CrypTech Open Source Cryptography Project – 2019 Update

ICANN DNS Symposium
May 2019
Phil Roberts: roberts@dkey.org
Hardware Security Module

• Dedicated appliance for cryptographic operations
• Generate, protect, and store secrets (private key in PKI)
  • Protect secrets
• Offload sensitive operations from general systems
  • Crypto acceleration

• Very expensive
• Very few vendors
• National interests – strong connection to agencies
Hardware Security Module

Where Keys Go to Hide

Diamond Key Security: a safer, more open, trusted Internet
160203 CrypTech  Creative Commons: Attribution-NonCommercial-ShareAlike 2.0
Many Flavors and Sizes
CrypTech Project

• Multi-year effort to move towards an open HSM platform developed using open, auditable, and trustable tools

• Started at the suggestion of Russ Housley, Jari Arkko, and Stephen Farrell of the IETF to meet the assurance needs of supporting IETF protocols in an open and transparent manner

• Composable, e.g. “Give me a key store and a signer suitable for DNSsec”

• Reasonable assurance of being open:
  • Core team from Sweden, Russia, USA, Germany, Japan, and Ireland
  • Open development: signed commits to Git repos, etc.
CrypTech Project

• 3-clause BSD license for all SW, FPGA code
  • All cores for crypto acceleration in HW (AES, SHA-256, RSA, EC)
• Creative commons for all documents
  • PCB layouts, BOMs

• Repos accessible via trac: https://trac.cryptech.is
• Maillists: https://trac.cryptech.is/wiki/MailingLists

• Step-by-step towards an open toolchain
• Goal is to be able to do reproducible builds, traceable builds
CrypTech: Thanks to our Funders:
CrypTech Alpha Board
CrypTech Alpha Board

• ARM Cortex-M4F based main CPU (STM32F429)
• Xilinx Artix-7 T200 FPGA
• AVR 8 bit MCU for tamper protection

• PKCS#11 and management software developed by the project
• Comprehensive set of FPGA cores developed by the project
  • RSA, EC, AES, ChaCha
  • SHA-1, SHA-2, and SHA-3
  • Keywrap, TRNG
DNSsec use case

- DNSSEC signer
  - Works with OpenDNSSEC, BIND, Knot, and PowerDNS
  - Supports both RSA and EC
  - Available soon as a product offering through Diamond Key Security
CrypTech Resources

- Website: https://cryptech.is
- Wiki: https://trac.cryptech.is/wiki
- Git repositories: https://trac.cryptech.is/wiki/GitRepositories
- Mailing lists: https://trac.cryptech.is/wiki/MailingLists
- CrowdSupply for buying Alphas: https://www.crowdsupply.com/cryptech
2018 Accomplishments

• Performance Improvements
  • Revising and updating implementation to improve performance
  • Some of that work has led also to improved security (FPGA implementation of AES keywrap, for example)

• Hash-based Signatures
  • Implementation of David McGrew’s hash-based signature draft: [https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/?include_text=1](https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/?include_text=1)
  • Quantum resistant signature scheme with potential uses in signing code updates

• Ed25519
  • Edwards-curve signature algorithm
  • Crypto implementation done, working on drivers
  • Could implement x25519 without a lot of additional effort if needed
2018 Accomplishments

- External Security Code Audit
  - Completed in September of this year
  - Cure53 report is on our website: https://cryptech.is/2018/10/external-security-audit-completed/
  - No critical vulnerabilities
  - Identified vulnerabilities were fixed by year-end

The results in the cryptographic realm are outstandingly positive. Not only were there no security issues found, but also the overall design has been evaluated as excellent. This especially holds for the TRNG, which displays many strengths despite its simple architecture. The testing team is happy to report that the cryptographic aspects connected to the tested items are well under control.
Ongoing developments

• Performance Improvements
  • Totally new RSA core architecture is being developed (10x – 20x seems possible)

• Hunting latencies for FPGA – SW communication
  • Endian conversion in SW being moved to HW in the FPGA
    • We can do memcpy() now

• Improving FPGA clock speed through floorplanning
  • 100+ MHz
Ongoing developments

• Security improvements
  • Moving SW crypto processing into the FPGA
    • PKCS#11 and management still in the STM32 MCU
  • Adding DMA engine inside FPGA for core – core transfer
    • Eliminate transfer of sensitive data across the FMC bus
  • Reproducible builds for releases
    • MCU, FPGA, Tamper
Open Master Key Memory

• Develop an open MKM, implemented in a FPGA
  • Lattice iCE40 – no external config mem, very lower power consumption
  • BGA device that can be mounted on PCB back to back with main FPGA
  • Active tamper detection with ns tamper response time
  • Zeroisation of KEK with remanence/imprinting protection
• Open toolchain and auditable FPGA bitstream
• http://www.clifford.at/icestorm/
Alpha v2, Alpha NG, Beta - something

- Integrate the MCU into the FPGA – using open RISC-V cores
  - Looking at VexRisc and Western Digital Swerv cores
- Rearchitect the FPGA DMA engine to allow core-core transfers
- Integrate new RSA cores when completed
- Integrate FPGA based MKM with no exposed wires to the main FPGA.
- Integrate small RISC-V in FPGA based Master Key Memory to add tamper functionality, root of trust (PicoRV32)
Alpha v2, Alpha NG, Beta - something

• Openness Improvements
  • No proprietary MCU – RISC-V is the open future
  • Open Master Key Memory, root of trust
  • We still need use proprietary tools for the main FPGA

• Cost and size improvements
  • Remove several components (the MCU being most costly)
  • Reduce the PCB dimensions
  • Cost reduction probably used to buy FPGA with better speed grade

https://symbiflow.github.io/ - SymbiFlow - open source FPGA tooling for rapid innovation
Cryptech as an open platform

• Diamond-HSM
  • First commercial HSM based on Cryptech
  • Developed, manufactured by Diamond Key Security (DKS)
    • Founded by people from Internet orgs. Focus on Internet infrastructure, research
    • First machines delivered. Used for DNSSEC, Federated Identity Management

• TorHSM
  • Developing dedicated Tor Directory Authorities (DAs) based on the Cryptech Alpha
  • Adding PCIexpress – USB bridge
  • Board 1mm smaller to fit inside a host PC
  • Removing tamper-MCU, current FTDI interface chips, headers, power supply
  • [https://trac.cryptech.is/wiki/ExternalProjectsTorHSM](https://trac.cryptech.is/wiki/ExternalProjectsTorHSM)
• Trustworthy Hardware Security Module
  • Low cost, open-source solution utilizing two CrypTech modules for speed and redundancy
  • High entropy, True Random Number Generator (TRNG) for secure cryptography
  • Rugged, tamper-resistant housing

• 1U 19” rack-mountable network appliance with USB and Ethernet interfaces

• Two (2) embedded CrypTech modules

• PKCS#11 API implementation supporting standard applications: OpenDNSSEC, BIND, PowerDNS, KnotDNS

• Product availability 3Q2019
For the security equipment provider, desiring an open, transparently designed, cryptography engine, Diamond Key provides a CrypTech module that is an embedded open-source security engine providing complete crypto key management functionality. Unlike existing expensive solutions from untrusted, unverifiable equipment sources, the Diamond Key Security CrypTech technology has trust built-in from the start in a fully open system.