Arm CCA will put confidential compute in the hands of every developer

June 23, 2021

By Richard Grisenthwaite, SVP, chief architect and fellow, Arm

Earlier this year we announced the new Armv9 architecture, which will form the leading edge of the next 300 billion Arm-based chips. This included the introduction of the Arm Confidential Compute Architecture (Arm CCA), a key feature of Armv9-A and the next step in transforming how we think about the trust model of compute environments in every application. Today, we're unveiling the initial technical specifications for Arm CCA and sharing our vision for the next steps to unlocking the power and full potential of data, by making the benefits of confidential computing accessible to all developers.

Confidential compute: the next era of secure processing

Currently, applications and virtual machines place huge amounts of trust in the supervisor software (kernels or hypervisors) that manage them. Supervisors can access the resources used by applications for their program code and data. Exploits against supervisors can therefore leak confidential data or algorithms held in the applications.

Confidential computing changes the traditional trust relationship between applications and supervisors by removing the supervisor's right to access the resources used by the application, while retaining the right to manage them. Removing that right of access is critical because the devices we use today handle large quantities of confidential data. Cloud systems can be running payloads from many different customers, while mobile devices can contain both personal and business information, from medical data to company emails. Confidential computing reduces the need to trust unseen technology within any compute environment.

Arm CCA: Protecting data and code wherever computing happens

As the computing architecture of choice in applications spanning the sensor to the smartphone to the supercomputer, Arm is uniquely placed to enable the industry with the robust security foundations they need while ensuring developers can implement Arm secure technologies as simply and quickly as possible.

Arm CCA extends workload isolation to enable a provider to shift from a position where service providers **will not** access customer data, to one where they **cannot** access customer data - thereby reducing the volume of software that must be trusted, the attack surface for hackers, and the potential for customer data or algorithm breaches. Arm CCA introduces a new kind of confidential computing environment called a Realm, which protects the data and code, even in use.

We're achieving this through our work in four key areas:

- Realm Management Extension (RME): Defines the hardware architecture for Realms
- Dynamic TrustZone technology: An extension to TrustZone enabled by RME that removes the need to dedicate memory to TrustZone, allowing TrustZone to be used for applications with large and dynamic memory footprints
- A software and firmware architecture: collaborating with OS vendors and industry bodies to drive standard interfaces for interaction with RME firmware by defining a Realm Management Monitor (RMM) and extensions to the Monitor to provide an architecture for Realms

- Working with open-source projects such as trustedfirmware.org to provide standard implementations of Arm CCA firmware, and creating new projects for confidential computing such as project Veraison, which will deliver open-source software for constructing attestation verification services

The code or data of a Realm is situated in memory that is assigned to that Realm, and any attempted access of that memory from the supervisory software that created the Realm (kernel or hypervisor), or by TrustZone code, other Realms or devices not trusted by the Realm, are blocked and result in faulting exceptions. To enable this, a new data structure has been

added to the architecture - the Granule Protection Table. This structure tracks whether a page is to be used for Realms, TrustZone or for the normal world, where existing applications, kernel, or a hypervisor run today. The hardware checks this table upon every access and blocks any that are illegal. A hypervisor or kernel can indirectly update this table, allowing pages to migrate between normal world use and Realms, or even between normal world use and TrustZone use. This ability to dynamically move memory resources among different security environments is a key change in the architecture. You can read more detail about Realms and how they work in this blog from my colleague and Arm Fellow, Charles García-Tobin.

Empowering all developers to access best-in-class security features

A key goal as we built Arm CCA was to make confidential computing accessible to every developer, whatever application they may be working on. With the hardware specifications now available, we are continuing to engage with our extensive software ecosystem as a critical next step in the development of Arm CCA.

Which is why at a Linaro Arm CCA Tech Event today, our team is introducing the hardware and software architectures and resources available to enable OSS software development and upstreaming, including compiler support, open-source Trusted Firmware A (TF-A) Monitor code, and Project Veraison. In the future Arm will provide reference implementations of the Realm Management Monitor and work closely with toolchain and OS vendors to ensure realms are accessible to the broadest possible range of application developers.

possible range of application developers.

