# Propagation of Insecure Coding in Configuration Scripts

Jonathan Dean, Electrical and Computer Engineering; Oluwatola Tofade, Electrical and Computer Engineering; Sushil Poudel, Computer Science;
Dr Rahman Akond, Assistant Professor, Computer Science;

## Abstract

- Infrastructure as code (IaC) is the practice of automatically managing configurations following the recommended software development practices.
- In our research, we investigate if insecure coding patterns (ICPs) in IaC scripts are propagated from one a repository to multiple repositories in the open source software (OSS) ecosystem.

## Research Objective

The goal of this project is to help practitioners secure configuration scripts by characterizing propagation of insecure coding patterns.

## Background

- We use a tool called Security Linter for Infrastructure as Code (SLIC) [1] to analyze and identify ICPs in repositories that are cloned from other repositories.
- We compare the resulting output from the SLIC tool to determine the propagation of ICPs for IaC scripts in OSS.

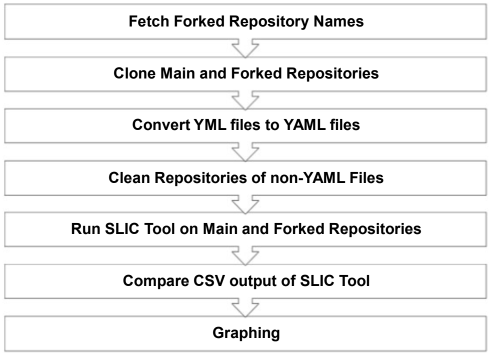
## Detected Types of ICPs

- Admin by default
- Empty password
- Hard-coded secret
- Invalid IP address binding
- Suspicious comment
- Use of HTTP without TLS
- Use of weak cryptography algorithms

## Problem Statement

Despite the popularity of IaC tools, insecure coding patterns (ICPs), such as hard-coded passwords, can be unintentionally introduced into IaC scripts, which eventually can propagate across other repositories with IaC scripts.

## Project Outline



Fetch Forked Repository Names

Clone Main and Forked Repositories

Convert YML files to YAML files

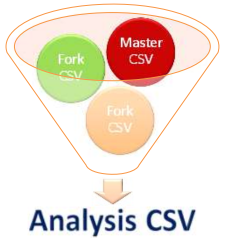
Clean Repositories of non-YAML Files

Run SLIC Tool on Main and Forked Repositories

Compare CSV output of SLIC Tool

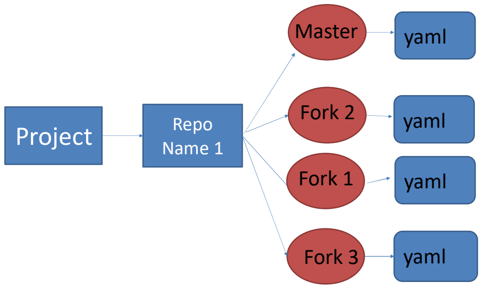
Graphing

## Comparison Process



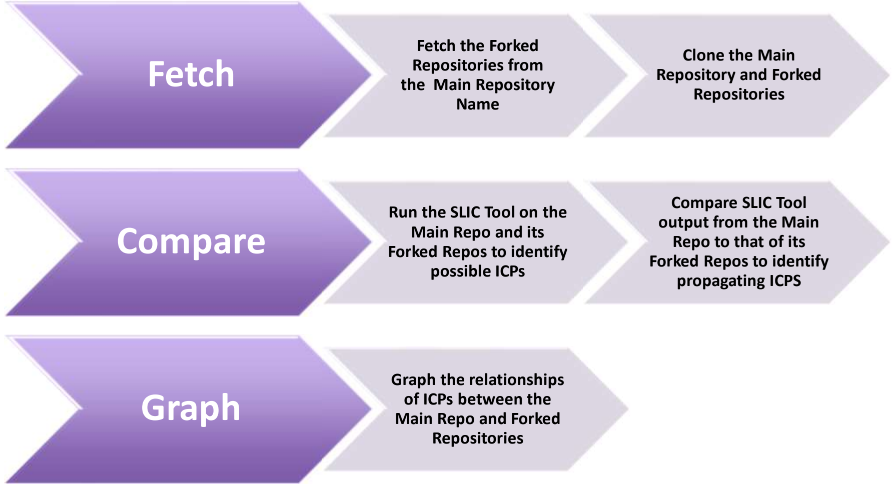
Visualization of comparison process from SLIC Tool Output

## Git Clone File Structure



Visualization of file storage structure for automated git-cloning.

## Methodology



**Fetch**

Fetch the Forked Repositories from the Main Repository Name

Clone the Main Repository and Forked Repositories

**Compare**

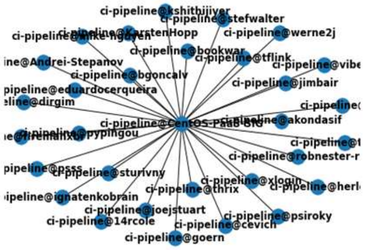
Run the SLIC Tool on the Main Repo and its Forked Repos to identify possible ICPs

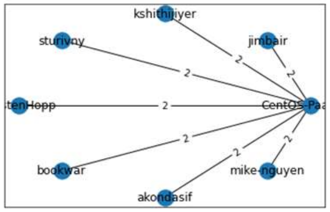
Compare SLIC Tool output from the Main Repo to that of its Forked Repos to identify propagating ICPS

**Graph**

Graph the relationships of ICPs between the Main Repo and Forked Repositories

## Graphs





## Preliminary Findings

| Main Repo | # of Forks | # of Original ICPs | # of Propagated ICPs | % of ICPs Propagated |
|---|---|---|---|---|
| 1 | 31 | 5 | 153 | 98.71 % |
| 2 | 2 | 492 | 487 | 98.98 % |
| 3 | 30 | 2 | 60 | 100 % |

Table of Results

**Based on preliminary findings we recommend practitioners take the utmost security consideration for ICPs in IaC scripts as they can propagate from one repository to another, creating large-scale propagation of ICPs in the OSS IaC ecosystem.**

## Next Steps

- Repeat the process for a larger dataset
- Perform a manual comparison to verify results
- Refine the tool to perform a more in-depth search
- Identifying Multi-Level ICP Propagation through forks

## References

[1]A. Rahman, C. Parnin and L. Williams, "The Seven Sins: Security Smells in Infrastructure as Code Scripts," *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)*, Montreal, QC, Canada, 2019, pp. 164-175.

*We would like to thank Dr. Akond Rahman and Department of Computer Science at Tennessee Technological University.*