Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

Arm

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Office of Science and Technology Policy
“Notice of request for information on Advancing Privacy-Enhancing Technologies”
Document Number 2022-12432
8 July 2022

On behalf of Arm[1], please find comments to the consultation on advancing privacy-enhancing technologies, or “PETs”. As the leading global provider of semiconductor intellectual property (“IP”) and supporting technology, Arm is at the forefront of developing the types of technologies discussed in the consultation and fully supports the U.S. Government and the Office of Science and Technology Policy promoting and supporting accelerated development, deployment and adoption of PETs.

Over the years, Arm has developed and licensed a number of technologies that have been used to provide protection of data in use from even privileged software. TrustZone™ [2] has been in the market in the form of central processing unit (CPU) IP since 2004 and can protect a set of fixed software payloads from the operating systems and hypervisors. TrustZone is used on billions of devices today to provide use cases such as mobile device management, payment, and user authentication through biometrics. TrustZone is designed to allow device vendors to implement security use cases associated with the platform, these are limited in number and so in general this is also true for the amount of memory that can be used by TrustZone workloads. Arm has also provided support for Virtualization in CPU IP since 2011. Virtualization is often used in deployments to protect security use cases from a primary operating system (OS) kernel. With virtualization there is no specific limit on the amount of memory resource that can be used by a secure workload, that is shielded from a primary OS kernel, but both the hypervisor and code in TrustZone need to be trusted by such a secure workload. This might not be practical in deployments where the provider does not have full control of the stack or where those pieces of software are large and complex.

In June 2021, Arm made a significant announcement for PETs with the launch of technical specifications for Arm Confidential Compute Architecture (Arm CCA). This combines the properties of TrustZone and virtualization, and provides trusted execution environments (TEE), called Realms, which are protected from supervisory code such as hypervisors or kernels, as well as from TrustZone code, or other Realms.[3] As is the case with virtual machines, Realms are not limited on the amount of memory they can use.

To further contribute to the development and adoption of PETs, Arm is also a Premier Member of the Confidential Computing Consortium, under the Linux Foundation, which is the leading group developing open source, and open standards and specifications focused on Confidential Computing and specifically the area of “data in use”. This was the key missing piece to

[1] See Defining the Future of Computing – Arm®
[2] See, for instance TrustZone for Cortex-A – Arm®
[3] For a more complete discussion on CCA, see Unlocking the power of data with Arm CCA - Architectures and Processors blog - Arm Community blogs - Arm Community

significantly enhancing security and privacy, as protection methods have existed for “data at rest” and “data in transit” and work continues to strengthen those two distinct areas.

Protecting data while in use was difficult as it required silicon, software, and other technology providers to coalesce around significant changes to underlying computing architecture, but the results will create a more secure digital world. As Arm’s Senior Vice President and Chief Architect, Richard Grisenthwaite, described in a blog on the announcement of Arm CCA:

> 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 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.[4]

And as Richard goes on to conclude: “Our vision for Arm CCA is to protect all data and code wherever computing happens, while empowering developers to implement strong privacy controls…”.

----

[4] See Arm CCA will put confidential compute in the hands of every developer – Arm®

In response to the specific questions from the consultation, please find Arm's responses below:

1. *Specific research opportunities to advance PETs: Information about Federal research opportunities that could be introduced or modified to accelerate the development or adoption of PETs. This includes topics for research, hardware and software development, and educational and training programs. This also includes information about specific techniques and approaches that could be among the most promising technologies in this space.*

Arm response

The Department of Defense (DoD), Defense Advanced Research Project Agency (DARPA) has funded work into a technology areas known as "fully homomorphic encryption" or "FHE" through a project named Data Protection in Virtual Environments (DPRIVE).[5] This technology area is one of the most promising ways of doing privacy-enhancing analytics on extremely sensitive data sets, and will have significant application across DoD and commercial applications. Four teams of researchers have been selected to perform this work and Arm are acting as a subcontractor to the SRI International team.[6] DPRIVE and similar projects should be a priority for the USG to continue funding, particularly if additional appropriations are made for technology research through the U.S. Innovation and Competitiveness Act (USICA) or through the potential increased funding allocations Congress is considering in the Fiscal Year 2023 National Defense Authorization Act.

3. *Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs: Information about sectors, applications, or types of analysis that have high potential for the adoption of PETs. This includes sectors and applications where data are exceptionally decentralized or sensitive, where PETs could unlock insights or services of significant value to the public, where PETs can reduce the risk of unintentional disclosures, where PETs might assist in data portability and interoperability, and sectors and applications where the adoption of PETs might exacerbate risks, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This topic covers opportunities to improve the effectiveness of data sharing among specific Federal agencies and between specific Federal agencies and entities outside the Federal Government, including the goals outlined in Section 5 of Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government.*

Arm response

Cloud will be the first area of computing where PETs will be deployed in scale. This has the potential to drive significant new use cases from sensitive workloads such as medical and

[5] See Data Protection in Virtual Environments (darpa.mil)

[6] See DARPA Selects Researchers to Accelerate Use of Fully Homomorphic Encryption

financial services which are currently done on premises out of concern for potential compromise in cloud servers. Research suggests that a significant proportion of server workloads (65% generally rising to above 90% in financial services) are currently hosted in private data centers. Data residency is ranked as a top reason for maintaining private infrastructure. Additionally, certain government use cases could transition to the cloud with cloud deployments of Arm CCA and other comparable technologies. A gold standard for cloud providers is to achieve a state where they are unable to access customer data.

