CrypTech

Building Transparency into Cryptography

Enterprise Public Key Infrastructure (PKI) use has grown dramatically, and so has the requirement to protect this critical part of enterprise infrastructure. The CrypTech project is designing tools to reduce the cost and increase the trust associated with building secure and scalable PKI.

A decade ago, an enterprise might have needed a few digital certificates each year for internal websites or a few certificates each week as new systems were and new employees were added. Today, Internet architects are calling for encryption to become the default mode of operation for all Internet traffic, and many websites have responded by making encryption the default. DNSSEC is being rapidly deployed across the Internet. More than 50% of all Internet email is encrypted in transit. PKI use has skyrocketed, and some enterprises use their internal PKI and certification authorities (CAs) hundreds of times each day. PKI has changed from a curiosity to a critical infrastructure service.

The most rigorous PKI designs call for hardware security modules (HSMs) to secure valuable key material. By protecting private keys and adhering to standardized cryptographic interfaces, HSMs reduce the risks of PKI operation by increasing the confidentiality, integrity, and availability of enterprise PKI without changing basic operating models. Simply put, if PKI is a critical infrastructure service for the enterprise, HSMs provide the type of security appropriate for this type of service.

Although HSMs have been around for years, and security professionals agree on their benefits, they are not commonly deployed primarily for the following three reasons:

- **Cost.** HSMs are expensive. A full deployment, including high availability, can cost from $50,000 to $100,000.
- **Creeping requirements.** Because PKI has slowly increased in importance, many security officers have not actively reevaluated the need for the higher security provided by HSM in their enterprise PKI.
- **Trust.** The HSM marketplace is specialized. It's dominated by a small number of vendors and no open source alternative. Security experts suggest that the cryptographic product chain is open to corruption, and an open source alternative can mitigate this risk.

The CrypTech project, an independent international development effort, was founded to create a trusted, open source, inexpensive hardware cryptographic engine. The first output from CrypTech will be a trusted reference design for a HSM that can be used as the basis for commercial products, CrypTech supports the Internet community by providing an open and auditable alternative to existing crypto devices.

CrypTech is starting from the beginning. It is reimplementing a wide variety of cryptographic algorithms for loading into a specialized Field Programmable Gate Array, designing the hardware required for a true random number generator, building high-assurance auditing and management tools for key and cryptographic operations, and writing support software to link the CrypTech HSM to existing PKI products.

By moving the R&D associated with hardware PKI to the Internet community, CrypTech can dramatically reduce costs, which enables enterprises to make much greater use of cryptographic hardware, thereby increasing overall security compared to software-based key management.

What Is a Hardware Security Module?

An HSM is a specialized device that is used to securely store the public/private key pairs used with digital certificates. An HSM provides significant additional security for enterprise PKI and CAs, because it removes the need—and the risk—of storing keys on disks or in memory.

When an HSM safeguards the private key, it must also be able to perform cryptographic operations with those keys. For example, when a CA needs to sign a digital certificate, it sends the information to the HSM and requests that the HSM create the digital signature. The HSM signs the certificate, and sends back the result.

By storing keys out of reach of any application, they are never exposed outside of the HSM and cannot be stolen, because they cannot be retrieved from the HSM. HSMs implement a combination of storage, cryptographic, and auditing functions, including:

- Key storage, backup, and management, including hardware tamper resistance
- Accelerated cryptographic processing, including common hash and encryption algorithms
- A true random number generator
- System management and integrity, including logging, authentication, and auditing

CrypTech: Building The First Transparent High-Assurance Cryptographic Device

One of the driving forces for the CrypTech project is a desire for an extremely diverse engineering group. This will help increase trust in the project by making it clear that no single country or sponsor has influenced or affected the design. The current team includes members from Russia, the United States, Japan, Germany, and Sweden. Together, they are implementing every major cryptographic algorithm, designing an inexpensive hardware platform to run this software, and putting together the tools to let large companies and manufacturers make their trusted HSMs for high-assurance applications at reasonable costs. CrypTech is developing in the most transparent way possible, and encourages outsiders to review their software and designs and to test their subsystems, to provide feedback on potential problems and weaknesses. A "bug bounty" program is also being planned.

Hardware Makes It Better … and Harder

Building a hardware cryptographic engine at the heart of the CrypTech HSM is significantly more complicated than writing open source software. Because the project must integrate both hardware and software components, there are also real materials which most open source projects don't incur. For example, HSMs should be tamper proof so that if the HSM falls into the wrong hands, the device won't release the keying material even under physical attack.

The CrypTech HSM includes a true random number generator, which requires some specialized hardware components to be a source of "randomness." Cryptographers have always been critical of algorithmic methods of generating random numbers, and poorly written random number algorithms have been critical factors in security failures. A true random number generator is an important building block in a secure cryptography infrastructure.

The most significant hardware component in the CrypTech project is the use of an FPGA for crucial cryptographic functions. When an encryption or hash algorithm is written in software and built into a general-purpose CPU, or loaded into a general-purpose computer, such as a Windows or Linux system, it remains very vulnerable to attack. Software can be changed, often very subtly. Memory contents can be read during operations. Even the length of time to perform operations can be measured and reveal information. However, when the cryptography is performed in a dedicated hardware device, completely inaccessible to the normal operating system, these weaknesses are reduced significantly.

Community Support for CrypTech

Open source has been one of the major success stories of the Internet, and open source software is part of every piece of hardware and software being produced today. The CrypTech project is no different: by bringing an open source philosophy to cryptographic software and hardware, we hope to increase trust and transparency, offer alternatives to commercial products, and reduce costs. CrypTech needs your support and invites you to visit https://cryptech.is/funding/ to help fund this important effort.

How Valuable Is That Private Key?

Few CISOs bother to ask themselves, "what's the single most valuable piece of data in my network?" If they did, most would answer, "the enterprise administrator passwords." After all, if someone gets those passwords, then they can do anything they want with the network and data assets.

But that's not the most valuable thing. After all, if a password is compromised, it can be changed in seconds. Imagine something even more powerful than the enterprise administrator—and if you lose that password, there is no easy way to change it quickly without a massive disruption to service. How valuable is that? And what are you going to do to protect it?

We're talking about the digital certificate and private key of the enterprise root Certification Authority, the core of every PKI. If the corporate PKI is compromised, an attacker can do almost anything. Impersonate internal web sites. Log onto Windows systems. Connect to VPN servers as any user they want. Break into enterprise wireless. Sign malware so that it is trusted by every computer in the enterprise. The list goes on. Compromising enterprise PKI is a short cut to compromising the enterprise.

CrypTech
https://cryptech.is

[1]DNS Security Extensions, commonly known as DNSSEC, provide a way to ensure that users are communicating with the requested website or service. DNSSEC provides a level of additional security where a web browser can check that the DNS information is correct and, for example, was not modified by an attacker to instead redirect the user to a phishing site. See http://www.internetsociety.org/deploy360/dnssec/basics/ for more information on DNSSEC.

[2]A Google Transparency Report indicates that 56% of incoming mail sent to Google's Gmail service is encrypted. Outbound from Gmail, 82% of providers accept encrypted email. See http://www.google.com/transparencyreport/saferemail/.

[3]CrypTech's first use case is for HSMs. However, there are other applications for this type of technology. The CrypTech development model is based on a "composable" system that enables the designer to select the bare minimum of components needed, thereby further reducing the risk and attack surface of a CrypTech-based device.