CrypTech

Building a More Assured HSM with a More Assured Tool-Chain

The Need

- Every week a new horror about Crypto/Privacy
- *der Spiegel* revelation of the "SpyMall Catalogue"
- Compromises of most network devices, servers, firewalls, ...
- We are relying on HSMs which are designed and made by government contractors
- Many people are not comfortable with this

Origins

- This effort was started at the suggestion of Russ Housley, Stephen Farrell, and Jari Arkko of the IETF, to meet the assurance needs of supporting IETF protocols in an open and transparent manner.

- But this is NOT an IETF, ISOC, … project, though both contribute. As the saying goes, we work for the Internet.

Goals

- An open-source reference design for HSMs
- Scalable, first cut in an FPGA and CPU, later allow higher speed options
- Composable "Give me a key store and signer suitable for DNSsec"
- Reasonable assurance by being open, diverse design team, and an increasingly assured tool-chain

Open and Transparent

- The project is being run in an open, transparent manner with traceability for all decisions etc.

- We do this in order to build trust in the project itself

Critical Tool-Chain

- If the compiler is trojaned, then nothing we build is at all safe
- So a controlled and reasonably assured tool-chain is critical
- See David Wheeler's solution to Ken Thompson's Turing paper *Reflections on Trusting Trust*
- The Build Environment is based on that

Minimal Organisation

- Finances at a non-profit in Sweden associated with SUNET or SE Registry
- Administration at SUNET, Maria Hall and Leif Johanssen
- Technical: cooperative of very senior folk with Randy Bush as cat herder
- Fund Raising - Russ Housley / ISOC Folk

