CrypTech 2016

End of Year Report

The CrypTech project was originally formed in response to the Snowden revelations of mass surveillance and to indications that the hardware implementations of key cryptographic algorithms and functions have been systematically targeted in an effort to weaken and subvert their utility. The goal of the project was to create an open source design for a hardware cryptographic engine or Hardware Security Modules (HSMs) and an associated reference implementation that allows anyone to deploy and audit a secure, low-cost cryptographic engine in their environments.

The vision of CrypTech is that key security infrastructure, like DNSSEC, RPKI, TOR Consensus, PGP, Let's Encrypt CA, etc. should not have to depend on closed HSM products that not only cannot be audited but where there is real possible cause to distrust the functions implemented in the product. Examples of this key security infrastructure include Domain Name System Security Extensions (DNSSEC), Resource Public Key Infrastructure (RPKI), TOR Consensus, Pretty Good Privacy (PGP), Identity Federations, and the Let's Encrypt Certificate Authority (CA).

To that end, the **CrypTech Mission Statement** is:

- Put hardware crypto capability in the hands of as many people as possible by
    - Making it low cost – under $1k for a real HSM
    - Allowing diverse manufacturing of HSMs by multiple vendors, anywhere, and
    - Enabling good crypto at the edge (i.e., in applications where it is out of scale and out of price range today)
- Making HSMs more trustable by
    - Facilitating diverse design and development by
        - Working in multiple diverse countries
        - Away from the DC beltway, NSA, GHCQ, Beijing, Tel Aviv, FSB
        - Utilizing a diverse testing community (US, RU, etc.) and
        - Being open source so it can be inspected

CrypTech High Level Goals

The fundamental goal of the CrypTech project is to create an open reference platform for an HSM. This includes:

- Hardware and software designs provided as source code. For hardware, FPGA Verilog code, schematics, board layout, BOM, and board stack up are provided
- Tools, documentation, and examples to allow anybody to implement (or have someone implement for them) an HSM that is tested and evaluated to establish trust in the HSM suitable for the users need

The HSM being developed supports several use cases, both in terms of functionality and performance. The HSM also provides security with a well-defined trust boundary, with support for physical tampering detection and response.

The specific functions being developed to meet these requirements are:

- A state-of-the-art random number generator
- Symmetric and asymmetric cryptographic implementations for AES, ChaCha20, RSA, GOST, and Elliptic Curve Cryptography
- Standards-based secure key wrapping and key management
- Active tamper detection with master key obliteration

The reference platform will not be sold as a commodity HSM by the CrypTech project: few will be made. Instead interested parties that need an HSM will have to assemble and manufacture their own HSMs or have a third party do the manufacturing. The open licenses used for the reference platform allow unrestricted use of the reference design, in part or in whole, including manufacturing and selling HSMs and/or other commercial, and non-commercial uses. The license used for all code and other technical artifacts is 3-clause BSD.

The open design principles mean:

- All code is open and available under open and unrestricted license
- Open, transparent, auditable, and traceable development process
- Open design that allows for customization, observation, and testability – in development as well as during operation.

The primary focus for the development is to produce a design of an HSM with better security than that of a commercial HSM. A secondary goal is to develop a trustworthy toolchain, test programs and documentation needed to implement and verify an HSM based on the reference platform. Unfortunately, the project does not currently have the resources to focus on things such as the toolchain, enclosure, usability, and commercial-grade user interfaces.

Current Technical Status

In 2016 CrypTech produced its first set of Alpha Boards, a CrypTech specific design that includes an ARM processor and an FPGA that is connected across a pair of USB devices. Applications interact with the driver code using a PKCS #11 interface. We delivered the boards to developers and supports. For the most part we recovered the costs of the boards through our delivery channel, CrowdSupply. A few boards are still available through them: https://www.crowdsupply.com/cryptech.

The alpha hardware is a 3Ux120 Eurocard board (100x120mm) with a Xilinx Artix-7 FPGA (the 200T which is pin compatible with the smaller 100T) , an STM32F4 series ARM processor, hardware for a tamper subsystem (though we do not have a tamper resistant enclosure), volatile and non-volatile key store memories. There are a pair of USB interfaces over which we communicate with the device from an external source. Applications interface with our driver code on the external source using PKCS #11.

