Resilient Architectures

Measuring Configuration Resistance for Proactive Cyber Resiliency -- Properties & Verification

Mohammed Alsaleh
PI: Ehab Al-Shaer
UNC Charlotte

Why Proactive Resiliency?

Systems Complexity	• Accounting for hidden undiscovered misconfiguration.
Asymmetric Cyber Warfare	• Static & undiscoverable attack surface.
Sophisticated Adversaries	• Uncontrollable margin of evasion.
Attacks are Inevitable	• Managing attacks if they are not prevented.

Resistance for Proactive Cyber Resiliency

The capability of cyber configuration to increase the required *time*, *effort*, *skill*, *resources* and *knowledge* for active attackers to achieve their goals, using static and dynamic *isolation* and *diversity*.

Goals

Resiliency Enforcement Verification

❑ How to ensure that the cyber configuration enforces the isolation and diversity resiliency specification accordingly?

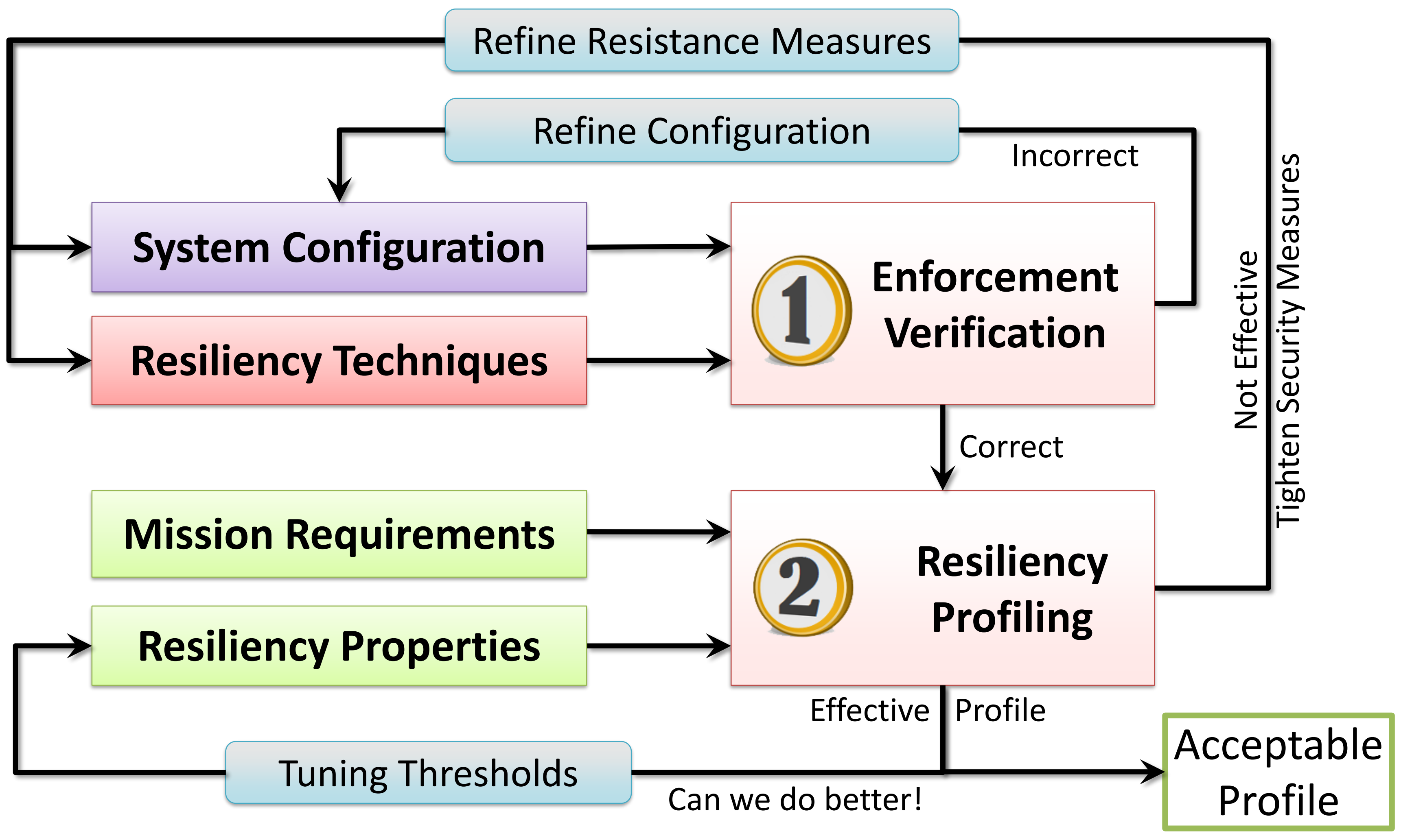
Resiliency Profiling for Validation

❑ Even if configured properly, are your techniques **effective** against sophisticated **attacks**?

