Adaptive Evidence Collection Using Attack Scenarios

Dr. Sorren Christopher Hanvey. Supervised by: Prof. Bashar Nuseibeh

1 Motivation

» **Increase in crimes targeting the cloud:** Such crimes motivate the need for more effective digital forensic investigations.

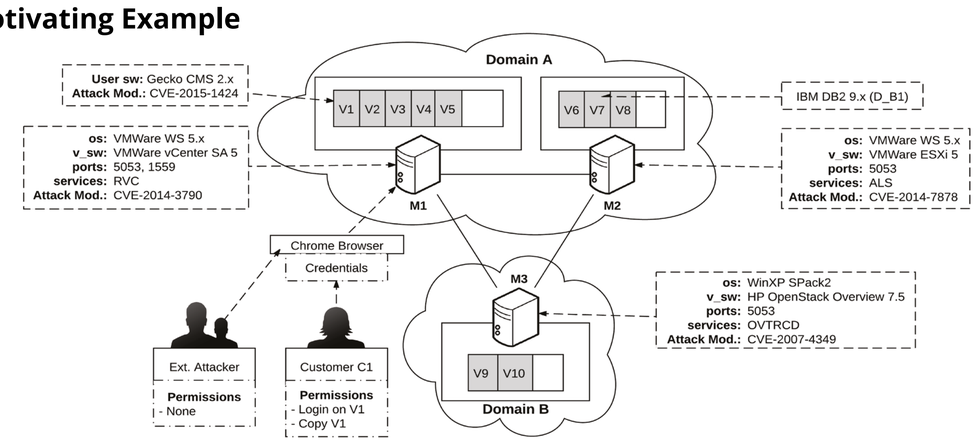
» **Large amount of data:** Forensic investigators must analyse a large amount of data generated in the cloud.

» **Cloud Elasticity:** The attack surface available to an attacker is constantly evolving, changing the way potential security breaches can arise.

» **Ephemeral Evidence:** Volatile evidence required to investigate a cyber-crime may no longer be available after a security breach is detected.

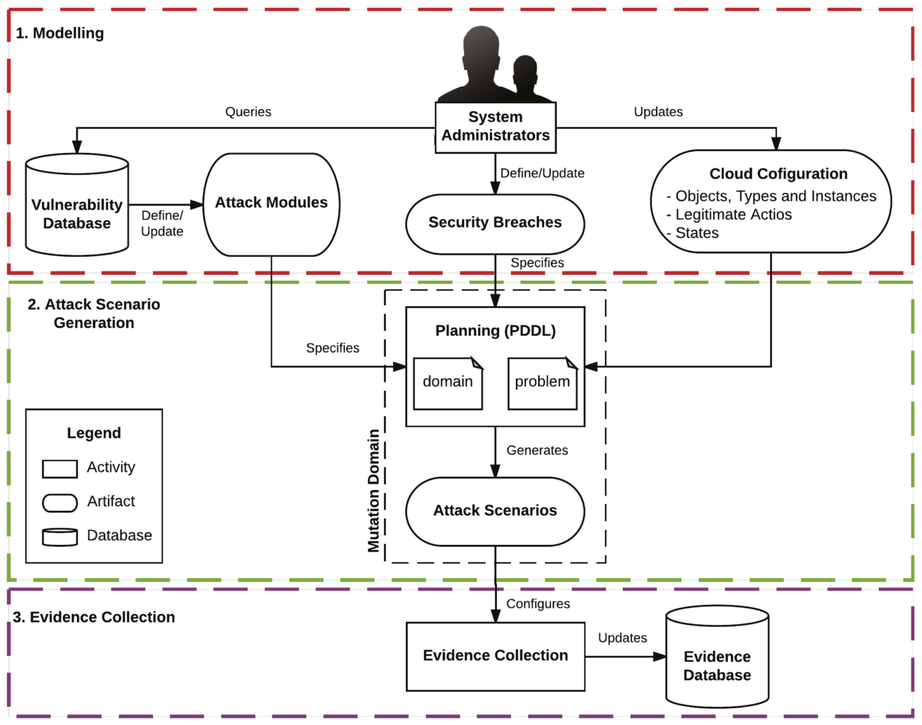
» **Attack Patterns:** Recreating how an attack was perpetrated can be cumbersome from unfiltered cloud data.

Motivating Example



There is a need for pro-active evidence collection that preserves the relevant data necessary to explain how potential attacks are perpetrated.

2 Approach (1)



1. Modeling

» **Cloud Configuration:** Models object types, object instantiations and their states. Modelled as domain and problem definitions.

» **Security Breaches:** Model possible violations of organisational policies or the regulations of a specific jurisdiction.

» **Attack Modules:** Attack modules leverage known vulnerabilities that are present in existing hosts to define malicious actions that can be performed by an attacker.

3 Approach (2)

2. Attack Scenario Generation

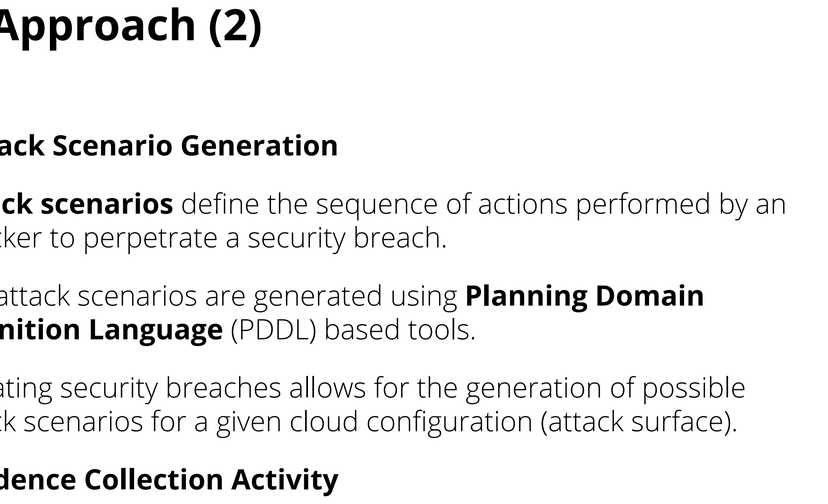
» **Attack scenarios** define the sequence of actions performed by an attacker to perpetrate a security breach.

» The attack scenarios are generated using **Planning Domain Definition Language** (PDDL) based tools.

» Mutating security breaches allows for the generation of possible attack scenarios for a given cloud configuration (attack surface).

3. Evidence Collection Activity

» Log data associated with the actions contained within the attack scenarios is collected as potential evidence, adapting to changes in the cloud configuration



4 Results

» Based on simulation, our approach filters out logs pertaining to 38% of the possible actions performed in the cloud.

» Based on the simulations run, storage overhead was reduced by over 95%.

» The efficiancy of the attack scenario generation was found to **be directly propotional to the complexity of the cloud configuration.**

» Based on the possible security breaches, using mutation techniques, our approach identifies the security breaches that lead to **unique attack scenarios.**

# Clusters	# VMs	# PMs	# Networks	Time (sec)
5	50	15	9	0.10
10	100	30	19	0.87
15	150	45	29	3.7
20	200	60	39	10.13
25	250	75	49	24.55
30	300	90	59	46.79

Table: Scalability Evaluation

# User Actions	Logs Generated	Reduction
10000	6.8 mb	98%
50000	34.1 mb	99%
100000	68.2 mb	99%

Table: Storage overhead reduction

Our approach configures and adapts the evidence collection activity to preserve the evidence that is relevant for a forensic investigation.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SOUTHERN Regional Assembly
Promoting our Region