TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Institut für Computertechnik
Institute of Computer Technology

CHEF: A Configurable Hardware Trojan Evaluation Framework

10th Workshop on Embedded Systems Security (WESS 2015)

Christian Krieg and Daniel Neubacher

October 8, 2015

Hardware Trojans

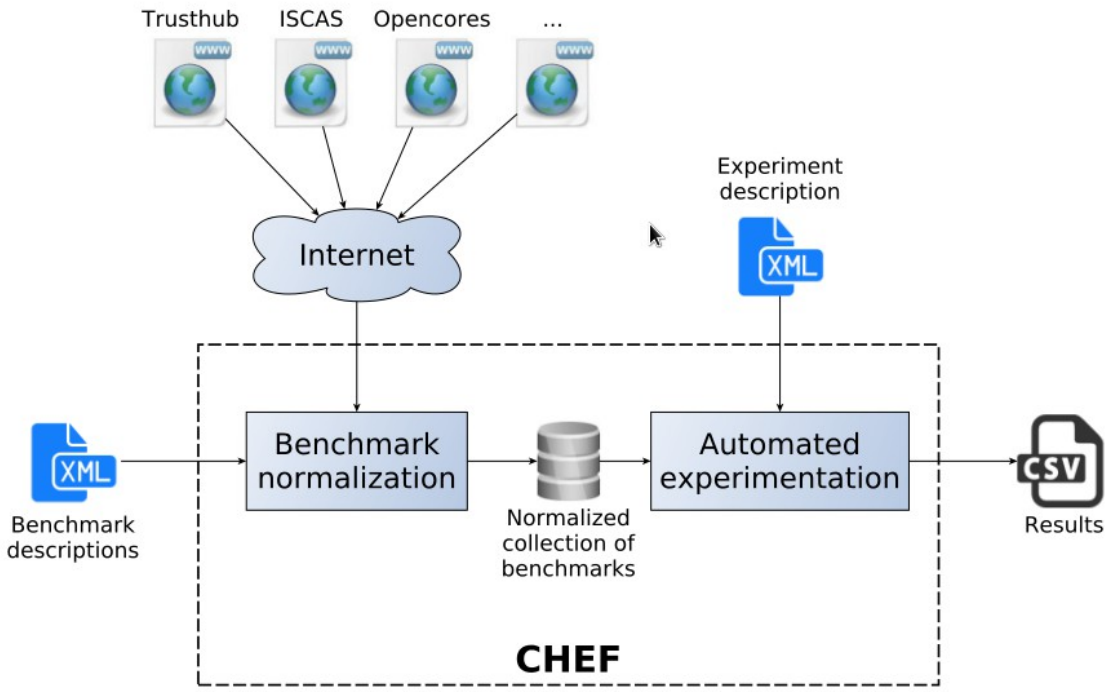
- System with malicious functionality
  - undocumented
  - unspecified
- Components
  - Trigger (time bomb, counter, temperature, ...)
  - Payload (leak data, back door, ...)
- System compromise
  - Design
  - Manufacture

Detecting HW Trojans at design level

- Verification and Test
- Methodologies proved with experiments
- Using benchmark designs (e.g., TrustHUB[1])
  - Download and install: time-consuming procedure
  - Designs can be buggy
  - Designs require individual tool chain