Looking ahead: No workload left behind

Arm CCA is going to provide the next layer of security required everywhere computing happens. In the data center, providers can use it to take more infrastructure out of the data path to reduce the risk of a breach while tenants can migrate ever more sensitive workloads away from on-premises systems and into the cloud.

Beyond this, just as other cloud computing is moving to the edge, so will confidential computing. Mobile and wearable devices now span our personal and work lives, placing new pressure on the ability of these devices to protect our data. For example, to progress health services and science we need secure ways to aggregate data anonymously. Smart cities and autonomous vehicles need increased levels of mutual trust and businesses need to know their data is safe on our personal devices.

We predict that soon, 100 percent of the world's shared data will be processed on Arm; either at the endpoint, in the data networks or the cloud. This pervasiveness brings a responsibility to deliver even more security, building on the strong foundations we have created with isolation technologies such as Arm TrustZone, which can be found in billions of devices today. Our vision for Arm CCA is to protect all data and code wherever computing happens, while empowering developers to implement strong privacy controls – today marks an exciting first step towards that vision.

You can find more information on Arm CCA here.

Ecosystem support

Fortanix:
"To truly unlock the potential and power of data, security needs to evolve to protect this data and code not just at rest and in transit but in use. Arm's Confidential Computing Architecture is an important step in putting confidential computing in the hands of as many developers as possible at a time when it has never been more critical for the industry to collaborate to

time when it has never been more critical for the industry to collaborate to deliver best-in-class security across every application, and drive new robust and open standards in this space."
Richard Searle, Customer Solutions Director, Fortanix, a General Member's Representative to the Governing Board of the Confidential Computing Consortium and Chair of the End-User Advisory Council

Google:
"Google Cloud and our customers have seen first-hand how the adoption of confidential computing can increase security, privacy, trust, and enable the most sensitive workloads to move to the cloud. The availability of Arm's Confidential Computing Architecture will give organizations even more choice for how and where to deploy this transformational technology to secure their critical assets."
Nelly Porter, Group Product Manager, Cloud Security, Google

Microsoft:
"The Armv9 confidential compute features were developed in close collaboration with Microsoft, and we believe that it is critical that we put confidential compute into the hands of as many developers as possible to enable the next era of secure computing. Through the use of realms, the Arm Confidential Computing Architecture has the potential to raise the security bar for all developers, bringing huge benefits across the ecosystem in terms of protecting computation and data in-use, delivering confidential compute for everyone whatever the application."
Dr. Leendert van Doorn, Distinguished Engineer, Microsoft

NXP:
"In our increasingly automated world where data privacy and confidentiality are imperative, Arm CCA provides an opportunity to add a complementary layer of security to the integrated security capabilities that have been foundational to our processing portfolio for IoT, industrial, and automotive markets. Data generated, processed and sent by intelligent edge devices must be protected, and this is a step toward achieving that desired integrity and confidentiality."
Ron Martino, Executive Vice President and General Manager of Edge Processing, NXP Semiconductors

Alex Harrod

Director Public Relations, Arm
Alexandra.Harrod@arm.com
+44 7795 363057

About Arm

Arm technology is at the heart of a computing and data revolution that is transforming the way people live and businesses operate. Our energy-efficient processor designs and software platforms have enabled advanced computing in more than 190 billion chips and our technologies securely power products from the sensor to the smartphone and the supercomputer. Together with 1,000+ technology partners we are at the forefront of designing, securing and managing all areas of AI-enhanced connected compute from the chip to the cloud.

Products

IoT Solutions

Processors

AI Platform

Graphics and Multimedia

Development Tools

Custom SoCs

Technologies

Arm Architecture

DynamIQ

big.LITTLE

Arm NN

CMSIS

Neon

TrustZone

Partner Ecosystem

Arm Approved Program

Artificial Intelligence

Automotive

HPC

Infrastructure

Mbed Partners

Support

Design Reviews

Developer Forums

Training

Documentation

Downloads

Contact Support

About Arm

Leadership

Security on Arm

Arm Blog

News

Arm Offices

English