We have implemented a number of functions as FPGA cores: AES, ChaCha; SHA-1, -2; RSA modular exponentiation; CSPRNG (with the ring oscillator entropy source and entropy mixer); the MKM interface; and GOST R 34.11-2012. ECDSA is in progress and additional elliptic curve work will be done in the nearterm.

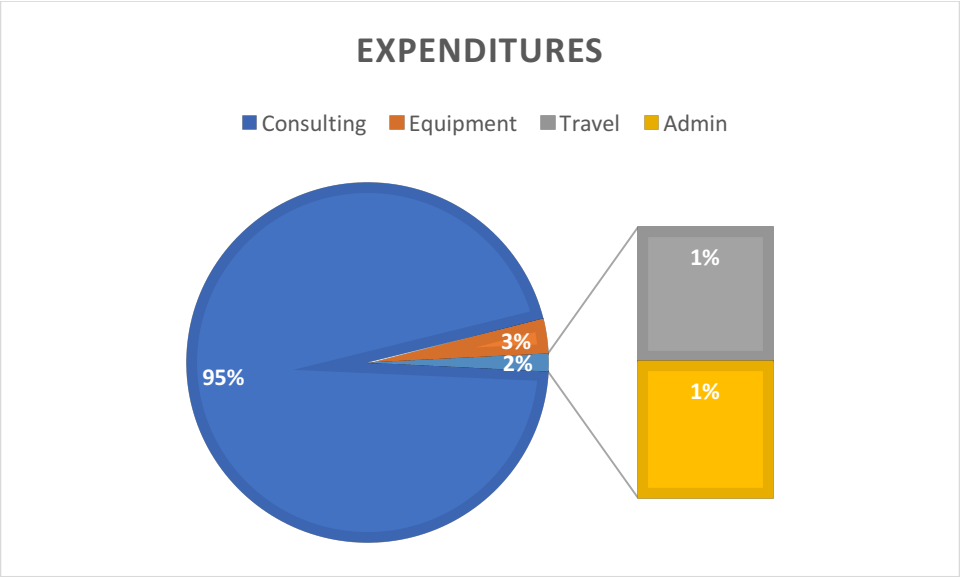
Software and firmware have been developed to manage the board, implement some functionality on the processor, and interface to the board. In addition we have used some third party software to implement some of the required functionality. Software was developed to allow an interface to Debian, Ubuntu, or OSX. All of this is available on the project Git (insert link)

We manufactured about 50 boards. Most of the boards have been delivered to developers, alpha-testers, and other interested parties. A few are still available through Crowdsupply (linked above). Development is ongoing and we expect to produce plans for the next iteration early in the New Year.

End of Year Status for 2016

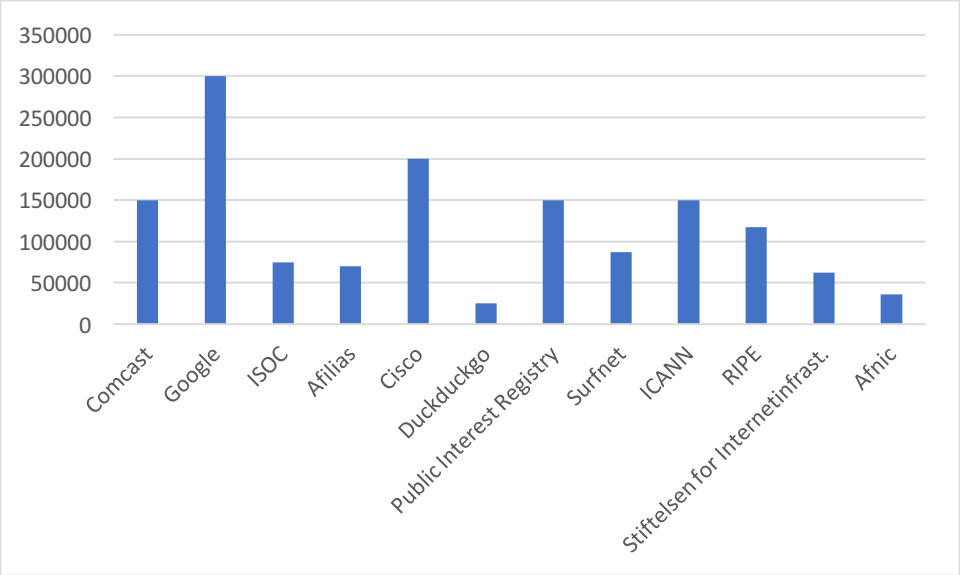
Expenditure By Type (work/expense)

The CrypTech project has spent about 95% of donated resources on engineering. In 2016 we incurred an expense for the manufacture of boards and the rest of the expenses are in travel for the few project meetings (typically combined with travel to other events to minimize travel costs for the project.



Donations

Donations to the CrypTech project are capped at $100k USD per donor per year. The graph below shows aggregated data for 2014-2016. To date donations totaled $1400k, approximately 2/3rd of the planned budget. Development could be increased significantly with additional funding. In 2015 engineers had to hold off on development due to lack of funds. That did not occur in 2016 but remains a systematic risk due to the variability of funding availability.


350000
300000
250000
200000
150000
100000
50000
0
Comcast
Google
ISOC
Afilias
Cisco
Duckduckgo
Public Interest Registry
Surfnet
ICANN
RIPE
Stiftelsen for Internetinfrast.
Afnic

2016 Goals in Review

Last year we stated a set of goals for 2016. The main focus for this year was the completion of an Alpha board. The first batch of Alpha boards were released in Jul 2016 at a workshop held in Berlin. A second set of Alphas has been produced and is being delivered through our CrowdSupply campaign (insert link). This was a significant accomplishment and demonstrates that CrypTech has delivered a working prototype, hardware and software, along the path to a real HSM product.

That list of goals is reproduced here with some brief status:

- Produce the Alpha board (done)
- More validation of the random number generator (done)
- Complete and test ECDSA in both software and hardware (in progress)
- Add curve 22519 in software and hardware
- Finish GOST hardware
- Sign and validate DNSSEC in software and hardware (done)
- Sign and validate RPKI in software and hardware
- Sign “Let’s Encrypt” CA
- Demo a “Let’s Encrypt” client with very slow TLS
- Hold workshops/hackathons to shake out use cases and usability (done)
- Prepare to help a few folk make HSM product in 2017 (see below)
- Prepare to help a few folk deploy and use applications in 2017 (see below)

2017 Goals

Our main priorities for 2017 are to complete the implementation of elliptic curve algorithms, adding documentation including user, administrator, and developer manuals, and improving the code base towards having a reference design that is close to what would be required for a commercial deployment (this includes continued focus on performance improvements and the completion of management functions such as the implementation of key sharing, key backup and restore).

In the near-term the list of work items includes:

- Improved keystore code to support larger key sizes and more storage slots
- Multi-core resource management
- Finish the Verilog ECDSA point multiplier
- Add an openssl engine
- Improve the debug log

Beyond that the list includes

- GOST drivers
- Implementation of key backup
- SHA3

- Completing documentation for user, administrator, and developer manuals
- EdDSA in Verilog (22519)

Being able to complete this work in 2017 depends of course on continued funding.

Long Term Sustainability

In 2016 we started working on plans for the long-term financial sustainability of CrypTech. CrypTech is very grateful to its existing contributors without whom CrypTech would not be where it is today. We recognize that to maintain ongoing development to deliver on the goals of the CrypTech project, we need a sustainable funding model that goes beyond the kind contributions of interested parties.

To that end, some enthusiastic contributors have constructed a plan to get CrypTech onto a long-term sustainable path. The plan is to set up a not-for-profit company, Diamond Key Security, to bring CrypTech technology to market. It intends to do this through delivering products and support directly and through interested third parties. Preliminary market research indicates there is a great opportunity for success on this path. The Internet Society has provided some initial seed money for Diamond Key Security to begin operations.

The goal of Diamond Key is the CrypTech goal stated above:
"Put hardware crypto capability in the hands of as many people as possible." We hope this entity is the agent to fulfill the goals articulated for this year of helping third-parties design and construct CrypTech-based HSM products in 2017, and deploy and use applications in 2017.

In the near-term CrypTech will continue to need financial support for ongoing development. Diamond Key Security is being structured to generate enough revenue to grow and sustain CrypTech in the future. Until that is established, we intend to devote some of the resources donated for CrypTech to sustainability: this will include activities like fundraising and developing channels for delivering CrypTech technology through third-party products. Decisions about this kind of spending will be taken by consensus for the CrypTech business team and will be reported to our funders.