PEACE OF MIND IN A DANGEROUS WORLD

Tuesday, Nov 16, 2021 15:00 CET Advantages of FPGA -based cryptography

Webinar series: Cryptography under the hood

Speaker **Kimmo Järvinen** CTO & Co-founder, Xiphera

PEACE OF MIND IN A DANGEROUS WORLD

Advantages of FPGA-based cryptography

Kimmo Järvinen CTO, Co-founder, Xiphera Ltd.

Nov. 16, 2021



Agenda

- Why is HW faster than SW?
- Why is hardware (HW) more secure than software (SW)?
- Benefits of Field Programmable Gate Arrays (FPGAs)

Processors, ASICs, FPGAs, ...

- Processor: An Integrated Circuit (IC) that executes programs consisting of instructions supported by the processor's Instruction Set Architecture (ISA)
- Application Specific Integrated Circuit (ASIC): An IC designed for a specific application
- Field Programmable Gate Array (FPGA): An IC designed to be programmable on the logic level



Programmability

Fast Cryptography with HW

- Cryptography often uses operations that do not map well into the ISAs of common CPUs
 → Multiple instructions → Long latency
- ISE (e.g. AES-NI) helps but only half the way
- Hardware (incl. FPGA) allow bit level and clock cycle level optimisations
- Unrolling and pipelining to increase speed



Round

Contemp Software Stack

- In SW-only systems cryptography and keys are "just" regular programs and data
 - Keys are in the main memory when in use, stored in the hard drive, etc.
- Bugs and features in the deep SW stack can compromise security

Security software
3 rd party libraries
Toolchain
Operating System
Drivers
Processor

Isolation of Cryptography

- HW based cryptosystems can isolate cryptographic computations and keys
 - Even if the SW side is compromised, keys remain protected



IP Core = Intellectual Property Core

Example: Heartbleed



Hardware Root-of-Trust

- Isolated cryptography and keys is only half of the story
- If compromised SW can call HW cryptography, then system level security is still likely to fail
- Trust to the entire system can be built upon a trusted HW component, the Root-of-Trust



Crypto Agility

- Ability to add, replace or remove algorithms
 - Broken algorithms
 - New algorithms
- Very important currently
 - Post Quantum Cryptography (PQC) algorithms are coming but are not standardized yet





Alg. 4 is not supported at all!

0

FPGA Device Security

- Integrity of the FPGA configuration is at least as important as the SW integrity!
- If secrets are embedded into the configuration, then it must also remain confidential
- Modern FPGAs support encrypted and authenticated configuration



Comparison

	Speed	Agility	Energy	Isolation	Integrity
SW-only	٠	••••	•	•	•
SW + ISE	•••	••••	••	•	•
SW + TEE	••	••••	•	•••	•••
ASIC: TPM	•	•	••••	••••	••••
ASIC: Accelerator	• • • • •	•	••••	••••	••••
FPGA	••••	••••	•••	••••	••••

When to Use FPGA Cryptography?

- Fast encryption speeds (>10Gbps)
- Energy/performance budget is too tight for SW
- High security requirements
 - The highest security certifications typically require isolated cryptography
- Long product life-time

- Crypto agility (+ any on the left) needed
- Retro-fitting security to FPGA-based products on the field ("brownfield")
- FPGAs are the best option more often than generally thought...

this sea busy are than

Althe all use seven numeric std all the

in the logic bytes valid in and logic.

Ingle, vector(deta, unit) (sowerts 0), din Ingle, tast : in Atd, logic, byter by twentist logic, digest, withing logic, vector(data, wight-t alwante 0).), and entity sip303. At any bary, any dag . o

Attentural: Ebrary men wes lead and house and all

e sentor(date, wight-1 downto-0); die, valid dewnto-0); die, valid - in efd, linge

tirs ctr value



Thank you!

hay in busy or as bury or ling an an long ready as an routy data out an are data buth ready

as ass ready, data out

downto 01 request data

are free, ready the are ready data out the ast data out; ready

ing work use work my package all entity sig 2034h is part? - cit

www.xiphera.com info@xiphera.com kimmo.jarvinen@xiphera.com

dist

CONTRACTOR OF LET

Next webinar

voctoridete width i sownio 01 din

State of Play of Post Quantum Cryptography

March 9, 2022

CPPR

as ses busy, etr. Reg as err Heg, ready

vector(data_width-1 downto 0)); and antity xip3034h; i_aas : aas

logic: last

Die Mine sie

ut std togic vector/data width-1 downto 01

in std logic; bytes

and entity viologa

ind writing sig 2034b.

an new bary, are they

PEACE OF MIND IN A DANGEROUS WORLD

brary work, me work.my package.all;

bytes, valid ; in ald Jogic, vestor 2 downto 0); request, data ;

can investigate and all library work use work my sackage all; entity sig3034h

au ready

www.xiphera.com info@xiphera.com kimmo.jarvinen@xiphera.com

as set ready data out as set data but ready

the and ready, data out on any data out; ready

out std. k

arti cià

as olk, rst

as any ready, data out

downto C), request data