



PROCESSOR
Products, News & Information Data Centers Can Trust

Sign Up For A
FREE SUBSCRIPTION! >>>>

Home | Register | Contact Us



CASH FOR COMPUTERS

- Desktops
- Servers
- Laptops
- LCDs
- Printers
- Storage

Contact: Joe Prochelo
(714) 939-2376
jprochelo@insightinvestments.com
www.desktopremoval.com

This Week's Issue

Browse All Issues

Search All Articles

Product News & Information

Company
News & Information

General Feature Articles

News

Opinions

Case Study



General Information

October 23, 2009 • Vol.31 Issue 26
Page(s) 28 in print issue

Keep Connecting

AEP Keyper Helps ICANN Address Vulnerabilities



During the summer of 2008, Dan Kaminsky discovered a serious vulnerability in the domain name system that lets attackers redirect network clients to alternate servers. Aptly coined the Kaminsky Attack, this flaw allows cyber miscreants to do such tasks as reassign Web addresses, reroute email, reset passwords, transfer money out of bank accounts, or just scramble the whole system.

ICANN, or the Internet Corporation for Assigned Names and Numbers, is an international not-for-profit organization that coordinates the DNS (domain name system) that maps host names such as www.Processor.com to IP addresses. In other words, ICANN ensures that Internet users can connect to Internet servers.

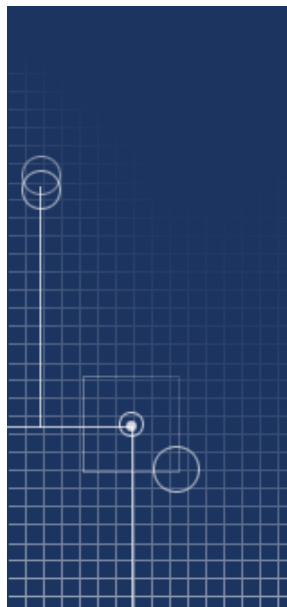
■ The Challenges

“Events over the last year, such as the Kaminsky attacks, have helped the nascent technology of DNS Security Extensions (DNSSEC) reach critical mass and remove many barriers to deployment . . . even at the DNS root,” says Richard Lamb, DNSSEC program manager at ICANN. “Often missed by technologists and politicians is the effect the world’s only cross-organizational/transnational source of authentication will have on combating the inherently global nature of cybercrime. Solution providers will now, at least, have a way to bootstrap trust when trying to identify friend or foe.”

According to Lamb, ICANN needed a product to generate, store, and sign keys for the root of the DNS. The company also needed a FIPS 140-2 Level 4-validated product to achieve the highest level of security in deploying DNSSEC at the root using an open-standards-based product.

AEP Networks (www.aepnetworks.com), headquartered in Somerset, N.J., had the solution ICANN needed: AEP Keyper Professional, the only network-attached HSM (hardware security module) that’s certified to FIPS 140-2 Level 4, the highest FIPS accreditation. Most competing HSMs are FIPS 140-2 Level 3 certified.

According to AEP Product Manager David Miller, the primary difference between FIPS Level 3 and Level 4 is the way both handle tampering. FIPS Level 3 HSMs have a tamper-evident label that says “do not open.” FIPS Level 4 HSMs automatically destroy keys in response to a tamper attempt, which significantly reduces the possibility of key compromise.



■ How It Works

Recently discovered vulnerabilities in the global DNS system have created a new urgency for the DNSSEC initiative, explains Miller. In its current form, it's possible for criminals to use the DNS to masquerade as trustworthy online entities by using a technique known as DNS cache poisoning. DNSSEC has become widely recognized as not only the solution to such forms of attack, but a way to provide additional security-in-depth for the Internet.

DNSSEC uses public key cryptography to digitally sign DNS messages, continues Miller. Responses to DNS queries are digitally signed by the DNS server using private keys, and then they are automatically verified by the client using the corresponding public key. Digital signing guarantees the validity of DNS responses. This protects Internet users from fraudulent DNS responses.