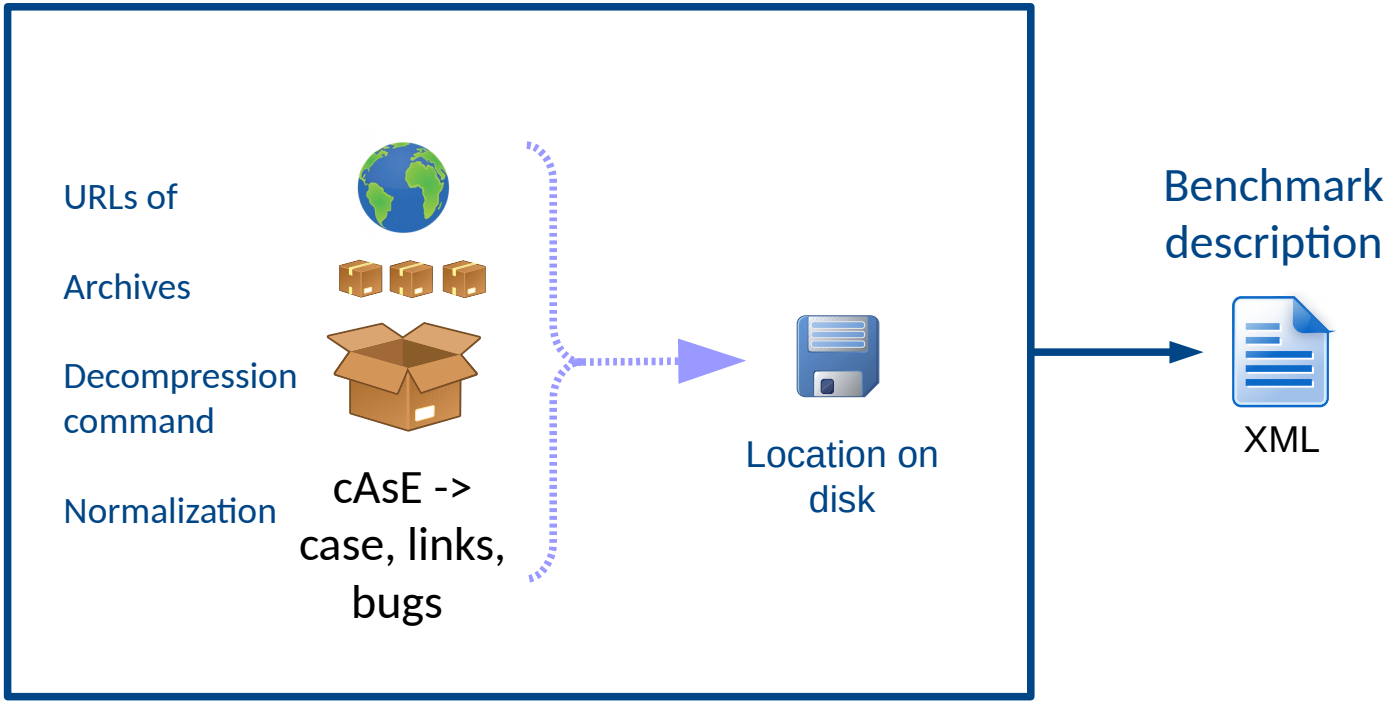
[1] https://www.trust-hub.org/taxonomy

CHEF: An outline



XML: Extended markup language
CSV: Comma-separated values

CHEF: Part 1 -- Benchmark description



XML: Extended markup language

CHEF: Part 1 -- Benchmark description

```
<benchmark>
  <archive>
    <checksum type = " sha256 " > HASH </checksum>
    <url> https://www.trust-hub.org/index.php/.../EthernetMAC10GE-T720.part01.rar </url>
  </archive>
  <archive>
    <checksum type = " sha256 "> HASH </checksum>
    <url> https://www.trust-hub.org/index.php/.../EthernetMAC10GE-T720.part02.rar </url >
  </archive>
  <decompress> unrar x EthernetMAC10GE-T720.part01.rar </decompress>
  <normalize>
    #!/ bin / bash
    find . - depth - exec rename 's /(.*) \/([^\/]*) /$1\/\ L $2/ ' {} \;
  </normalize>
<benchmark>
```

