CrypTech 2018

End of Year Report

Summary

The CrypTech project continues to progress. In 2018 we completed the implementation of hash-based signatures, Ed25519 cores, and continued to make improvements to the performance of the device. In addition, we completed an external security audit, published the results, and implemented the corrections. 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. CrypTech's first commercial user, Diamond Key Security, NFP, shipped its first prototype HSMs incorporating the CrypTech Alpha device.

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 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 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 2018, 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 2018

Organizational Home

From 2014-2018, SUNET has been the host for the CrypTech project through Nordunet A/S. This meant that Nordunet A/S collected all of the donations, paid the developers, reimbursed expenses, kept the books, held the copyright on the source code, and handled other administrative overhead for the project as needed. When the project began to get organized in early 2014, Nordunet agreed to handle this for CrypTech for the "first three years or so." They ended up taking care of this for 5 years. For all of this effort, the CrypTech project is very grateful.

Over the previous 15 months CrypTech evaluated alternate candidates for an organizational home. CrypTech has chosen the Commons Conservancy to be our new organizational home. CrypTech is now an active programme of The Commons Conservancy, a pro bono legal umbrella established in 2016 in Amsterdam to promote and support technology commons, and with the mission to enable human innovation at the widest possible scale. The Commons Conservancy is a "stichting" according to Netherlands law, and acts as the moral and legal steward of all intangible assets of CrypTech as well as a number of other programmes such as FileSender, Let's Connect and IdentityPython; the foundation is statutorily and irrevocably barred from any financial involvement with any of the programmes.

CrypTech finances are professionally managed by NLnet Foundation, a recognised public benefit organisation (ANBI). NLnet's history started in April 1982 with the announcement by Teus Hagen as chairman of a major initiative by the EUUG to develop and provide network services in Europe under the name EUnet. NLnet was one of the founders of AMS-ix (the oldest European internet exchange) and the .nl registry SIDN. Stichting NLnet is one of the oldest internet-related grantmaking organisations in the world, and operates a dedicated fund for CrypTech where you can easily donate to the programme.

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 95% of donated resources on engineering. In 2016, we incurred an expense for the manufacture of boards; there has been no additional manufacturing expense in 2017 or 2018. 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.

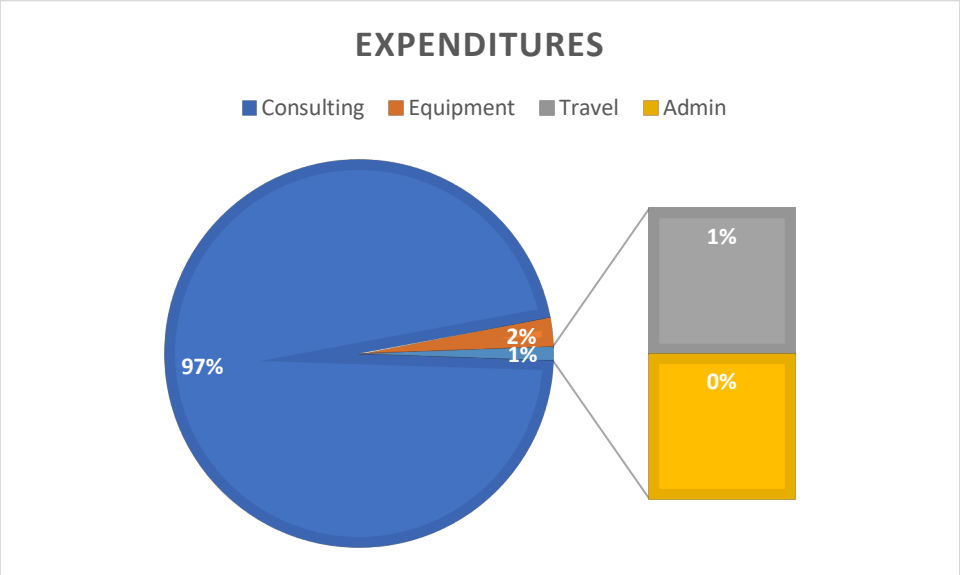

Figure 2: Expenditure By Type (2014 – 2018)

Donations

Donations to the CrypTech project are capped at $100k USD per donor per year. The graph in Figure 3 shows aggregated data for 2014-2018. Donations from the beginning of the project until the end of 2018 totaled $1,900,000, 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. Similar development delays have not occurred since but development delays remain a systematic risk due to the variability of funding.

