Case Study: **The ICANN Story**

Protecting the root of the Internet

Challenge:

In order to bolster DNS security, and contribute to Internet security as a whole, the Internet community developed a new technology called DNS Security Extensions (DNSSEC). Technologists and the Internet community believe DNSSEC will augment DNS over the coming years. In its current form, it is possible for fraudsters to use the DNS to masquerade as trustworthy online entities by using what is called DNS cache poisoning. Since the first DNSSEC deployments in 2006, it has become widely recognized as not only the solution to such forms of attack but may also provide additional security-in-depth for the Internet as a whole in conjunction with other security measures.

Summary

Challenges

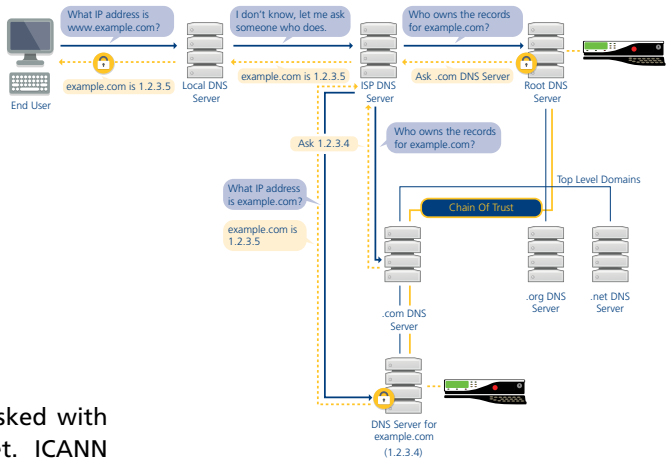
- With DNS in its current form it is possible for fraudsters to use the DNS to masquerade as trustworthy online entities by using what is called DNS cache poisoning.

Solution

- Ultra Safe Keyper HSM, the only network attached HSM on the market certified to FIPS 140-2 Level 4, the highest FIPS accreditation.

Benefits

- Keyper destroys keys if tampered
- Keyper runs an embedded operating system and delivers unmatched operational stability and reliability
- Keyper's load balancing architecture scales to work with the most complex and demanding implementations
- Keyper is simple to deploy and manage, and can be used to completely automate the key generation and rollover process.



Background

There's a lot at stake when you're tasked with securing and stabilizing the Internet. ICANN - or the Internet Corporation for Assigned Names and Numbers - plays a critical role in all online activity. The international not-for-profit organization coordinates the Domain Name System (DNS), which maps host names like www.amazon.com to IP addresses. In other words, ICANN makes sure that every Internet user can connect to every Internet server. It's an important job that ICANN takes very seriously.

DNSSEC uses public key cryptography to digitally sign DNS data. Here's how it works: responses to DNS queries are digitally signed by the DNS server using private keys and are automatically verified by the client using the corresponding public key.

Digital signing guarantees the validity of DNS responses. What's the result? Internet users are protected from the fraudulent DNS responses that could contribute to phishing techniques and other forms of fraud. Digital keys are generated and stored in a Hardware Security Module (HSM). In addition to highly secure key generation and storage, HSMs provide fast cryptographic processing, which offloads computationally intensive calculations from servers.

When Security and Reliability Matter

When it comes to protecting key management and storage, security is the top ICANN priority. The FIPS certification program, developed by the US Dept. of Commerce, certifies cryptographic products.

AEP Keyper is the only network-attached HSM on the market certified to FIPS 140-2 Level 4, the highest FIPS accreditation. Most competing HSMs are FIPS 140 - Level 3 certified.

Making the choice: Why the AEP Keyper HSM?

ICANN built its first DNSSEC deployment testbed in 2007 using a hardware security module (HSM) from AEP.

Richard Lamb was responsible for implementing DNSSEC at ICANN. After evaluating various HSMs, he opted for AEP Keyper because it provides the highest security level, exceptional support and easy maintenance.

AEP | Ultra ELECTRONICS

Benefits

The key difference between FIPS Level 3 and Level 4 is this: Level 3 HSMs have a tamper-evident label that says "do not open", while Level 4 HSMs automatically destroy keys in response to a tamper attempt. Level 4 devices significantly reduce the possibility of key compromise. "Security is a critical factor for ICANN's DNSSEC deployment, so Keyper and FIPS Level 4 was an easy choice," said Lamb.

Security without reliability is pointless. Competing HSMs run on general-purpose hardware with a standard operating system. Alternately, Keyper is a sealed, designed-for-purpose unit with no moving parts. It runs an embedded operating system and delivers unmatched operational stability and reliability.

Exceptional Support

Another of Lamb's core requirements was access to top-notch engineering support. He needed to be sure before deploying an HSM that ICANN completely understood how the technology worked, AEP happily obliged.

"Many people in the Internet community don't know a lot about cryptographic devices," said Lamb. "AEP showed a real willingness to work with this new DNS market and made it easy for us to get up-to- speed quickly."

Support contributions from AEP included advice on security policy, architectural guidance, and providing sample PKCS#11 code that Lamb could modify to meet his requirements.

In addition AEP now also offers a turnkey virtual DNSSEC solution for businesses requiring an enhanced solution to DNS Security

Simple Maintenance

Hands-off maintenance reinforced ICANN's purchasing decision. Though Lamb evaluated a competitor's product that was priced lower than AEP Keyper, he passed on it because, "it was clunky to operate and maintain." Keyper is simple to deploy and manage, and can be used to completely automate the key generation and rollover process.

Secure Multi-Site Load Balancing

Keyper's load balancing architecture scales to work with the most complex and demanding implementations. Plus, additional units can be easily added to provide linear scalability. Keyper units can be installed in any location for multi-site geographical load balancing with secure key distribution, even over unsecured networks.

ICANN

"DNSSEC incorporates a chain of trust into the DNS hierarchy. Secure key generation and storage is a fundamental element in that chain."

Richard Lamb, ICANN

Future of DNSSEC and the Internet

DNSSEC may be poised to help protect the internet, but implementations are just beginning to roll out.

"The Internet community is testing the waters when it comes to DNSSEC and the best way to deploy it," said Lamb. "Many are looking for a turnkey solution and don't have big budgets to do it."

The adoption of DNSSEC deployments is slow, in part, because cryptography standards can be complicated to grasp and implement. Lamb believes by partitioning security properly - as he's done with AEP Keyper, you can reduce complexity and improve security at the same time, making DNSSEC easier to deploy.

About Ultra Electronics AEP

AEP, is a business unit of Ultra Electronics with a high degree of operational autonomy where local management teams are empowered to devise and implement competitive strategies that reflect their expertise in their specific niches.

AEP are experts in cyber security and are also one of the UK's leading enablers of cyber security solutions. The company operates at the very forefront of technological advances with products that are approved and certified at the highest levels, thus providing protection for even the most sensitive of data.

AEP delivers its products and services via managed service providers and channel partners covering almost every industry sector for both domestic and international markets.

Made in Britain

ISOQAR REGISTERED UKAS MANAGEMENT SYSTEMS 0026

ISO 27001

Ultra ELECTRONICS

Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater, Buckinghamshire
HP10 9UT, England

Tel: +44 1628 642 600
Email: marketing@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com