CrypTech 2019

End of Year Report

Summary

Progress on the CrypTech project has slowed considerably due to a serious slow-down in funding. However, we were still able to implement several FPGA enhancements, which added up to a more than 10x improvement in RSA signing speed.

At the end of 2018, CrypTech wrapped up its time under the administrative umbrella of NorduNet and SUnet and moved to the Commons Conservancy/NLnet Foundation. 2019 was CrypTech's first full year as part of the Common's Conservancy.

Although CrypTech's first commercial user, Diamond Key Security, NFP, shipped prototypes in 2018 and was well on its way to completing a commercial offering, it was unable to get sufficient funding to ship a supported product and ended up closing its doors. Acquiring funding remains the critical issue for CrypTech to continue and advance.

Vision

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 but that there is real possible cause to distrust the functions implemented in some of these products. 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 deploy 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 reference design 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 2019, 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.

We have implemented several functions as FPGA cores: AES, ChaCha, SHA-1, SHA-2, ECDSA, Ed25519, RSA modular exponentiation, random number generation with a ring oscillator entropy source and entropy mixer, the MKM interface, and GOST R 34.11-2012.

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 2019

Organizational Home

From 2014-2018, SUNET was the host for the CrypTech project through Nordunet A/S. At the beginning of 2019 the NLnet Foundation began the professional management of CrypTech finances. Stichting NLnet is one of the oldest internet-related grantmaking organizations in the world and operates a dedicated fund for CrypTech where you can easily donate to the programme. We discussed the process for making this move in the end of year report for 2018.

The CrypTech programme also collaborates with Commons Caretakers BV, a not-for-profit company supporting sustainable development and maintenance of technology commons.

Expenditure By Type (work/expense)

The CrypTech project has spent about 97% of donated resources on engineering. In 2016, we incurred an expense for the manufacture of boards; there has been no additional manufacturing expense since then. 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. As you can see from the chart below, 97% of our expenditures have been for engineering consulting, 2% on equipment, 1% on travel, and less than ½% on administrative overhead.

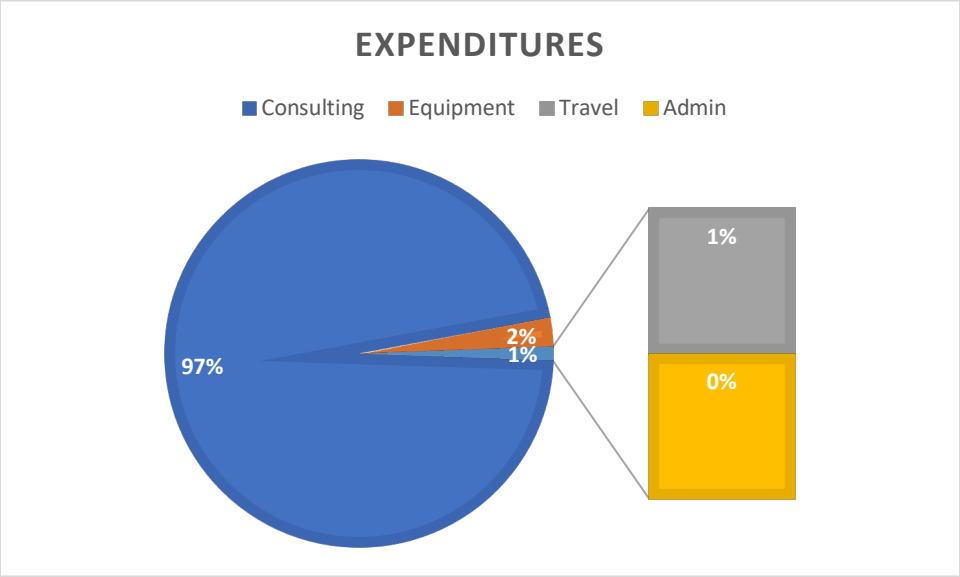

Figure 2: Expenditure By Type (2014 – 2019)

Donations

Other than in the case of openly run grant schemes, donations to the CrypTech project are capped at $100k USD per donor per year. The graph in Figure 3 shows aggregated data for 2014-2019. Donations from the beginning of the project until the end of 2019 totaled $2,014,000, 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 and in 2019 we had a significant work stoppage as funding dried up before the middle of the year.

