PIC Model: Provenance Identity Continuity (PIC) Model for Distributed Execution Systems

Nicola Gallo[1]

***Abstract*— The Executor-First Paradigm mandates that identity is an emergent property of the current execution state and its verifiable cause. The Provenance Identity Continuity (PIC) Model defines the invariants that identity MUST satisfy across the entire causal sequence of execution, addressing the inherent limitations of artifact-centric security models.**

The model includes the Structural Impossibility Claim (NO-GO Result), which presents a structural impossibility argument, not a mathematical proof. Formal treatment is delegated to future work.

I. Introduction

This model is derived from a natural observation of the delegation pattern and the multi-hop nature of distributed systems. Even in a paper-based artifact format, delegation involves the delegator (who signs) and the delegate (who proves their identity). In such a model, an artifact loses its meaning if the delegate is removed; anyone who acquires it can claim its use, thereby nullifying the intrinsic value of the delegation artifact itself. The two minimal required entities are the delegator and the delegate. Therefore, the validity of both the delegator and the delegate must be proven—two single inputs. Any other method that introduces complexity only increases the attack surface, rendering the approach weaker from a security perspective.

Naturally, artifact-centric security models are widely used today, and it may seem counter-intuitive that they are inadequate for securing distributed systems. The problem, as anticipated, stems from the artifact's inherent coupling with the delegator (the artifact holder). Current delegation models operate only under severe restrictions:

- The initial single hop requires authenticated transport channels (e.g., TLS authentication), essentially binding the delegate's identity to the transport channel.
- Subsequent calls over authenticated transport channels are often maintained via token exchange mechanisms.
- Second and subsequent hops are often assumed to be protected solely by network isolation (VPNs, firewalls, private networks), leading to situations where identity continuity cannot be reliably preserved.

For example, in systems like Apache Kafka, **relying on a traditional static security artifact is often impractical for safe and functional transmission**, as this immediately creates a large attack vector. If the signature is removed, it ceases to be a security artifact; if it is encrypted, there is no guarantee it will be processed before expiration. This fragmented approach necessitates multiple methods to handle exceptions, ultimately leading to superior complexity and an increased number of vulnerabilities.

To fully grasp the paradigm shift, we **MUST** first formalize the inherent multi-hop nature of distributed systems.

[1]Nicola Gallo, Software Architect. All opinions and contributions are my own. github.com/ngallo

II. Terminology and Granularity

xxxxxxx xxxxxxx

Acknowledgments

Author's Note on Intellectual Property and Generative Assistance

The **PIC Model**, its complete axiomatic system, formal definitions, and the **Structural Impossibility Claim (NO-GO Result)** represent the sole original intellectual property and core theoretical contribution of the author.

Generative AI tools were employed exclusively for editorial refinement, stylistic polishing, structural organization, and ensuring notational consistency, and made no conceptual or scientific contribution to the model presented.