Topic: Formal Methods for Cloud Security

Cloud environments continue to explode in complexity. How can we verify them at scale?

Ideas

- Cloud security is a function of cloud configurations
- Cloud configurations can be represented and manipulated via declarative policy languages on hyperscale clouds (AWS, GCP, Azure)
- We can parse cloud policies into first-order logic and use SMT solvers to verify them against well-known specifications (e.g. No instance is internet-facing without a bastion)
- We can integrate this verification into CI/CD pipelines to ensure the cloud is “correct-by-construction”

Methodology

- Implemented AWS IAM policy verifier based on AWS Zelkova Paper (Semantic-based Automated Reasoning for AWS Access Policies using SMT)
- Created a collection of “golden specifications” expressed in first-order logic
- Created a GitHub action to integrate verification with CI/CD pipelines

Results

- Gave a preliminary talk at SANS CloudSecNext about potential efforts on GCP and Azure
- Presenting AWS verification work at fwd:cloudsec in July 2022
- Continue to work on verification tools for cloud security