❑ Your configuration is **evolving**, but is it becoming **more or less resilient**?

Verify Various Resiliency Properties
Even if a *random* set of machines are **infected** by a worm, the worm will **NOT propagate** to more than **20%** of the network.
The network infrastructure always **allows critical services to communicate** even if **50%** of critical links are attacked by DDoS (or X% of internal/external/ bots are used).
Even if the authentication key is **compromised**, **these files can not be ex-filtrated.**

Framework



Refine Resistance Measures

Refine Configuration

Incorrect

System Configuration

Resiliency Techniques

1 Enforcement Verification

Correct

Not Effective

Tighten Security Measures

Mission Requirements

Resiliency Properties

2 Resiliency Profiling

Effective

Profile

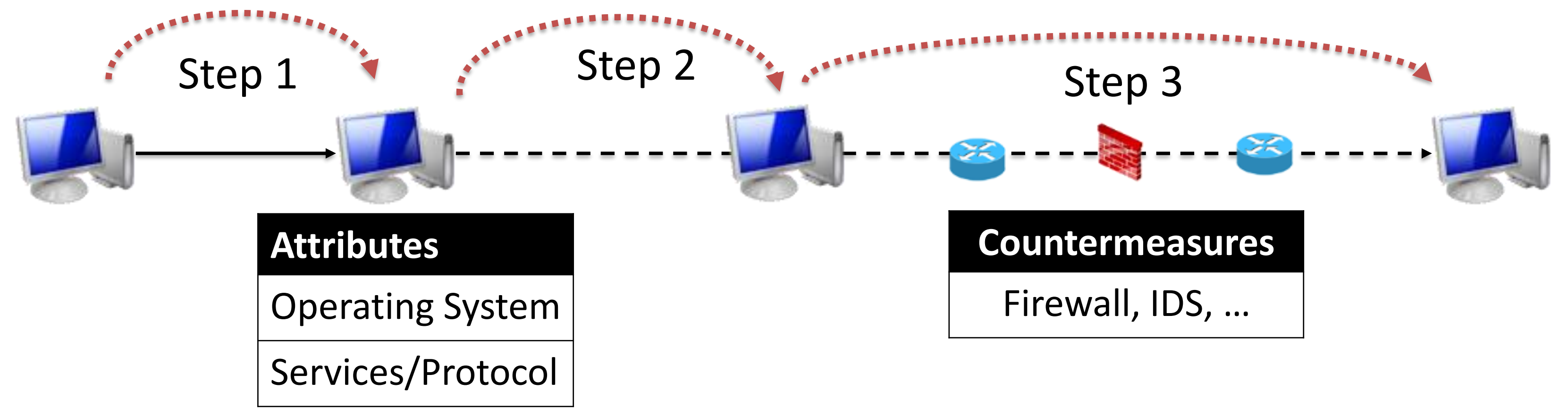
Tuning Thresholds

Can we do better!

Acceptable Profile

Resistance/Resiliency Specification

❑ The **isolation** and **diversity** specification language specifies "what", "where" and "how" isolation and diversity pattern will be enforced in the all paths from sources to destinations.



Examples.

Source	Critical Asset/Dest	Resistance Pattern
DMZ	Database Servers	ESP OR (Filter AND D-Inspect))
Internet	Authentication Server	OS OR Application

Resiliency Profiles Specification

Resiliency Properties Definition

Attack Specification	Mission Requirements
• Attack class (i.e. malware, DoS). • Attack Capabilities, Resources, and Tactics.	• Impact Thresholds. • Operational Reachability, QoS, and Security requirements.

Property. The system can ensure the specified mission requirements even under the specified attack instance.