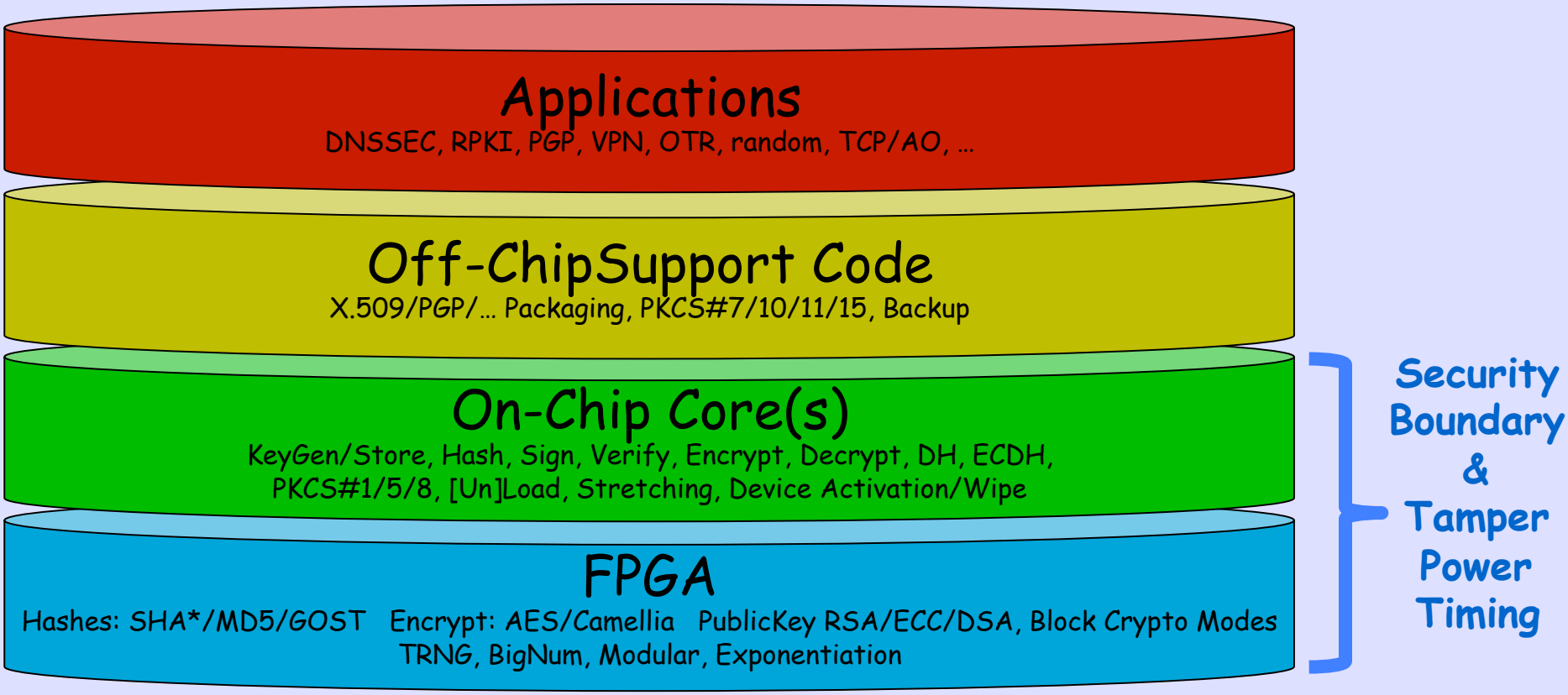
Diversity Improves Trust

- Diverse Technical Team - from diverse countries / environments
- Transparent Development - code, designs, documentation all public
- Auditable and Audited – Please help audit

Diverse Funding

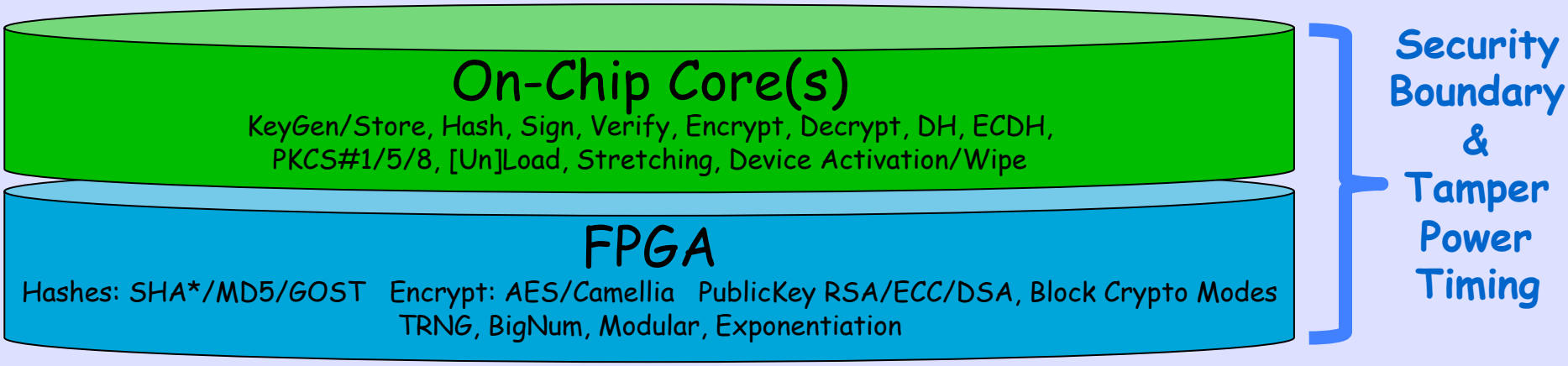
- Multinational and Multi-Stakeholder
- Industry, Academe, Social, …
- Diversity is critical, no donor > 10%

