Discussion Leading Write-Up

Title: eZTrust: Network- Independent Zero- Trust Perimeterization for Microservices

Authors: Zirak Zaheer, Hyunseok Chang, Sarit Mukherjee, Jacobus Van der Merwe

Research question/ goal of the paper: The paper explores eZTrust, a network-independent perimeterization approach for securing microservices by enforcing access control policies based on fine grained workload identities rather than traditional network based perimeterization.

Challenge: The traditional perimeterization approach based on the principle of "trust but verify", such as network- endpoint- based access control, struggles with being unreliable and error prone, particularly to malicious lateral movement, and insider threats. There are also issues with regard to management, scalability and policy granularity. Existing methods for policy enforcement can be dynamically changed, spoofed, or misconfigured.

Claims: This paper claims that eZTrust is more efficient and reliable than traditional perimeterization approach as it adopts the principle of zero trust "never trust, always verify". This paper claims that eZTrust enables fine-grained, workload-identity-based access control, improving security without relying on network attributes. The paper also claims that this approach reduces packet latency by 2-5 times and CPU overhead by 1.5 - 2.5 times compared to traditional network based perimeterization methods.

Evidence: The authors provide empirical evidence through experiments conducted in a controlled cloud testbed using Cloudlab. Their evaluation examines: Packet processing overhead , Comparison with alternative approaches, and Correctness in dynamic environments(demonstrating that eZTrust correctly enforces security policies when microservices are scaled or reconfigured.)

Statistical Analysis: The authors compare fast-path and slow-path packet verification latencies under different policy conditions. eZTrust achieves minimal latency overhead, outperforming traditional perimeterization schemes. eZTrust's processing incurs lower computational costs compared to DPI-based or transport-layer perimeterization solutions. Results show that eZTrust can support many microservices while maintaining efficient enforcement of security policies.