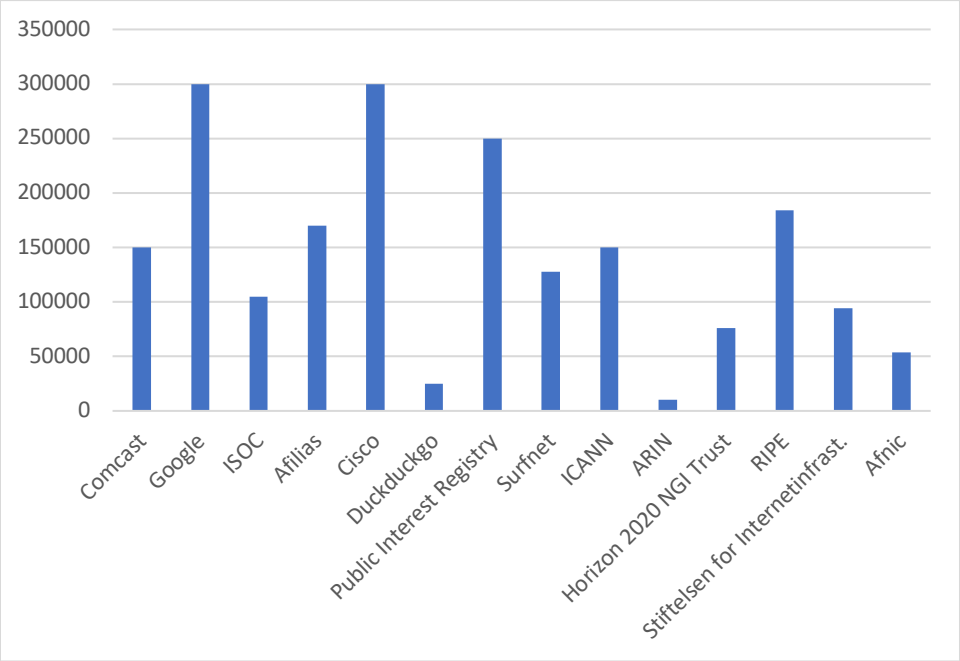

Figure 3: Donations (2014 – 2019)

The following graph illustrates how donations have come into the project by year. As you can see, the last two years have been our lowest in terms of donations coming into the project. The work stoppage in 2019 reminds us that shortage of funds is a significant risk for the project.

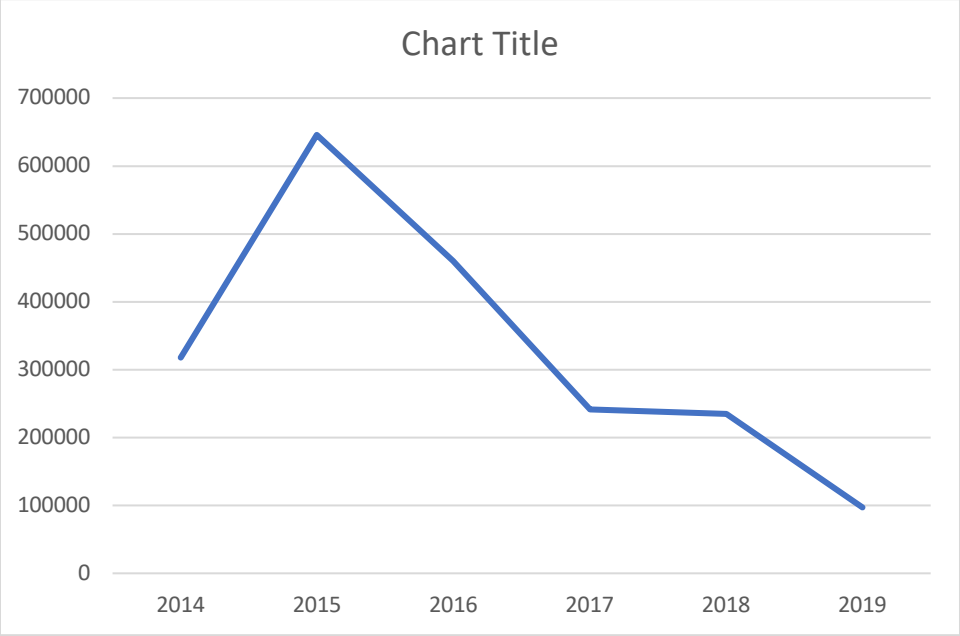

Figure 4. Donations by year (2014-2019)

Research Grant

CrypTech received a research grant as part of the EU Horizons 2020 NGI Trust Program, called CryRev. Like other grants we have received, there is a workplan for the grant and it includes completing a set group of tasks.