Layer Cake Model

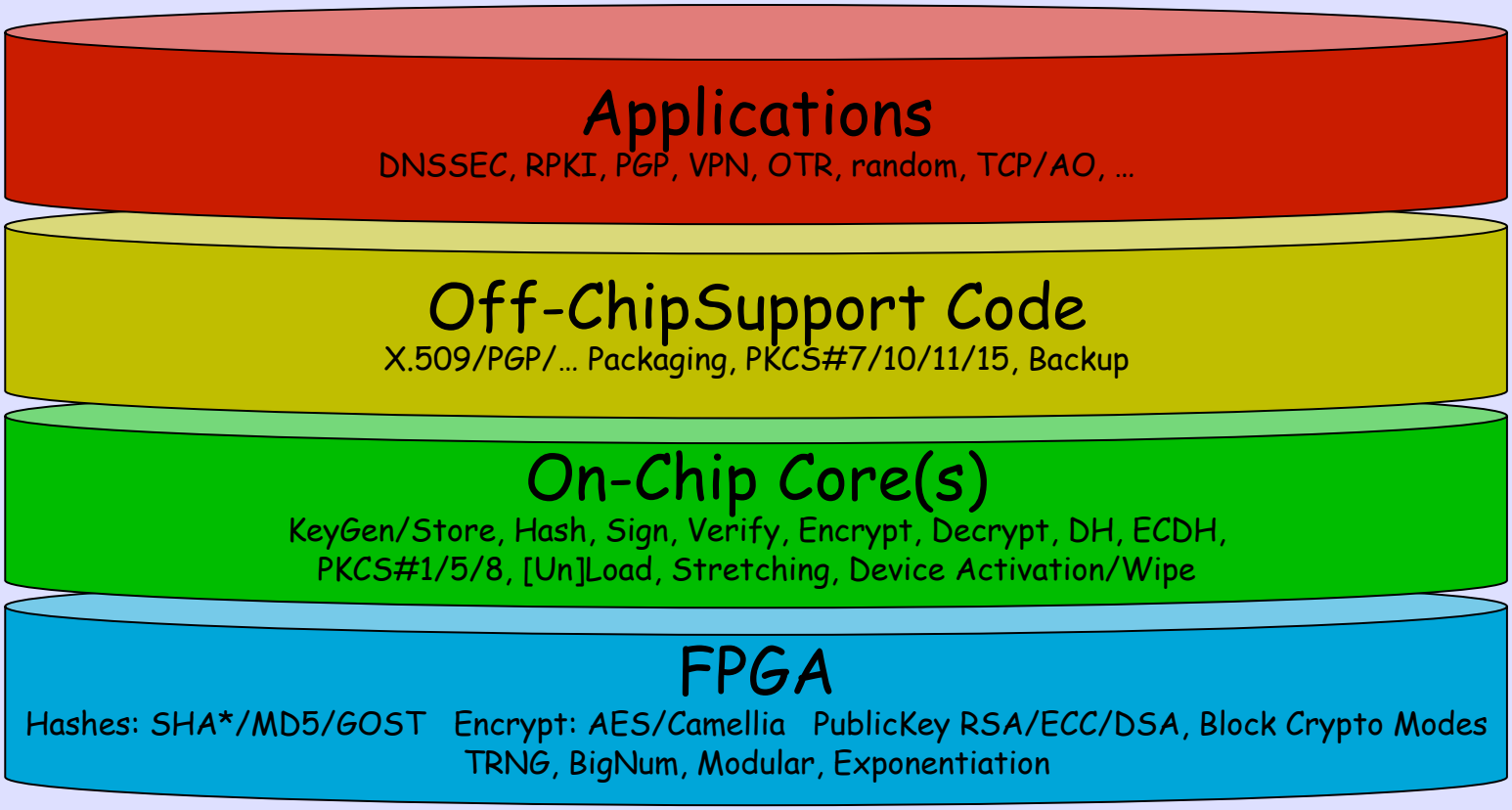


Potting Boundary

- The FPGA/ASIC and accompanying Core(s) (ARM, whatever) are within the physically protected boundary of the chip carrier potting.
- We worry about side channel attacks, i.e. information leakage from how power is used, RF, data-dependent time to do an operation, etc.
- We worry about tampering, what if the chip is opened and attacked? So the potting includes tampering sensors and code to wipe all keys if tampering is detected.



Writing 'Code'



C or HLL
e.g. Python

C or HLL
e.g. Python

C &
Assembler

HDL, e.g.
Verilog

Process Independent RTL

- Implementation agnostic bottom layer of cake
- Produce and provide HW-cores to implement them in FPGA
- But not use specific FPGA technologies, to allow implementation in different kinds of FPGAs as well as in ASICS
- https://en.wikipedia.org/wiki/Register-transfer_level
- Will have in C SW-cores anyway, if only for validation. So can run on arbitrary CPUs

Side Channel & Tampering

- Exponentiation circuit timing leaks are exploitable remotely
- Power leakage is exploitable locally
- Physical attack detection critical
- Wipe signal to chip
- On-board battery/capacitor to buy the time to wipe if unplugged from power

Trade-Off Spaces

- Cheap vs High Assurance vs Fast
- Trust boundaries vs Composable
- Side-channel & tampering protection costs

Some Phases

- First Year: Tool-chain, Basic Design, not all cyphers, not all protocols, prototype implementations on FPGAs and boards
- Second Year: Better Tool-chain, all needed cyphers, hashes, crypting, … and integration with some apps, DNSsec, RPKI, TLS, PGP, Tor
- Third Year: Solid packaging, ability to compose designs for use cases, etc.