"The digital keys are generated and stored in a hardware security module (HSM). In addition to key generation and storage, HSMs provide fast cryptographic processing, which offloads computationally intensive calculations from servers," says Miller.

According to Miller, AEP Keyper offers generation, storage, usage, and management of cryptographic key material, which is contained in a FIPS 140-2 Level 4-certified crypto module, or ACCE (Advanced Configurable Cryptographic Environment), to guarantee the safety and integrity of critical key material. Each Keyper provides load-balanced, fail-safe, network-accessible cryptographic services, including random seed-based key generation, signing, and encryption, within an automatic tamper-reactive boundary.

AEP Keyper is ideal for companies that require secure key management, including Web servers, smart card issuers, and certification and registration authorities. Keyper is specifically designed for high-security and high-availability applications, Miller says, and enhances PKI security in any PKCS#11 or Microsoft Crypto API-compliant environment.

■ Problem Solved

According to Lamb, the Internet community has been pressing for the root of the DNS to get signed in order to improve security on the Internet by helping solve the DNS cache poisoning problem. AEP Keyper Pro provided the solution. "The Keyper made it easy for us to satisfy this demand in a timely and unquestionably secure manner by making such a high security device accessible to DNS programmers and developers," says Lamb.

"We have three to four AEP Keyper Pros and have been using them since July 2007," says Lamb. Although Lamb says AEP Keyper is the only FIPS 140-2 Level 4-validated standalone networked product on the commercial market, ICANN chose AEP primarily because of its excellent technical support.

"Sophisticated specialized products like this have a sharp learning curve for those who wish to integrate such security into their systems," Lamb says. "The AEP staff not only provided coding samples but then went on, recognizing the nascent DNSSEC market, to educate and familiarize this new segment of the population on HSM, standards, and how to use them."

AEP Keyper also has a proven track record and is available in a standalone configuration, Lamb says, plus it's PKCS#11-compliant and very stable.

"Implementation went better than expected," says Lamb, with no formal training required. AEP sent loaners for software development, and the product's adherence to a standards-based PKCS#11 interface simplified programming, he notes. The learning curve was only two months, "but I do not consider this a prolonged learning curve for starting from scratch," he adds. "The willingness of AEP to provide email and phone access to its engineering staff short-circuited any long development cycle. There were no negative results."

In the near term, ICANN plans to create mirror backup sites that will also be equipped with multiple Keyperes. "However, if other products with the same high bar hit the market, we will have to include those, as well, for technical diversity, as part of good engineering practice. But yes, we will continue to use the Keyper," Lamb says. ■

by Julie Sartain

AEP Networks Keyper Professional

A state-of-the-art hardware security module that offers generation, storage, usage, and management of cryptographic key material, which is contained in a FIPS 140-2 Level 4-certified crypto module to guarantee the safety and integrity of critical key material.

“The Keyper made it easy for us to satisfy this demand [for improved Internet security] in a timely and unquestionably secure manner by making such a high-security device accessible to DNS programmers and developers,” says Richard Lamb, DNS Security Extensions program manager at ICANN.

(732) 652-5200
www.aepnetworks.com

Share This Article:



[Return to Previous Page](#)

An advertisement banner for PDUdirect. On the left is a close-up photo of a woman's face. The background shows server racks in a data center. The text reads: "Outfitting a Data Center? We have an economical power solution for you." The PDUdirect logo is on the right, with the website URL www.pdudirect.com below it.

Outfitting a Data Center?
We have an economical power solution for you.

PDUdirect
www.pdudirect.com

[Home](#) [Copyright & Legal Notice](#) [Privacy Policy](#) [Site Map](#) [Contact Us](#)

Search results delivered by the Troika[®] system.

Copyright © by Sandhills Publishing Company 2009. All rights reserved.