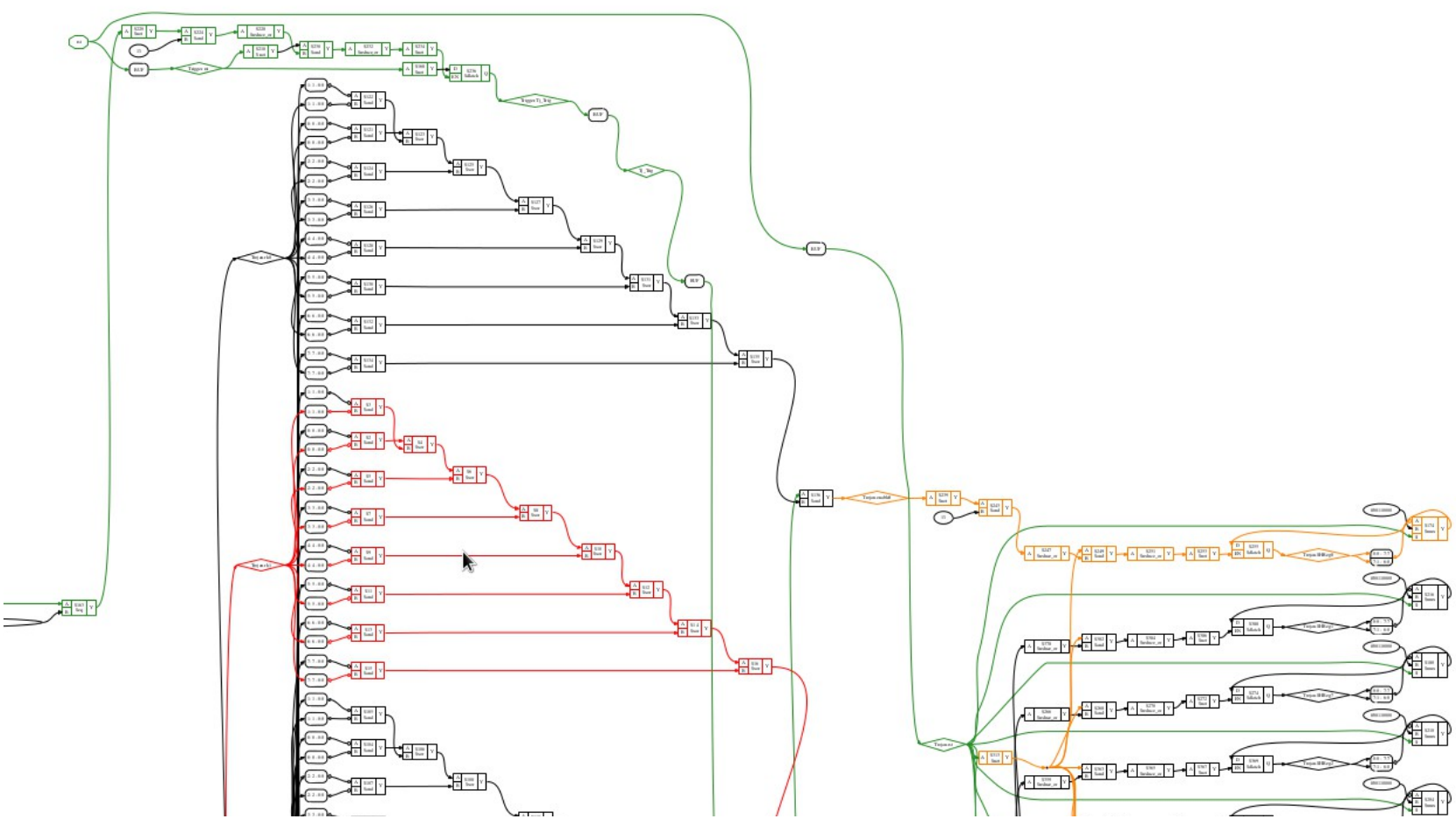
Archive part 1

Archive part 2

Extract

Normalization

CHEF: Part 2 -- Trojan insertion



CHEF: Part 2 -- Trojan insertion

Malicious functionality also part of benchmark description

<benchmark>

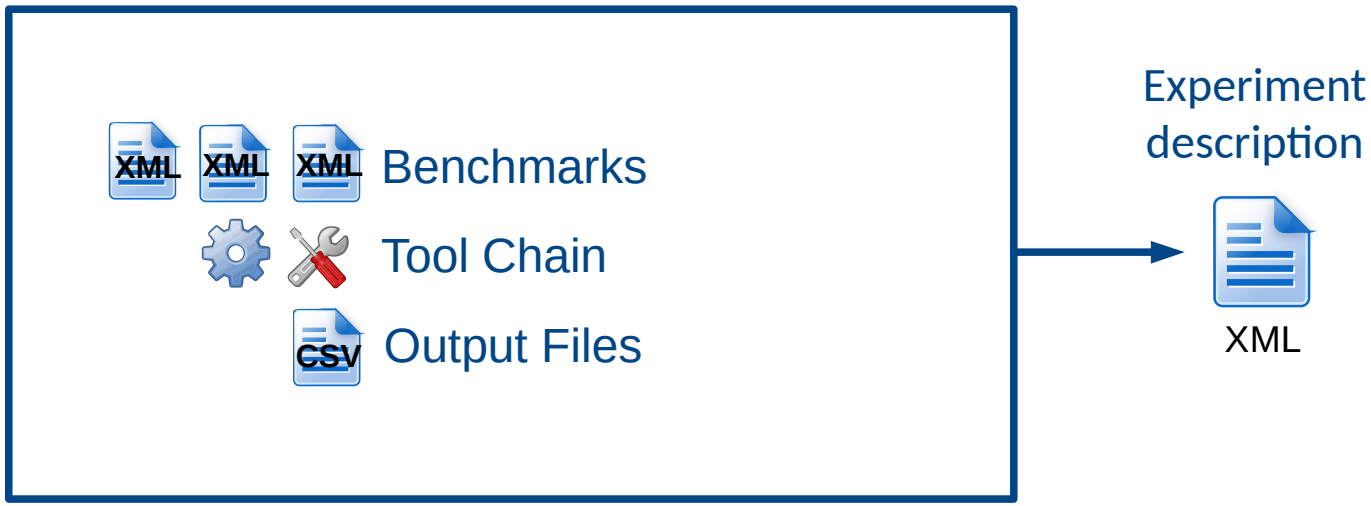
```
<trojan>
  <trojan_description>
    Whenever a predefined input plain text is observed, the Trojan demonstrates an
    attack on the AES-128 block-cipher [...]
  </trojan_description>

  <trojan_patch>
    diff -rupN trojanfree/xge_mac_scan.v trojaninserted/xge_mac_scan.v
    --- trojanfree/xge_mac_scan.v       2015-08-20 09:02:18.827949923 +0200
    +++ trojaninserted/xge_mac_scan.v              2015-08-20 09:02:18.871949924 +0200
    [...]
    +  // Trigger ----------------------
    +    AND2X1 Trojan1 (.IN1(n22798), .IN2(n130965), .Q(Tj_OUT1));
    +    AND2X1 Trojan2 (.IN1(n130261), .IN2(n131096), .Q(Tj_OUT2));
    +    AND2X1 Trojan3 (.IN1(n130129), .IN2(n131471), .Q(Tj_OUT3));
    +    AND2X1 Trojan4 (.IN1(n131545), .IN2(n130687), .Q(Tj_OUT4));
    [...]
  </trojan_patch>
</trojan>
```

</benchmark>

Example taken from www.trust-hub.org, Trojan: EthernetMAC10GE-T720

CHEF: Part 3 -- Experimentation



CHEF: Part 3 -- Experimentation

```
<workbench>
  <eval_script>
    yosys -s trojan-detection.ys
  </eval_script>
  <results_dir>results</results_dir>
  <results_file>trojan-detection_results.csv</results_file>
  <benchmark>
    <uid>c13c5ccf-04d3-44f9-853e-06380e4dc422</uid>
    <path>benchmarks/xml</path>
  </benchmark>
  [...]
  <benchmark>
    <uid>2f8d2253-2edd-4323-bf75-bfaeee2cb743</uid>
    <path>benchmarks/xml</path>
  </benchmark>
</workbench>
```