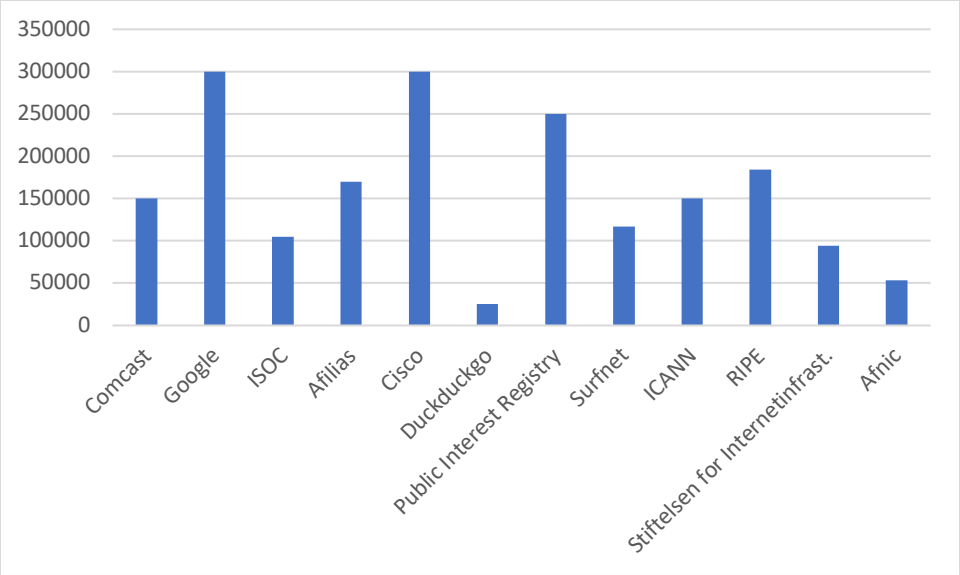

Figure 3: Donations (2014 – 2018)

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. Although CrypTech has only once been forced to stop work due to lack of funds, it remains a systemic risk to the project.

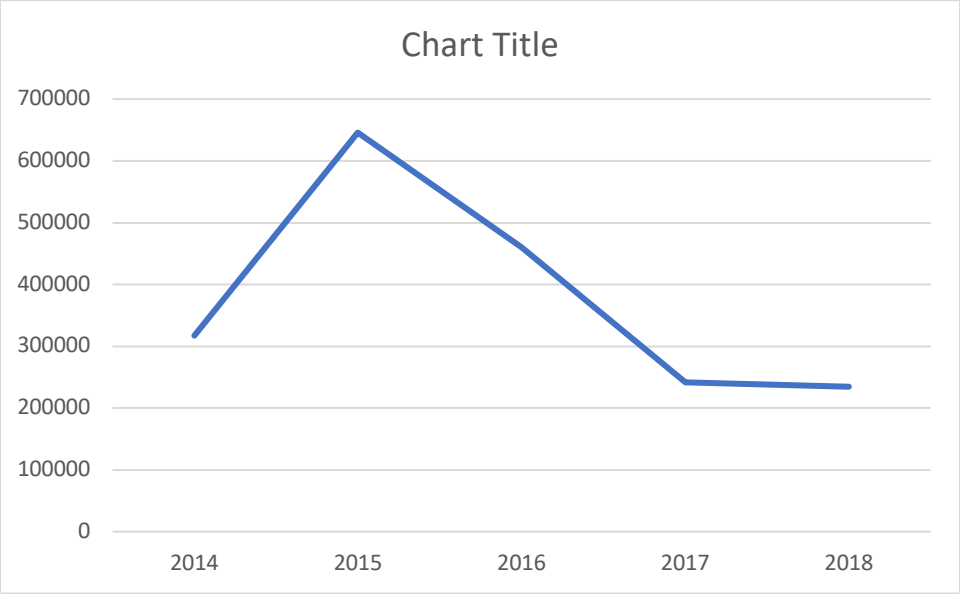

Figure 4. Donations by year (2014-2018)

2018 Goals in Review

In our last end-of-year report, we articulated a roadmap of future work that included performance improvements, implementation of hash-based signatures, and implementation of Ed25519. There were additional items around hardware improvement, such as adding Ethernet interfaces (but not TCP/IP) with a daughtercard, securing the RPC between the host and the alpha, and adding middleware to support multiple alphas inside a single chassis.

