the CE and video Internet distribution sectors characterize such efforts as "overreaching."

"The thing that concerns us most is that this bitter fight just continues to alienate consumers with hassle, until they say, 'I'll just go read a book instead,'" says Dmitry Shapiro, CEO of video Internet portal Veoh

Networks and former CEO and founder of Akonix, a peer-to-peer security company whose solutions are now in use among banks and other enterprise markets.

"I encourage mainstream broadcasters to understand a scenario that isn't about creating technical roadblocks, but about providing a user experience that makes piracy less tempting," Shapiro says. "In an office next to me, a dozen engineers are smart enough to pirate content. The reason they don't is that it's easier and less expensive to buy it on iTunes. That's what [Apple Computer chairman Steve] Jobs did well: piracy is just too time-consuming. The motion picture industry needs to get to a great price point and user experience."

Coral Consortium president Jack Lacy agrees. Pointing to iTunes as a winning consumer proposition, Lacy argues that "sometimes the best security is a really good business model. We've seen solutions that are not completely secure, but that have enjoyed great success. We need to create intuitive propositions with high quality and ease of use: I buy a device, I know how it's going to be useful. That's the biggest challenge."

Meeting that challenge "is not a trivial problem," he says. "But right now we have a situation where the consumer runs into the boundaries. It's predictable that the industry would first have created a situation that is a bit too confining. Now we need to remove that barrier so consumers don't see it."

Like Shapiro, Panasonic's Fannon argues that the reasonable goal of content protection "is to keep honest people honest or provide enough of a speed bump to make real pirates or thieves know that the content owner has a right to go after them in court. All you need is simple, inexpensive mechanisms that are enough for vast majority of users and uses, and for anyone who intends to misuse it, you have the right to legal recourse."

While Panasonic, a producer of devices using DTCP (Digital Transmission Content Protection), is glad the Digital Living Network Alliance is embracing link security (see p. 1), Fannon says his company is concerned that other technologies threaten to discourage content consumption. He points to MPA's efforts to "revise the broadcast flag law with language defining enforcement 'over digital networks,' which could be your home network. Who has the right to tell you what you can send from point to point on

See **SECURITY** | 28

High Security at Low Costs Is New Mantra

As major players strive to resolve the tension between rights holder desires for maximum security and device maker desires for optimal costs, new technology innovations may yet open doors to reasonably priced solutions.

In March, for example, Verimatrix announced availability of a new user-specific forensic digital watermarking solution. While many content providers watermark movies before encryption, they also want to see "watermark post decryption and post-decoding, so you have a clear chain of custody" and to close the analog hole, says Steve Oetegenn, executive vice president, global sales and marketing, for Verimatrix.

To continue that chain down to the set-top level, the new VideoMark software incorporates an algorithm optimized for the limited processing power of a set-top box. Although it enables association of specific content with a specific set-top and subscriber, VideoMark won't prohibit illicit copying at the analog hole. However, he adds, "you'll be able to trace the culprit."

In its entirety, the Verimatrix copy protection solution stores encryption keys at the headend, then decryption at the set-top. Every set-top receives a digital certificate for authentication on the network, "and then we provide key management," Oetegenn says. "It's what we call DRM-plus, a content protection DRM package designed for IPTV."

As a Coral Consortium member Verimatrix is mindful of complexity and costs associated with additional protection schemes, hence the algorithm designed around minimal processing requirements, Oetegenn says. Caught between industry sectors, its primary constituencies are content providers and network operators.



Steve Oetegenn, EVP, global sales and marketing, Verimatrix

"We're seeing considerable uptake and requirements for watermarking across the globe," he notes. "The early adopters will likely be in the hospitality industry, due to earlier release windows, but we have already signed IPTV customers in Japan, Europe and the U.S., all of which will deploy session based, set-top box watermarking this year."

Conditional access system suppliers also are seeking to satisfy content owners while tackling the increased complexity associated with extending their reach beyond closed IPTV systems into networked consumer devices. In January, for example, Widevine Technologies reached an agreement to pre-integrate its Widevine Cypher Virtual SmartCard technology into media processors produced by Sigma Designs, which claims approximately 70% of all IPTV set top boxes, as well as use in a variety of Blu-ray players, DVD players, digital media adapters and portable media players. ■