eShard — Scaling Security Testing

Open API for Trace Data Formats

Overview of the Ecosystem

Libraries currently in use

No standard for SCA trace storage | Dataset formats | File formats

Existing libs: estraces, trsfile (python, java, julia), chipwhisperer, lascar, scarr, ...

Dataset formats: ets, trs, numpy, chipwhisperer cwp, lascar containers, scarr containers, ...

File formats: hdf5, zarr, sqlite, bin, .npy npz, .trc, ...

→ Highlights the need for unified API to access trace data.
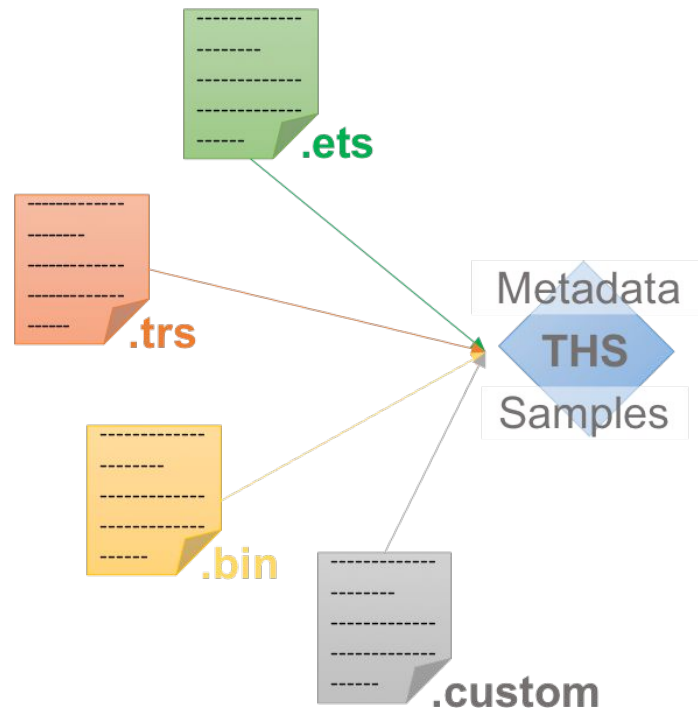   **Dataset abstraction**

Agnostic Dataset Abstraction

Benefits of an open API

The goal is to build an API that is format independent.

Analysis toolkits leveraging this API can handle many types of data format **transparently.**

→ Enable analysts to feed any kind of dataset without conversion hurdle.

Agnostic Dataset Abstraction

How to efficiently make the data available

1) Separate dataset management from analysis toolkit   → estraces
2) Define common view for all datasets (may evolve)   → THS object
3) Define what is a trace   → Trace object

Unified and straightforward usage

```python
import estraces

ths = estraces.read_ths_from_<format>()

traces_chunk = ths.samples[100:200, 1000:2000]
```

4) Implement THS readers for various formats → ets, trs, bin, sqlite, numpy, random… Map the data model to the view

5) Let people write custom reader classes for their **own** formats…

Common API requirements

Core must-have features

Limited number of requirements

- Load traces and their metadata consistently

- Slice in number of traces (batch)

- Slice time-window (frame)

- Type handling (including big integers)

- Proper memory management - memmap/out-of-core, dynamic chunk size depending on the machine resources.

Nice to Have Features

Decide if in Common API or Low-level formats ?

Fancy indexing
(not continuous)

Multi-channel

Composition of datasets
(concat, subset, filter)

Integrity
Confidentiality

Support
global metadata

Compression

Support
heterogeneous metadata
(e.g. images)

Read buffering
Async operations

Type cast
conversion

Multilang support
(libs, docs, users...)

Dataset
Writers

Thank you.
Any questions?

✉ contact@eshard.com

🌐 www.eshard.com

in /company/eshard

𝕏 @eshard

France HQ

Bâtiment GIENAH
11 avenue de Canteranne
33600 Pessac, France

France R&D

7 rue Gaston de Flotte
13012 Marseille, France

Singapore

#03-07 Jit Poh Building
19 Keppel Road
Singapore 089058

eShard