CrypTech 2017

End of Year Report

The vision of CrypTech is that key Internet security infrastructure is transparent and trustworthy. This infrastructure does not have to rely exclusively on closed HSM products that not only cannot be audited and there is real possible cause to distrust the functions implemented in some of these 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 to:

- Put hardware crypto capability in the hands of as many people as possible by
    - Making it affordable – under $1k for a real HSM when produced in volume
    - 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), and
- Make HSMs more trustable through:
    - 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

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 for Hardware Security Modules (HSMs) and an associated reference implementation that allows anyone to deply and audit a secure, low-cost cryptographic engine in their environments.

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. For software, open source code and documentation is available.

- 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 currently 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, SHA, RSA, GOST, and Elliptic Curve Cryptography,
- Standards-based secure key wrapping and key management, and
- 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, and
- 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 2017, we continued to develop code on the Alpha we produced in 2016, pictured below. This Alpha 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. A pair of USB interfaces is used for communication with other devices. Applications interface with the alpha hardware using PKCS #11.

Figure 1: The CrypTech Alpha

We have implemented several functions as FPGA cores: AES, ChaCha, SHA-1, SHA-2, RSA modular exponentiation, random number generation with a 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 near-term.

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 for interfaces to Debian, Ubuntu, and MacOS. All of this is available on the project Git (https://trac.cryptech.is/wiki/GitRepositories).
Below we review our work plan and what we accomplished against that work plan.

Financial Summary for 2017

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; there was no additional manufacturing expense in 2017. The rest of the expenses were for travel covering the few project meetings. These meetings were typically combined with travel to other events to minimize travel costs for the project.

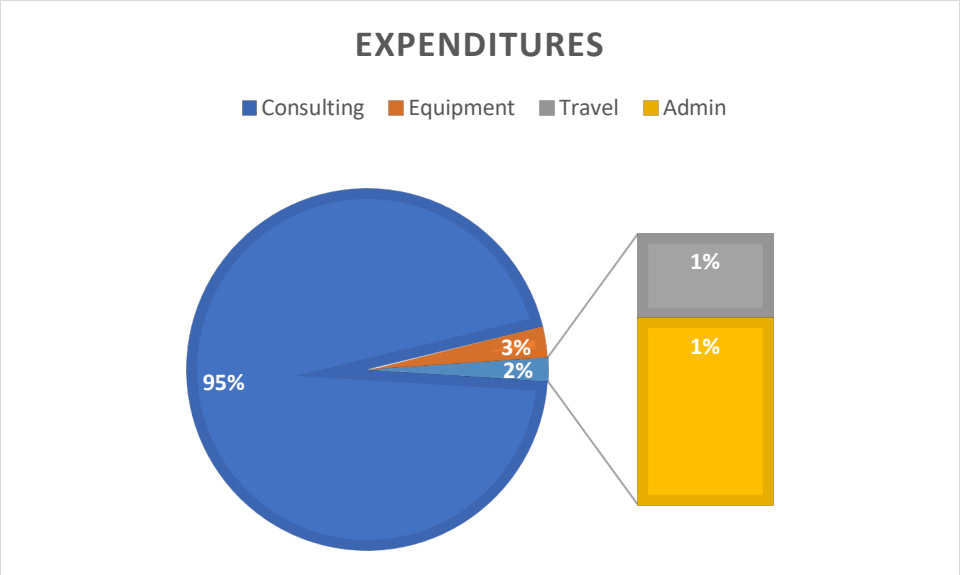

Figure 2: Expenditure By Type (2014 – 2017)

Donations

Donations to the CrypTech project are capped at $100k USD per donor per year. The graph in Figure 3 shows aggregated data for 2014-2017. Donations from the beginning of the project until the end of 2017 totaled $1666k, 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. Similar development delays did not occur in 2016 or 2017 but development delays remain a systematic risk due to the variability of funding.

