IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2004 Published by the IEEE Computer Society
Vol. 5, No. 5; May 2004

Features Editor: Rebecca Deuel

Digital Postmark Helps Fight Spam, Virus Attacks

Terry Costlow

Researchers at Penn State have developed a method to trace Internet messages' regions of origin. By marking only the messages' region, not the specific source site, the technique alleviates some privacy concerns while enabling you to trace the origins of spam, virus attacks, or illegally copyrighted materials.

The approach, dubbed *border router packet marking*, was created to make it simpler for organizations to block distributed denial-of-service attacks without blocking legitimate users from accessing a Web site—often the goal of virus creators.

Developed by Penn State researchers, Ihab Hamadeh and George Kesidis, the process works by having perimeter routers place identifying data on messages, much like a postmark on conventional mail. Kesidis, an associate professor of electrical engineering, explains that header information could be put in obsolete blocks that are rarely used.

When there's not enough space in the header, the technique divides up perimeter routers' 32-bit addresses with "a clever way of hashing," Kesidis says. When this method is used, it's possible to get router information from even a small number of packets. The data can be assembled in

real time, so attacks can be detected and blocked quickly. Additionally, he explains, because the router will apply the header information as it handles messages, there's no way to spoof router addresses or otherwise enter phony information.

Any tracing process immediately raises privacy concerns. However, because the digital postmark doesn't identify individuals, only regions, this might not be a big issue. "We're really only clawing back privacy in the same way that postmarks reduce privacy on regular mail," Kesidis says.

Kesidis notes that the technique also requires efficiency. "We need a lot of accuracy," he says. "We can't have false positives. They would take time and would bar legitimate users from accessing a site." The researchers at Penn State predict the technique will return less than one percent of false positives for every 1,000 attacking addresses.

Although Kesidis feels the technique is ready for commercial deployment, he's not sure what group would drive the digital postmark's use. Government agencies might help, and institutions concerned that they could be liable for attacks that they help transmit might also promote adoption.

CONCLUSION

The vendors that dominate the field aren't expected to push the idea, as they might view it as something that costs money without bringing in additional revenue. "Support won't come from vendors like Microsoft, Cisco, or Jupiter," Kesidis says.