1105 MEDIA

www.secprodonline.com

Security Products

November 2008

# INSULATING INNOCENCE

## Network security technology part of emerging standards in Internet child protection

By Nat Hillary

It's an important decision when choosing a network security technology within industry standards, using the Children's Internet Protection Act as an example. While addressing a specific concern—the safety of children while using the Internet in schools and libraries—the scope of CIPA is so limited that there are other pieces of legislation in its wake, such as the proposed Deleting Online Predators Act.

The question is, how is it possible to select a technology that helps to address current standards while keeping an eye toward emerging standards?

The trick is to ensure that the technology selected can competently handle current and future threats. Marry this with a culture that incorporates a rigorous security and acceptable usage policy, ongoing security education and suitable controls to ensure continued compliance. As background, it is important to examine CIPA in more detail.

The Schools and Libraries Program of the Federal Communications Commission Universal Service Fund, commonly known as E-Rate, makes discounts available to eligible schools and libraries for telecommunication services, Internet access and internal connections services. Discounts for support depend on the level of poverty and the urban/rural status of the population served and range from 20 to 90 percent of the costs of eligible services.

### CURBING ILLICIT CONTENT

In an attempt to limit children's exposure to pornography and explicit content online, CIPA was introduced as part of the 2001 appropriations bill and passed by Congress. CIPA requires that any school or library that intends to use E-Rate discounts for computers and Internet access adopt an Internet safety policy and employ technological protections that block or filter certain images deemed obscene, pornographic or

harmful to minors.

Although the security technologies that CIPA regulates must be used to address threats of a specific nature, the combination of technologies and policies that CIPA advocates helps to reinforce the creation and maintenance of a culture of security. However, it is important to understand the limitations of this standard to ensure that any security technologies procured for compliance also position the user for compliance with any future standards.

There are essentially two components of CIPA—the technology measures for blocking and filtering access to images that are obscene, child pornography or otherwise harmful to minors, and the creation of a Neighborhood CIPA.

The NCIPA component essentially states that in order to be eligible for E-Rate discounts, a school or library must have a valid safety and acceptable use policy that is defined via collaboration with the local community. This ensures that the policy matches the values of the community that the school or library serves.

NCIPA provisions require the policy to address access by minors to inappropriate matter on the Internet and the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications—including instant messaging, unauthorized access, hacking and other unlawful activities by minors online. The act also requires policy regarding unauthorized disclosure, use and dissemination of personal identification information regarding minors and measures designed to restrict minors' access to materials harmful to them.

So, for breeding a culture of security, the provisions of NCIPA are really quite sound. But there's the security technology piece also.

When CIPA was created, exposure to threats that are obscene, child pornography or otherwise harmful to minors was considered to occur only via an Internet browser, so the security technologies that are typically deployed to address the CIPA standard include URL filters, Internet browser content scanners or HTTP caching proxies with built-in content blocking.

Each of these technologies serves a very specific purpose and is not extensible for dealing with emerging threats. While these technologies improve Internet security, they do not make accessing the Internet safe.

## SAFETY VERSUS SECURITY

In addition to content filtering, Internet security includes those systems as well as processes that are used to manage user identity and Internet access rights, as well as those that prevent malicious software. Internet safety, on the other hand, refers to the human element and social engineering factors of Internet use. To put the two terms in context, consider an example: a system that secures against malware infections from the Internet will not protect children from posting personal information to a social networking site like Facebook—information that can be used to identify and locate them, compromising safety.

By combining network security technologies with up-to-date security policies, CIPA provides the basis for a culture of security. However, the security technologies required by this standard are limited.

The limitations of the security technology required by the CIPA standard have been recognized. In an attempt to increase the level of safety in schools and libraries eligible for E-Rate discounts, the Deleting Online Predators Act was brought before Congress in 2006 but never passed. This act would have required that schools and libraries that receive E-Rate funding, in addition to meeting CIPA requirements, protect minors from online predators by prohibiting them from accessing commercial social networking Web sites such as Facebook or MySpace, and chat rooms such as AOL Instant Messenger or Yahoo! Chat, when not under parental supervision.

Whether passing this stalled bill would make the Internet safe for minors while respecting their First Amendment rights is still subject to debate, but irrefutable is the fact that the nature of online threats to minors is changing. So how does one make the right security technology choice?

