

# **Angry birding: evaluating application exceptions as attack canaries**

Tolga Ünlü

Lynsay A. Shepherd

Natalie Coull

Colin McLean

This poster was presented at the 6th IEEE European Symposium on Security and Privacy, (EuroS&P 2021), all-digital event, 6-10 September 2021

# Angry { } Birding

Tolga Ünlü, Lynsay A. Shepherd, Natalie Coull, and Colin McLean

Evaluating Application Exceptions as Attack Canaries

“Can we utilize the **trial-and-error** process of **attackers for defence?**”

## Motivation

Successful attacks require multiple **failed attempts**. Exceptions generated in this process could play the role of an **attack canary**, an early warning system.

**Web applications**, to this day, have no **detective defences** as native applications do with techniques such as stack canaries.

**Attacker-induced exceptions** could augment both the security visibility and QA efforts of developers.

## Proposed Approach

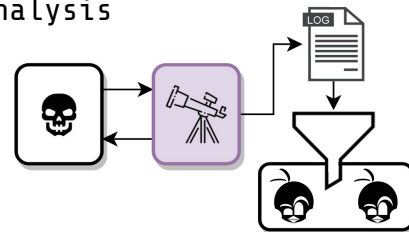
Instrument test applications in a controlled environment to monitor and log attacker-induced exceptions.

Exceptions generated by **data sinks** such as **filesystem**, **network** and **database APIs**.

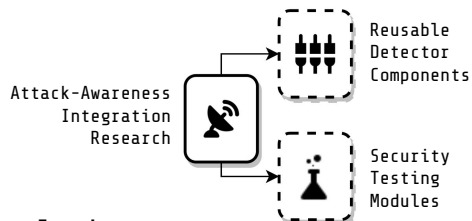
Analyse the recorded exceptions and evaluate the approach:

- \* Scalability
- \* Accuracy
- \* Reproducibility
- \* Effectivity

## Analysis



Assign set of exception combinations to specific attacks or attack payloads



## Outlook