The goal for the project is to develop the next iteration of the CrypTech board. The main goals of this new board design are:

- Extend the openness of the design through porting it to KiCAD, and open design tool
- Enhance the security of the CrypTech design through 1) implementing the master key storage in a dedicated tiny FPGA replacing the SPI connected SRAM and the AVR MCU; this will provide tamper response with ns latency; 2) moving all key related processing and sensitive information into the FPGA
- Enhance the speed of the CrypTech design through 1) implementation a new architecture for RSA acceleration and 2) moving more processing into the FPGA including the integration of a RISC-V core that runs some software functions
- Reduce cost through the removal of some components

CrypTech would also like to thank Assured AB of Sweden for handling the administration of this grant for the CrypTech project.

2019 Goals in Review

In our last end-of-year report, we articulated a roadmap of future work that included evaluation of incorporating components that use RISC V in particular as a core on our FPGA to replace the current ARM processor on the board. We also anticipated using that in a new smaller FPGA that could function as a more secure Master Key Memory. Some preliminary investigations showed a possible substantial performance improvement, through revision of the modular exponentiation cores. In addition, we planned to complete the port of the physical designs to the KiCad open software suite for the physical design layout. The plan was to complete some preliminary investigations and reconvene to evaluate how to proceed.

Due to the funding shortage, our investigations on all but the improved modular exponentiation cores halted. A great deal of work on these cores was completed by the end of the year, and the updated code has been tested and committed to the project Git repositories. Work has begun on evaluation of RISC V cores since we resumed work at the end of the year, and the port to KiCad has been completed.

Significant developments in the FPGA include:

- Synchronous clocking for the FMC bus and the FPGA cores eliminates polling on the bus, and simplifies the design.
- A new ModExpNG ("next generation") core moves most of the RSA signing operation to the hardware.
- A new keywrap core moves most of the AES key wrap/unwrap operation to hardware.

All of these improvements, taken together, improved RSA signing speed from less than 8 sigs/sec to more than 87 sigs/sec with a 2048-bit key. Furthermore, testing has shown that building a dedicated RSA signer (without ECDSA support) can push this past 116 sigs/sec. We believe that further gains are possible without too much effort.

Commercial Partner Update

Some of the 2019 work items were picked up by Diamond Key Security for their commercial HSM built on CrypTech. The plan for adding an Ethernet interface through a daughtercard was a combination of simplicity for interfacing and the possible of adding high throughput applications. Diamond Key added an Ethernet interface through a single board computer inside their tamper resistant enclosure. This allows for easier connectivity but does not address the throughput issue. Because the host and the alphas will be communicating over this interface, it was necessary to secure communications and Diamond Key implemented this by running TLS between the host and the single board computer. This work is not revising the CrypTech RPC to make it secure natively. Also, because Diamond Key uses a pair of alphas inside their enclosure, they modified the CrypTech code to allow for multiple alphas inside a single chassis. The code for implementing these has been contributed to the CrypTech code base.

Diamond Key Security built prototypes of this device as a 1u rack-mounted tamper-resistant HSM. They shipped 6 prototype units last year, 2 each to 3 different operators. They continued to revise their prototype implementation and were on the path to have commercial offerings in 2019. Sadly, Diamond Key Security was unable to obtain sufficient funding to ship a supported commercial product and closed operations in 2019. They made all their code and designs available on GitHub (https://github.com/DiamondKeySecurity) under permissive licenses.

Work Plan for 2020

Due to the lack of funding, we have not held a face-to-face meeting since our meeting in Amsterdam in February, 2019. In the near-term, our work items are driven by the deliverables in the Horizon 2020 NGI Trust Grant. These include a draft of the CrypTech 2.0 board design, a manufacturing test run of the new boards, new cores for the v2 board (the RISC-V cores), and then software for those cores.

CrypTech Sustainability

The long-term sustainability of CrypTech remains an ongoing concern. This is a common concern for many open source projects that represent key parts of Internet infrastructure.

In the near-term CrypTech will continue to need financial support for ongoing development. We are grateful to the companies, organizations, and research entities who have contributed so far. We had hoped that Diamond Key Security would generate enough revenue to grow and sustain CrypTech in the future, but this will not materialize. 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 five years. 2019 was a year that saw significant results for CrypTech before we had to put work on hold due to funding contraints. 2020 will begin with investigations to give us a clearer idea about what might be capable within the context of the project going forward. We see many positive signs, and we are looking forward to an excellent year. We have a solid work plan and a growing community.