We completed the implementation of hash-based signatures and that is now part of the standard CrypTech code release. We posted details of this on our blog (https://cryptech.is/2019/02/cryptech-implements-hash-based-signatures/). The work on Ed25519 has progressed well and is nearing completion. A fair amount of effort has been spent on performance improvement, specifically performance of RSA key signing. Work remains to be done here – the work would benefit from detailed profiling and concentrated effort to find performance bottlenecks. In addition, we added a hardware implementation of AES Key Wrap (RFC 5649) allowing us to wrap and unwrap big objects with high performance.

External Security Audit

Diamond Key Security sponsored an external audit of the CrypTech code base. Cure53 performed the audit during the summer. The results were published on the website here: https://cryptech.is/2018/10/external-security-audit-completed/. There were 5 identified vulnerabilities and 4 miscellaneous issues. All of the identified vulnerabilities except CT-01-008 MCU have been addressed and the code has been updated. CT-01-008 has a long term of solution of implementing a secure channel for CrypTech communications. This is on our roadmap. (Diamond Key Security has reported that in their implementation of an HSM using the CrypTech alphas, this does not remain a vulnerability because of the implementation of communication between the host and the HSM.)

Commercial Partner Update

Some of the 2018 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 will be 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 continue to revise their prototype implementation and expect to have commercial offerings based on this

sometime around mid-year 2019. Diamond Key Security is a US-based not-for-profit entity with a broad mission which includes "conducting scientific research in the development, enhancement and deployment of transparent, auditable cryptographic technologies to help safeguard the Internet for the public good, educating the general public concerning cryptographic technology, facilitating initiatives to enhance the security and stability of the Internet, encouraging the effective use of cryptographic technologies in educational and other nonprofit organizations, and making reliable cryptographic security technologies widely available."

Work Plan for 2019

We held a face-to-face meeting in Amsterdam in February, 2019. This meeting was a follow-up to a face-to-face in Stockholm last September. In September, there was still a lot of uncertainty about potential needs of a next iteration of CrypTech development. More clarity has been achieved since then with some concrete steps to take in 2019. For the past year or so we have been considering whether it is time to produce a new iteration of hardware. Our goals in doing such an iteration of hardware would broadly include increasing performance, in particular for RSA signing applications, and improving the overall security of the device. A few specific ideas have percolated up, including replacing the master key memory with an FPGA-based implementation and replacing the separate ARM processor with a processor core inside the FPGA.

We enumerated a list of things to do and chose to work hard on a couple of them in the next couple of months, then share results and make decisions about how to proceed for the rest of the year.

The first area of investigation will be around prototyping the use of a RISC-V core inside the FPGA to replace the ARM processor we currently use. There are a number of implementation details to work out but this work could demonstrate that we might have a reasonable alternative to our existing processor. We expect this prototyping effort to be complete in Q2. Success in implementing this would allow us to increase the openness of our design, simplify auditing, and more tightly couple the processing with the accelerator cores – improving both performance and security.

The second area of investigation involves some promising directions in improving the implementation of modular exponentiation to improve the performance of RSA key signing operations. The early investigations into the math involved, and the corresponding implementation in an FPGA, give us some promising indications of the possibility of substantial performance improvement. This too should begin to show results in Q2.

We are also investigating the development of a first generation of a tamper responsive master key memory implemented in a low power, high integrity FPGA. The memory will provide remanence protection and rapid (ns) zeroisation of sensitive information. The FPGA used is supported by a fully open development flow (Project Icestorm: http://www.clifford.at/icestorm/) which allow an open, auditable implementation of the master key storage and protection. We also intend to investigate the

integration of a RISC-V processor core to provide intelligent control and usage of multiple types of tamper sensors such as accelerometer, light, and motion.

After these investigations are complete, the CrypTech core team plans to reconvene to discuss the appropriate next steps based on these results. Beyond this initial list we have targeted work on detailed logging, the implementation of an FPGA core for the Poly1305 algorithm, and a secure channel for communication.

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.

Last year we introduced Diamond Key Security and its goal of eventually generating enough revenue to sustain and expand the CrypTech project. They have begun shipping prototypes and expect to have a commercial product offering in the market this year. But it will take some time for that project to come to fruition and generate enough revenue to sustain both Diamond Key Security and CrypTech.

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. 2018 was a year that saw significant results for CrypTech. 2019 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. The CrypTech Project continues to have an excellent relationship with Diamond Key Security, and we are excited about the direction that this exciting collaboration will enable us to move in.