## CHOOSING THE RIGHT SECURITY

A wide variety of solutions provide the specific security technology protection measures required by CIPA. A word of warning though; despite what some vendors may claim, there is no such thing as CIPA-compliant software or filtering devices. The question is, what network security technologies can help to address the requirements of CIPA now, as well as any emerging standards, such as DOPA?

Again, Internet security is defined as those systems and processes used to manage user identity and Internet access rights and prevent the ingress—or even egress—of malicious software, in addition to content filtering. A comprehensive and cost-effective solution for this involves unified threat management appliances.

UTM appliances incorporate network security technologies encompassing firewalls, antivirus, intrusion prevention systems, e-mail spam filtering and World Wide Web content filtering into a single appliance. Furthermore, they also include user identity management technology, either built-in or in concert with other solutions such as an active directory server, to make a complete Internet security solution.

CIPA standard compliance with most UTM devices is straightforward. The best appliances provide a URL categorization mechanism that can be used to prohibit access to images that are harmful to minors. The technology also prevents children from accessing this material via the many workarounds that are in common use, such as using URL proxies or simply accessing sites via the https:// version of the URL rather than the http:// version.

For DOPA, the same URL filtering technology can be used to prohibit access to any social networking or chat room sites, but these appliances also are able to detect whether an IM or peer-to-peer application is in use and prohibit that use.

In addition, these UTM appliances help combat current and emerging threats by offering user identity management, gateway antivirus, intrusion prevention systems and e-mail spam filtering. When combined with the type of security policy advocated by CIPA, UTM solutions provide a powerful means of meeting current and emerging security standards for both education and business.

## A BALANCED APPROACH

CIPA provides a great starting point for defining a culture of security via a combination of technology, procedures and policies. The following excerpt from a National Telecommunications and Information Administration report on CIPA discusses one approach for meeting this standard:

"Members of the International Society of Technology in Education adopted numerous methods to ensure that students had a safe, educational and age-appropriate experience online, including acceptable use policies, software technologies, teacher monitoring and supervision, and student education programs."

The same report also summarizes the need for balancing the importance of allowing children to use the Internet against the importance of protecting children from inappropriate material. The report discusses accessing online educational materials with minimal content blockage, deciding locally how best to protect children from Internet dangers and understanding how to use Internet protection technology measures. Further, the report recommends considering a variety of technical, educational and economic factors when selecting technology protection measures and adopting an Internet safety strategy that includes technology, human monitoring and education.

Whether in education or business, combining Internet security technologies and a culture of security is a powerful combination to create a safe Internet environment. Making the right Internet security technology choice ensures that this environment will continue to be safe in the face of current and emerging threats. When combined with an appropriate culture of security, UTM appliances provide a compelling solution not only for meeting CIPA, but also the potential requirements of DOPA and of any emerging standards for some time to come.

*Nat Hillary is a marketing analyst for WatchGuard Technologies.*

### *About WatchGuard*

Since 1996, WatchGuard has been building award-winning network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. These fully extensible threat management (XTM) solutions feature reliable, all-in-one security, scaled and priced to meet the unique security needs of enterprises. Our products are backed by 7000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including education, healthcare, and retail. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

### *About WatchGuard Network Security Solutions*

WatchGuard offers affordable, all-in-one network security appliances that combine firewall, VPN and security subscriptions to protect your network from spam, viruses, malware, spyware, intrusions and more. Our extensible threat management (XTM) solutions scale to meet the unique needs of your enterprise, feature easy to use management tools, and support for secure mobile connectivity. Education, retail and healthcare enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

**Contact us:**
**WatchGuard Technologies, Inc.**
505 Fifth Avenue South
Suite 500
Seattle, WA 98104
United States
Tel: +1.206.613.6600
Fax: +1.206.521.8342

**Americas Sales**
United States, Canada, and Latin America
Tel: +1.800.734.9905 (United States and Canada)
Tel: +1.206.613.0895 (Latin America)
Email: americasinfo@watchguard.com

**EMEA Sales**
Europe, Middle East, and Africa
Tel: +1.206.613.0895
Email: emeainfo@watchguard.com

**APAC Sales**
Asia Pacific, Australia, China, and Japan
Tel: +1.206.613.0895
Email: apacinfo@watchguard.com