Veracruz is an open-source software project[7], adopted by the CCC, which is developing a framework for privacy-preserving collaborative computing that may be useful for Federal Agency sharing and collaboration, as posed in the question. The aim of Veracruz is to explore and create a demonstrator for how secure distributed systems can be built using strong containerization technology and remote attestation protocols. As the Wiki discusses, possible use cases include privacy-preserving machine learning, delegated computation, and commitments.[8]

Secure transport protocols like TLS will be updated to support mutual attestation, enabling workloads everywhere to establish the trustworthiness of cloud services before data is exchanged or trusted. When PETs that support platform and workload attestation are deployed across a broader range of form-factors, cloud services will also be able to assess the trustworthiness of devices like edge servers, laptops, and phones. It is expected that the PETs will be deployed on microprocessors before they're deployed with microcontrollers.

4. *Specific regulations or authorities that could be used, modified, or introduced to advance PETs: Information about Federal regulations or authorities that could be used, modified, or introduced to accelerate the development or adoption of PETs. This includes privacy-related rulemaking authorities under the Office of Management and Budget, the Federal Trade Commission, and financial regulatory bodies, as well as acquisition regulations under the Federal Acquisition Regulations. This also includes the Federal authority to set procedures for agencies to ensure the responsible sharing of data. This also covers hiring authorities to recruit Federal employees with expertise to advance PETs, as well as acquisition authorities (e.g., Other Transaction Authority) to procure PETs for development.*

Arm response

The U.S. approach to privacy and security has historically been based on a sector-specific, sensitivity-based approach. Health information, financial information, and children's and minors' online activity, for instance, all have been required to be handled in specific manners due to unique sensitivities. While the U.S. Congress is currently debating and attempting to legislate a more consistent and comprehensive approach to general data and privacy protections, the agencies regulating these more sensitive forms of data which already require

[7] See Veracruz Project – Just another Linux Foundation Projects 2 site (veracruz-project.com)

[8] See What are some use cases for Veracruz? · veracruz-project/veracruz Wiki · GitHub

special treatment should encourage, incentivize and in some instances mandate use of PETs. This should not be read as support for mandating a specific technology; as is the case in cybersecurity which the U.S. government generally addresses appropriately, technologies evolve, improve, and become outdated more quickly than government rulemaking. Rather, having already determined certain data types are more sensitive and therefore deserve special protections, appropriate agencies should consider whether commercially available technologies and industry best practices for protecting and preserving privacy of those types of data require more regulation or could be incentivized in other ways, as has been done in the cybersecurity space.

Further, the US government should use its procurement and purchasing power to drive adoption and broader take up of PETs. This could be done by moving certain government workloads currently done on-premises to the cloud in instances where cloud provider use or PETs that can offer comparable levels of data privacy protections to on-premises.

Lastly, NIST standards such as FIPS 140-2 have been instrumental in helping buyers procure secure products and services. The US government may like to consider supporting or developing a similar standard to define security requirements for cloud instances that support PETs such as Confidential Computing. This would help government and private sector organizations choose between products. In the absence of standardization, organizations will need to undertake their own security assessment, an activity that requires specialized resources and access to information pertaining to each vendor's platform architecture; this would result in either applications staying on-premises, or data being placed at risk.

8. *Existing best practices that are helpful for PETs adoption: Information about U.S. policies that are currently helping facilitate adoption as well as best practices that facilitate responsible adoption. This includes existing policies that support adoption, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This also includes information about where and when PETs can be situated within tiered access frameworks for accessing restricted data, ranging from publicly accessible to fully restricted data.*

Arm response

USG should include discussion of PETs in all relevant government and industry guidance documents, and should keep them updated on a regular basis as the technology develops. These include, but are not limited to, the NIST Cybersecurity Framework,[9] the NIST Privacy Framework,[10] CISA's Privacy Impact Assessments,[11] and all relevant FTC privacy and security guidance.[12]

[9] Cybersecurity Framework | NIST

[10] Privacy Framework | NIST

[11] Privacy Impact Assessments | Homeland Security (dhs.gov)

[12] Privacy and Security | Federal Trade Commission (ftc.gov)

Further, an expert agency could be tasked with drafting a guidance document that would enable migration to, and greater uptake of, current and emerging PETs. NIST have done something similar to this with its work to prepare for and facilitate the migration and adoption of post-quantum cryptography when that technology is ready for wide deployment.[13] While not an exact parallel, something similar could be done to prepare for and facilitate greater adoption of PETs among government agencies.

Conclusion

Arm appreciates the opportunity to contribute to the Office of Science and Technology Policy's information gathering on PETs, and share perspectives on how to advance their development and adoption. Please be in touch if we can provide additional information on our responses or other questions the Office may have.

Respectfully Submitted,

Vince Jesaitis[14]
Hugo Vincent
Charles Garcia-Tobin
Mark Knight

[13] See Migration to Post-Quantum Cryptography | NCCoE (nist.gov) and https://www.nccoe.nist.gov/sites/default/files/2022-06/Migration-to-PQC-05-16.pdf

[14] Contact for additional questions: