MICROARCHITECTURAL LEAKAGE TEMPLATES

AND THEIR APPLICATION TO CACHE-BASED SIDE CHANNELS

*Ahmad Ibrahim, Hamed Nemati, **Till Schlüter**,
Nils Ole Tippenhauer, Christian Rossow*

PROBLEM: SIDE-CHANNEL DISCOVERY BY EXAMPLE

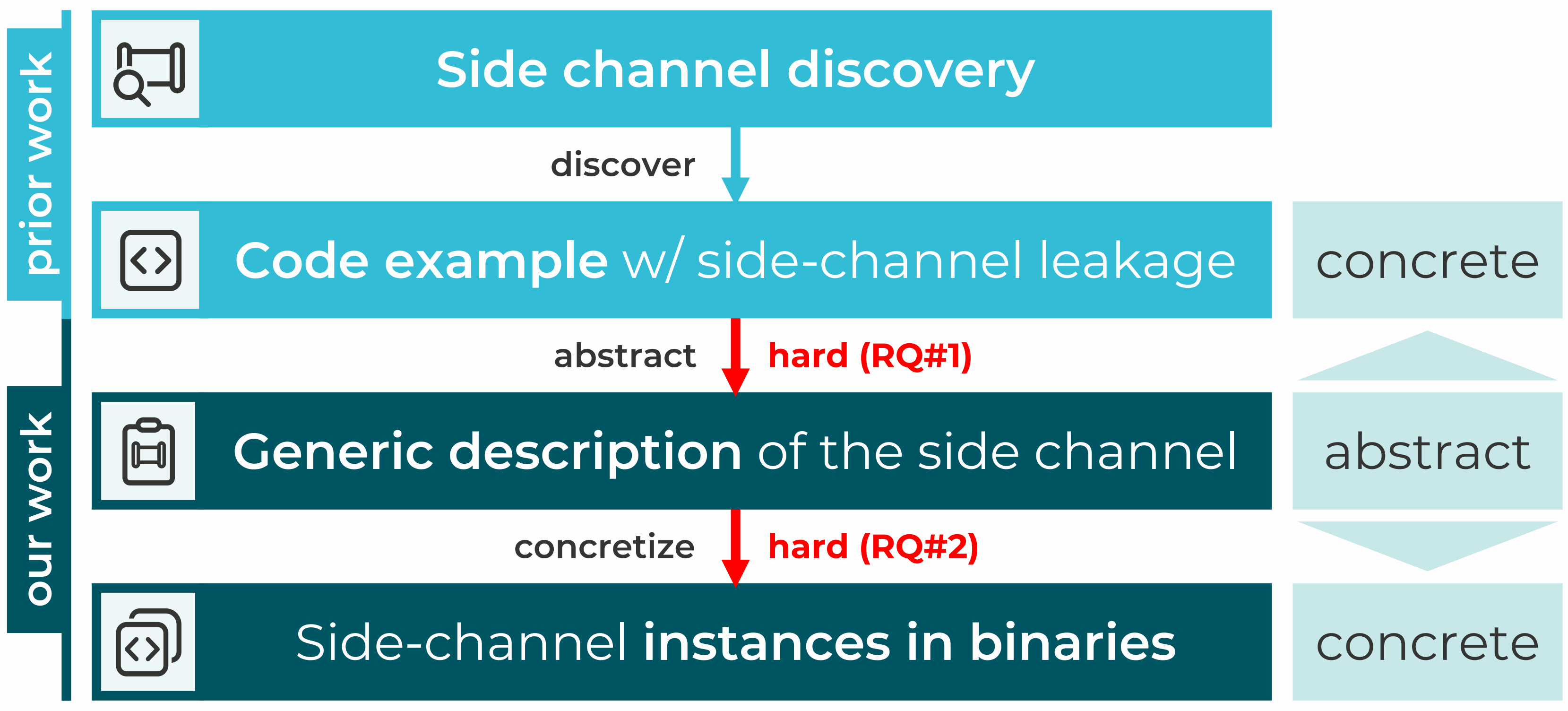
Microarchitectural side channels can be discovered by means of a concrete code example, which shows leakage behavior but does not characterize the side channel in detail.

Research Questions:

- **RQ#1:** How can side channels be specified in a generic way?
- **RQ#2:** How can side-channel instances be identified in binary code?

CHALLENGE: FROM 1 TO *N*

ABSTRACT, THEN CONCRETIZE



CONTRIB.1: LEAKAGE TEMPLATE

GENERIC SIDE-CHANNEL DESCRIPTION

In our definition, a side channel is characterized by three attributes:

- A **code** template
- Distinct **behaviors**
  - *e. g. timing: {fast, slow}*
- **Relations** between inputs, leading to a certain behavior
  - *"When inputs X and Y are in relation, then behavior Z."*

Leakage Template

This is a Leakage Template for a cache-timing side channel:

Code $\mathcal{P}(A)$ — Behavior and Relations

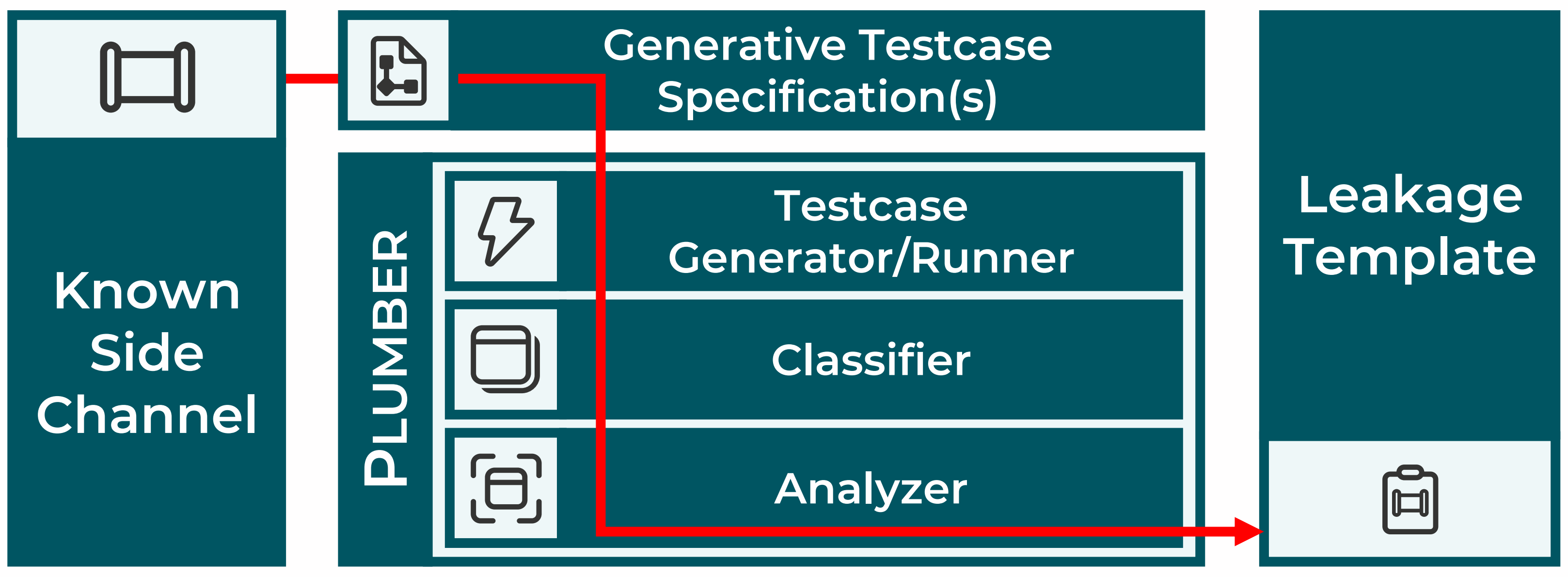
```
ldr x0, [x1]
; ...
ldr x0, [x2]
```

$\mathcal{B}$	$\mathcal{R}(A, b)$
(●) fast	$\texttt{sameTag}(x_1, x_2) \land \texttt{sameSet}(x_1, x_2)$
(○) slow	$\neg\texttt{sameTag}(x_1, x_2) \lor \neg\texttt{sameSet}(x_1, x_2)$

CONTRIB.2: PLUMBER

FROM EXAMPLE TO LEAKAGE TEMPLATE

Our open-source framework PLUMBER facilitates the process of creating a Leakage Template:


Known Side Channel
Generative Testcase Specification(s)
PLUMBER
Testcase Generator/Runner
Classifier
Analyzer
Leakage Template

CONTRIB.3: CASE STUDIES

3 LEAKAGE TEMPLATES

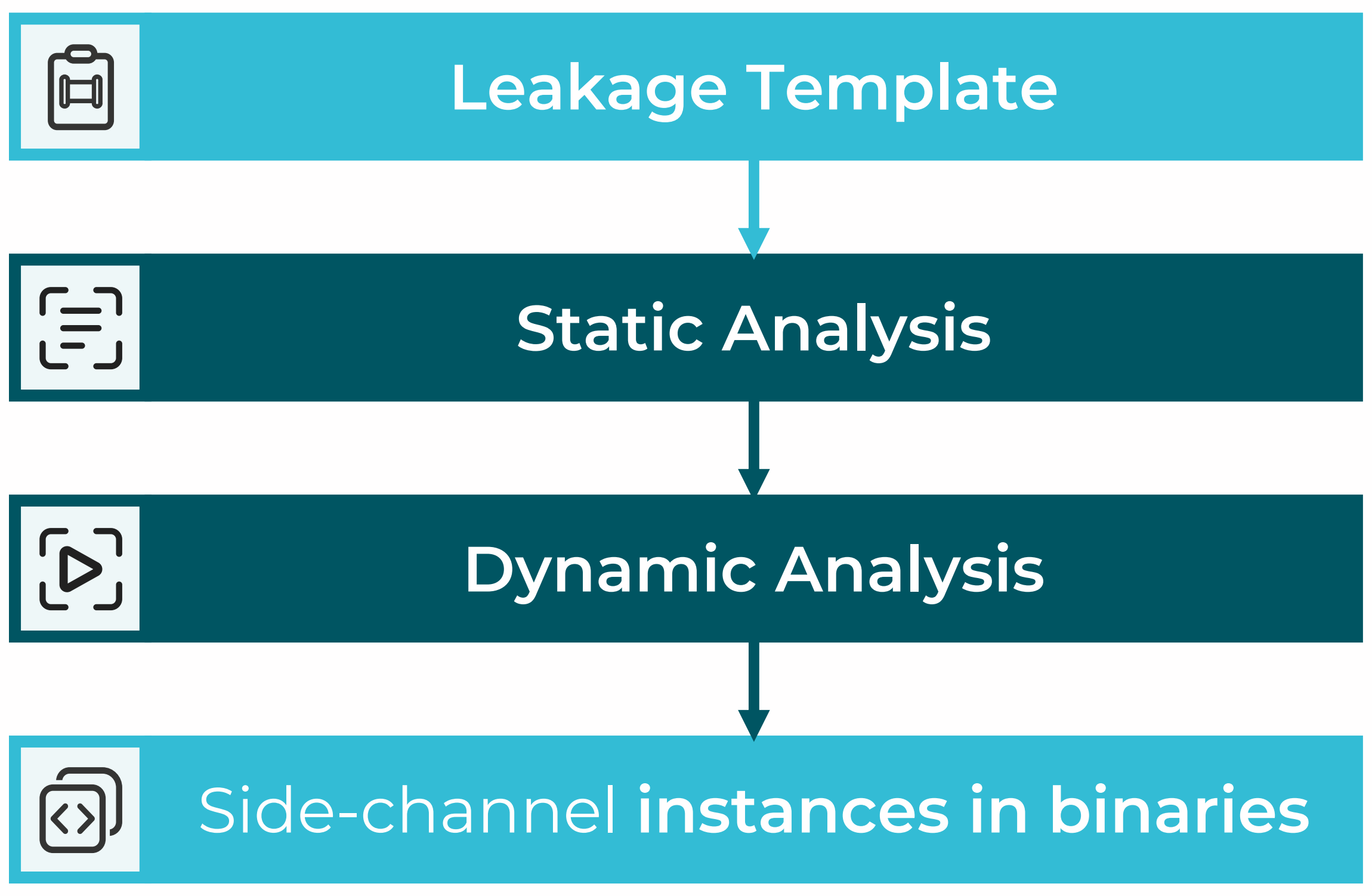
We present 3 Leakage Templates:

- **Previction Side Channel**
- **Prefetching Side Channel**
- **Cache Eviction**

We evaluate 4 covert channel attacks that we derive from these Leakage Templates.

CONTRIB.4: BINARY MATCHING

FROM LEAKAGE TEMPLATE TO INSTANCES



As a case study, we re-identify a prefetching-based side-channel vulnerability in OpenSSL 1.1.0g.

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

This poster is based on the following publication:

[1] Ahmad Ibrahim, Hamed Nemati, Till Schlüter, Nils Ole Tippenhauer, Christian Rossow, "Microarchitectural Leakage Templates and Their Application to Cache-Based Side Channels"
2022 ACM SIGSAC Conference on Computer and Communications Security **(CCS '22)**