A Few Related Projects

- Truecrypt audit: `http://istruecryptauditedyet.com`
- OpenCores: `http://opencores.org`
- Icarus Verilog: `http://iverilog.icarus.com`
- Valgrind: `http://valgrind.org`
- clang+llvm: `http://clang.llvm.org`

No Project is an Island

- We'll steal from anybody! ☺
- We'll share with anybody!
- We incite others to help, copy, clone, …
- If donors are generous, we will finance others working on related/needed work
- We desperately want to further diversify and to build trust

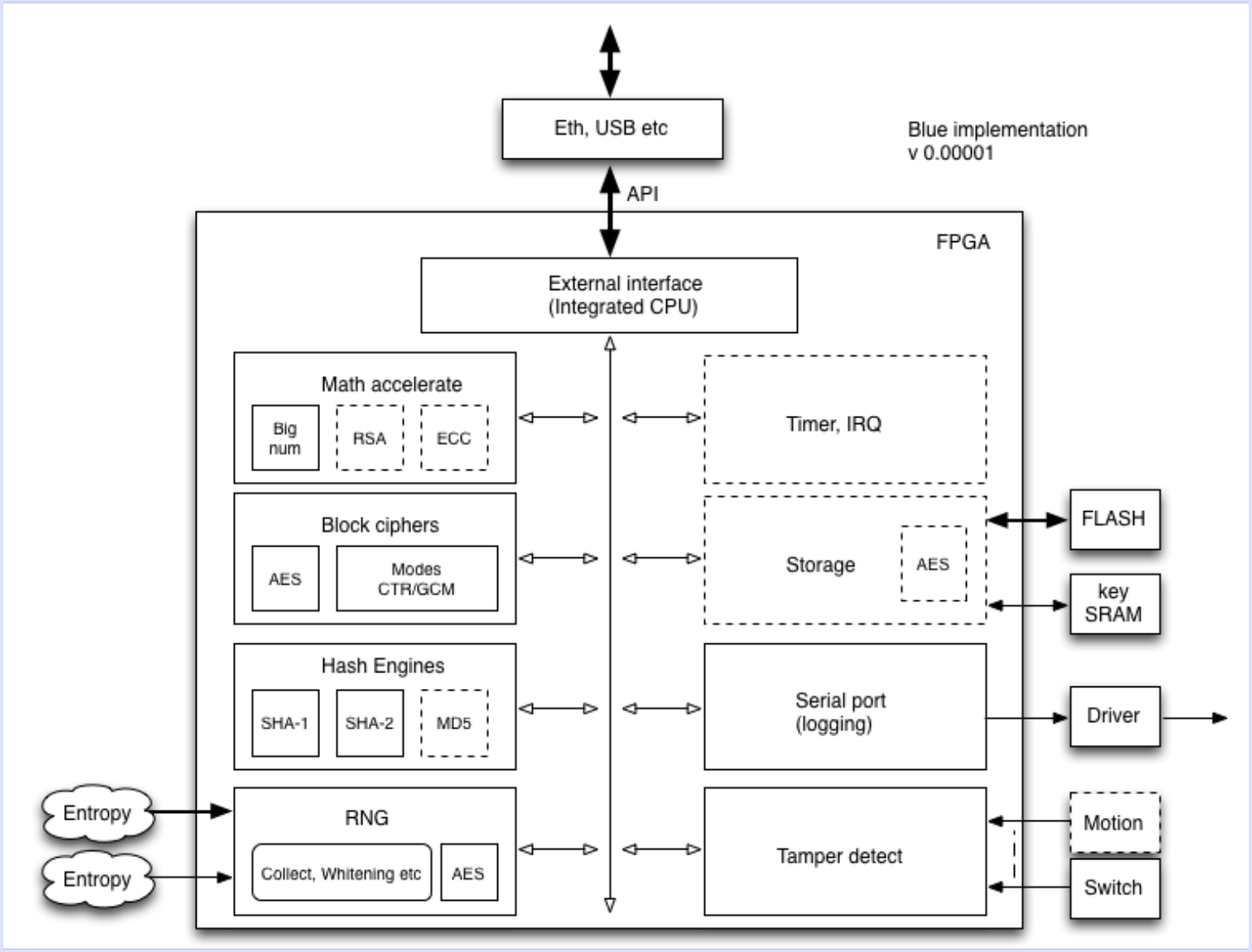
We Seek Review

- We seek, expect, and encourage any form of open and transparent review
- We will not (soon) seek certification as cost/benefit is high
- But we encourage/expect others to take the designs down that path
- We will document all security claims

Begging

- We have some small initial funding: $50k from ISOC, $50k from SURFNET, $20k from SUNET, …
- Folk such as Vint at Google are digging in their corporate pockets
- We have no organized funding effort as everyone is overworked
- We need to give funding assurance to a small team of very senior engineers

FPGA Cat Video



Contact

Wiki at https://cryptech.is/

(yes, you will need to accept our cert)
(and do follow the, often subtle, links downward)

Mailing list is tech@cryptech.is

Contributions to:

- Cryptech
- TBD
- Sweden