The Confidential Computing Consortium's Response to the Internet Architecture Board's Statement on Attestation

Approved by the CCC Technical Advisory Council on November 2, 2023.

The Confidential Computing Consortium (CCC) requests that The Internet Architecture Board (IAB) amend its September 25, 2023 Statement on the Risks of Attestation of Software and Hardware on the Open Internet. The CCC believes the statement as worded may adversely impact the adoption of beneficial security technologies which make use of other embodiments of attestation.

The title of the statement is immediately problematic for its unqualified use of the term attestation and does not, we believe, address the IAB's intent. Moreover, the statement includes specific recommendations which are also problematic (emphasis added):

> *"If client attestation signals are used in open services to mitigate fraud or abuse, they should be designed to only signal the authenticity of a user or client without imposing strict software or hardware requirements."*
>
> *"For services that have intentionally restricted access, such client attestation (as described in Remote ATtestation procedureS (RATS), RFC 9334) is a valuable security measure, particularly when used in conjunction with user authentication. However, this approach is not appropriate for openly accessible services."*
>
> "*[f]undamentally, attesting specific properties about a networking client (e.g., there is some human user involved in this interaction) maintains the openness of the Internet, whereas attesting that a specific piece of software is in use does not and should be avoided*".

These statements appear to have been made in reaction to a recent Web Environment Integrity (WEI) proposal, and the IAB's guidance is derived from a principle that "*Allowing clients to use a variety of software as long as it is protocol-compliant is an essential part of the IETF development process and the openness of the Internet*". However, we would like to highlight that the IAB statement goes beyond a response to WEI and is at once imprecise in its terminology, broad in its scope, and categorical in its prescription. Literal application of the guidance would inhibit positive uses of attestation in the Internet, to the detriment of security and privacy. We therefore request that the IAB revisit its guidance to recognize and explicitly support positive usages.

The CCC and RATS working groups define attestation with a specific technical sense (definition 1 herein) that should not be conflated with the term's usage in the WEI proposal, the compliance community, and/or the software supply chain community. Attestation is "*the process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements*". We note that there are many positive uses of attestation whether on both clients and servers, including:

- Detecting unpatched software
- Enforcing supply chain integrity at the point of use (particularly valuable for enabling the broader open-source software ecosystem)
- Protecting workloads (containers/processes/VMs) from malware
- Authenticating software endpoints and software components in emerging zero trust architectures (see NIST Special Publication 800-207)
- Assuring the authenticity of a workload implementation that may have been analyzed for specific privacy or behavioral properties (especially useful for multiparty analytics)
- Transferring institutional trust to measured software and authentic hardware, which in turn is key to minimizing the attack surface area by removing unnecessary parties from the chain of implicit trust, such as the OS vendor, a cloud platform operator, or an untrusted party with physical access to the device.

To support these benefits, Confidential Computing implements and relies on attestation as the fundamental mechanism underpinning policy specification and enforcement, and these benefits cannot be broadly proscribed without undermining security and privacy, and innovation in security and privacy.

We note that Internet architects have long recognized the inevitability of tensions between competing principles such as security and openness [Tussle2002]. One thoughtful approach to mediating such tensions is to separate mechanism from policy, and to develop mechanisms in conjunction with flexible policy engines to support innovation in the use of the mechanism. Ultimately, it is a specific policy decision that is harmful or not - as opposed to the use of the underlying mechanism. There is room for productive discussion around what aspects of appraisal policy are beneficial, damaging, or neutral to the IAB's goals without condemning all mechanism uses in a specific context.

Confidential Computing as a mechanism will itself evolve in many ways including in its uses and applications. Stakeholder interests (service owners, end users, infrastructure providers, etc.) will need to be balanced and rebalance as innovation proceeds. We therefore support innovation in the use of Confidential Computing mechanisms, and in particular we support open source projects and initiatives that will help enable future choice and flexibility in attestation policy specification and attestation verification. The protocols and deployment models associated with remote attestation play an important role in openness, and we value work in privacy-preserving attestation mechanisms (e.g., Direct Anonymous Attestation in the IETF RATS working group). We also recognize the importance of work that provides flexibility in the deployment and control of attestation verification functionality within a trust domain such that users' interests are represented.

We hope that in the coming years that our combined communities can continue to innovate jointly and openly in ways that respect the openness, fairness, security, and privacy concerns of all stakeholders in the global computing infrastructure. Existing collaboration between the CCC and IETF RATS and Trusted Execution Environment Provisioning (TEEP) working groups have been working well. We welcome additional participation in all three groups. Like IETF meetings and mailing lists, CCC meetings and mailing lists are open and public.