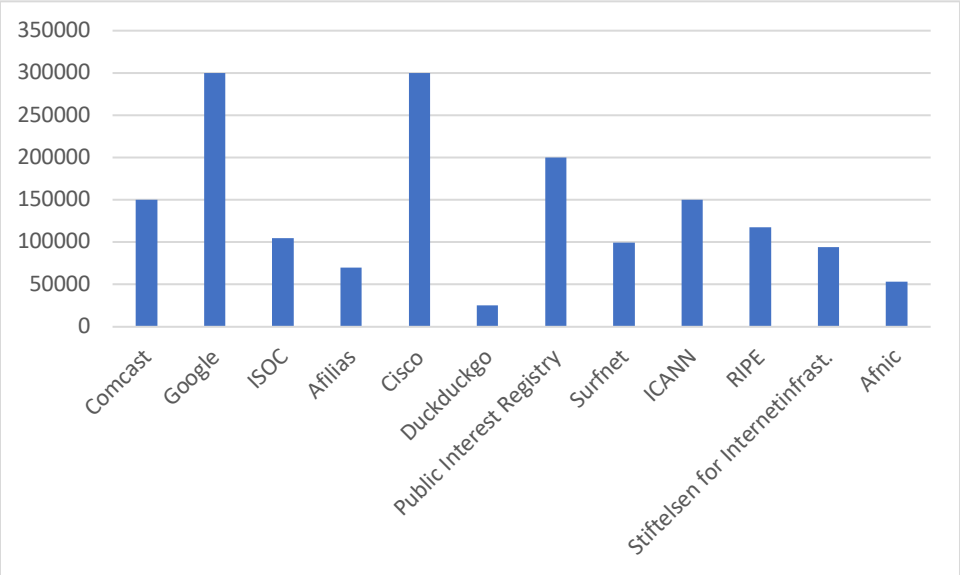

Figure 3: Donations (2014 – 2017)

2017 Goals in Review

In our end-of-year report for 2016 we stated that our main priorities for 2017 were to complete the implementation of elliptic curve algorithms, adding documentation including user, administrator, and developer manuals, and improving the code base. This was all with the objective of working towards having a reference design that is close to what would be required for a commercial deployment, including continued focus on performance improvements and the completion of management functions like key sharing, key backup and key restore. Specific work items are identified below.

The year began with a lot of work to identify and fix issues with the implementation that were discovered during testing. We released a new version of the firmware in May (version 3) that fixed these issues and implemented some of the work items below.

The early work items included:

- 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 included:

- GOST drivers
- Implementation of key backup
- SHA3
- Expanded documentation for user, administrator, and developer manuals
- Ed25519 in Verilog

In the second half of the year we focused on improving the speed and performance of the code base, and we believe a near-term optimization for the existing hardware has been reached.

Work Plan for 2018

We held a face-to-face meeting in Stockholm in September 2017 to discuss current status and next steps for the CrypTech Project. We agreed to a rough work plan for 2018 with specific work items identified by near-term, mid-term, and long-term. We identified work items for both hardware and software. In general, the major work items for next year will be the implementation of Ed25519 and hash-based signatures for quantum-resistant code signing.

In the near-term we plan both hardware and software work including:

- Convert hardware layout for use in the open source KiCad tool
- Find the source of the battery drain and fix it

- Add a programmable microcontroller with a USB interface to replace the FTDI chips
- Get external review for these changes
- Continue ongoing profiling work to identify easy improvements to performance
- Implement ECDH
- Implement Ed25519

For the mid-term we have some additional work items including:

- Add 2 GigE Ethernet interfaces (for raw Ethernet, no TCP/IP) via a daughter card
- Add a larger flash
- Make the RPC (used between the host and the Alpha) secure
- Implement hash-based signatures[1]
- Add host middleware to support multiple devices

Long term we expect to:

- Improve performance through faster hardware
- Implement X25519

All of these depend of course on sufficient funding to do the work.

CrypTech Sustainability

The long term sustainability of CrypTech has been an ongoing concern. This is a common concern for many open source projects that represent key parts of Interneet infrastructure. In 2017 some enthusiastic contributors to the CrypTech project formed a not-for-profit company in the United States called Diamond Key Security. One part of Diamond Key Security's mission is to facilitate initiatives to enhance the security and stability of the Internet through the development and deployment of open source technology and its various applications.

In line with that mission, Diamond Key Security plans to bring CrypTech technology to market by delivering products and support, both themselves and through third-parties who are interested in using the CrypTech open source base. The purpose of this is two-fold. First, support the CrypTech mission "to put hardware crypto into the hands of as many people as possible." Second, to use the revenue generated from these operations to sustain CrypTech over the long term to realize its expansive vision of a secure open source Crypto engine for a wide range of use cases. Early in 2017 the Internet Society generously provided seed money to establish Diamond Key Security and enable them to begin operations. Additionally, in late 2017 the Internet Society provided a substantial contribution to allow Diamond Key Security to hire initial staff members and take the first steps in delivering on the product and support portion of the sustainability plan.

[1] https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/

In the near-term CrypTech will continue to need financial support for ongoing development. We are grateful to the companies who have contributed so far. Diamond Key Security is being structured to generate enough revenue to grow and sustain CrypTech in the future, but this will take some time to stabilize. Until that funding is established and consistent, the CrypTech project intends 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. It is expected that these activities will constitute a relatively small percentage of overall CrypTech expenditures. Decisions about this kind of spending will be taken by consensus of the CrypTech business team and will be reported to our funders.

A Final Word

The CrypTech project would like to once again thank all of our supporters and contributors (both technical and financial) over the last four years. 2017 was a year that saw both progress and setbacks for the CrypTech project. For 2018, we see many positive signs, and we are looking forward to an excellent year. We have a solid work plan and a growing community. The CrypTech Project has an excellent relationship with Diamond Key Security, and we are excited about the direction that this exciting collaboration will enable us to move in.