Resiliency Profile Scoring

⊟ **Profile: Gov-mandated-resiliency**	**Score: 80%**	
Resist high-rate *Slowloris* attack	100	Pass
Protect all *critical DBs* against *Zeus* worm	60	Fail
…	…	…

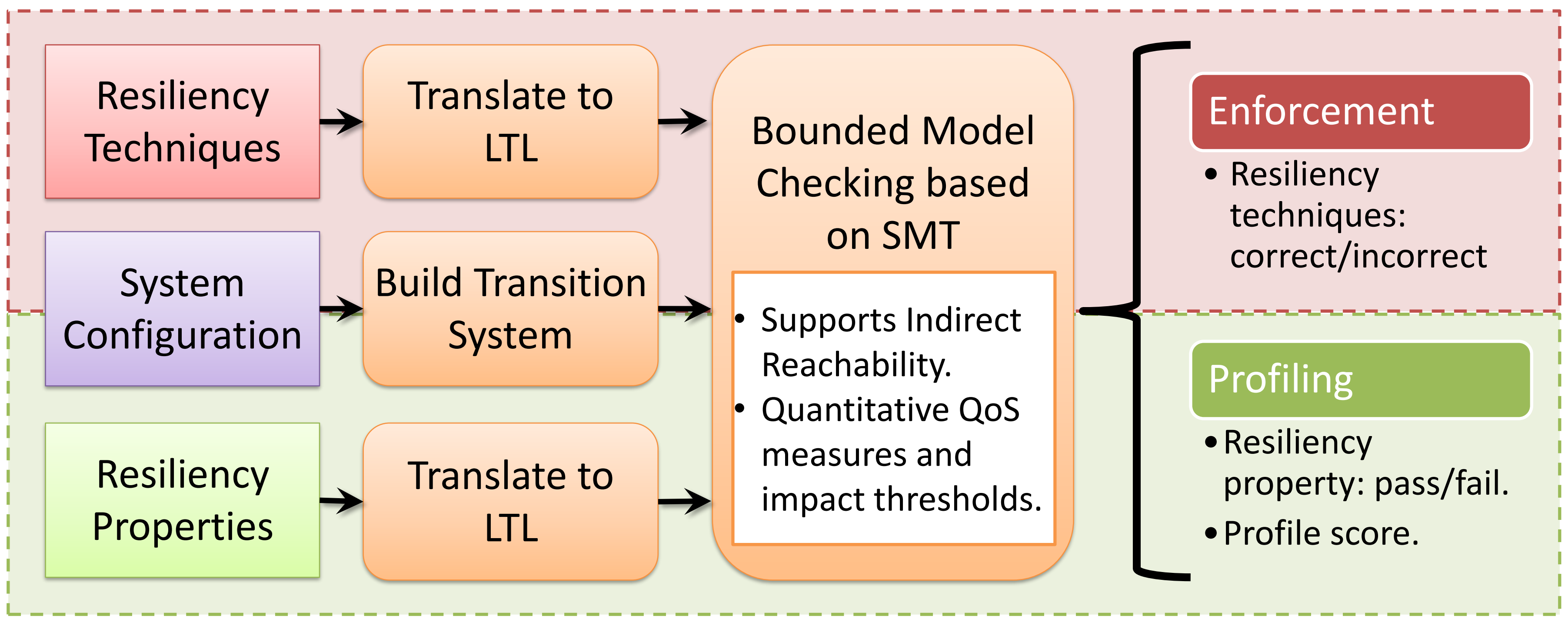
Profile Score

Weighted Resiliency Properties

❑ The **total score** of a profile pr is the weighted sum of the properties that are satisfied normalized to the total weights of all properties.

$$S_{pr} = \frac{\sum w_j \times R_j}{\sum w_j}, \qquad \text{where} \quad R_j = \begin{cases} 0 & \text{Property j } \textbf{failed} \\ 1 & \text{Property j } \textbf{passed} \end{cases}$$

Bounded Model Checking Approach: CyResChecker



Resiliency Techniques → Translate to LTL

System Configuration → Build Transition System

Resiliency Properties → Translate to LTL

Bounded Model Checking based on SMT
- Supports Indirect Reachability.
- Quantitative QoS measures and impact thresholds.

Enforcement
- Resiliency techniques: correct/incorrect

Profiling
- Resiliency property: pass/fail.
- Profile score.

Science of Security Lablet