Tool Chain

Results Directory

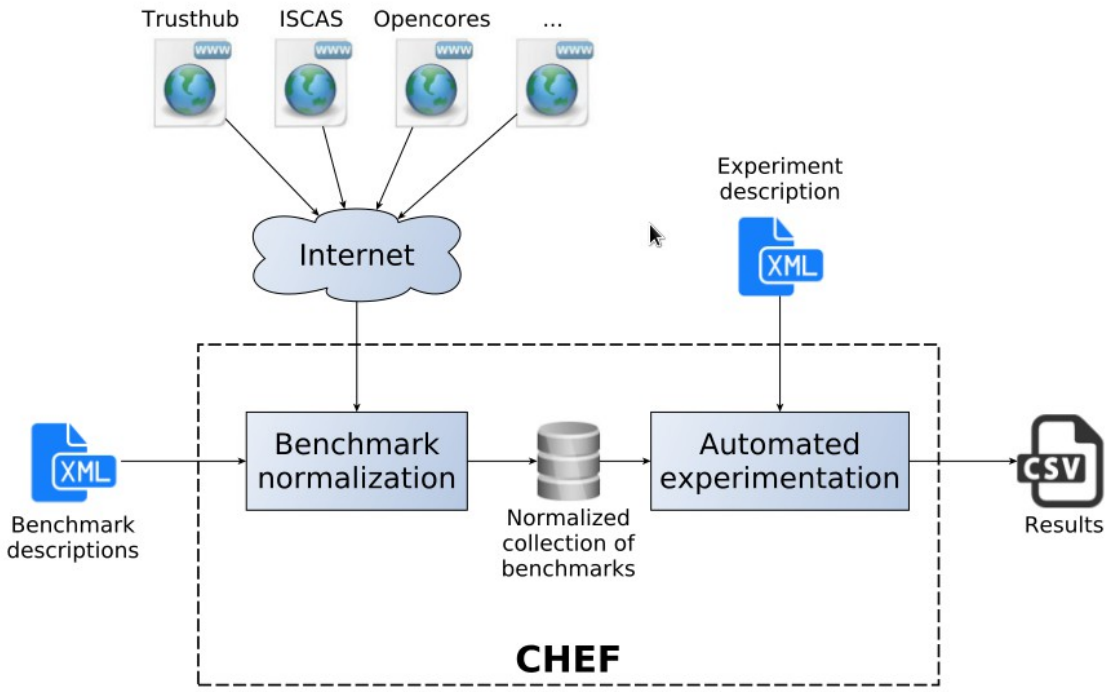
Results File

Benchmark 1

...

Benchmark n

CHEF: Putting it all together



Current state of development

- **Early-beta** command-line version available
- Basic set of **language** features
- Basic **documentation** (man-page like)
- Now we need **feedback** by the community

= YOU!

Source: https://upload.wikimedia.org/wikipedia/commons/1/1d/Unclesamwantyou.jpg

Getting the CHEF

https://github.com/shape-ht/chef

Conclusion, future work

- With CHEF, it is possible to **reproduce experiments**
- Thus, it **allows comparison** of different approaches
- Future: RSS-like Trojan benchmark **notification**
- Future: **GUI** to the CHEF

https://github.com/shape-ht/chef

RSS: Rich site summary, GUI: Graphical user interface

Contact us!

- Christian Krieg
  Project Lead
  christian.krieg@alumni.tuwien.ac.at
  +43 1 58801 38464

- Daniel Neubacher
  Development
  neubacher@ict.tuwien.ac.at
  +43 1 58801 38423

https://github.com/shape-ht/chef