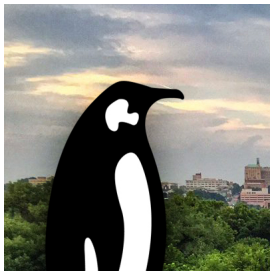

Contribution ID: **258** Type: **not specified**

How to Build a Confidential Attestation Client

Tuesday, 14 November 2023 15:20 (20 minutes)

When designing an attestation framework, implementing a client which runs inside a confidential guest might seem like the simplest part, but this session will introduce several subtle factors that can undermine security and usability if not addressed. We will discuss how these issues might apply to different confidential projects and how they can be resolved. We will include some provocative examples and interesting proposals. For example, the session will introduce evidence factory attacks, which can compromise not just one enclave, but an entire service or deployment. We will show how severe these attacks can be and how they can be prevented. We will look at how to design an attestation client that supports separation of privileges within one guest. We will discuss best practices for populating the guest data in an attestation report and for providing extra information to a relying party. We will also consider challenges in orchestration including how to provide connectivity to attestation clients running in minimal environments. Even with a standardized attestation flow, a thoughtful guest implementation is essential to building a secure, performant, generic, and easy-to-use system. There are many open questions in this space that will be discussed as a group.

Primary author: FELDMAN-FITZTHUM, Tobin (IBM)

Presenter: FELDMAN-FITZTHUM, Tobin (IBM)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC