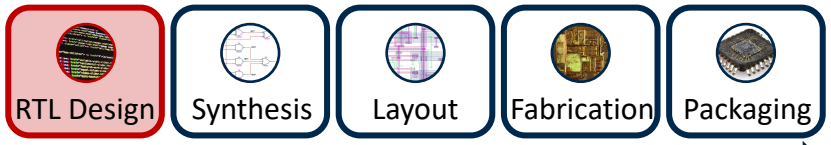
Bomberman: Defining and Defeating Hardware Ticking Timebombs at Design-time

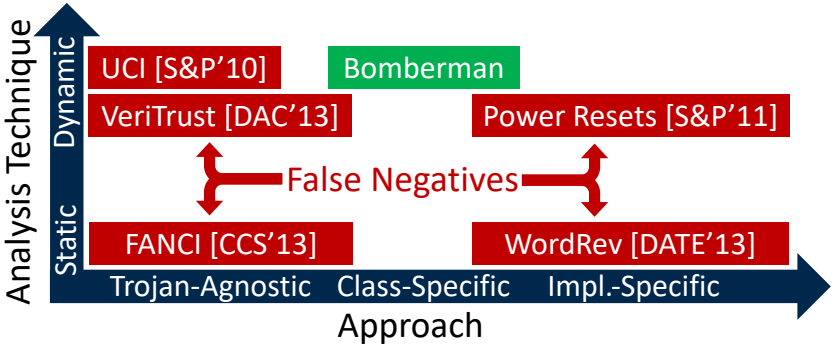
Timothy Trippel, Kang G. Shin, Kevin B. Bush, and Matthew Hicks

Problem



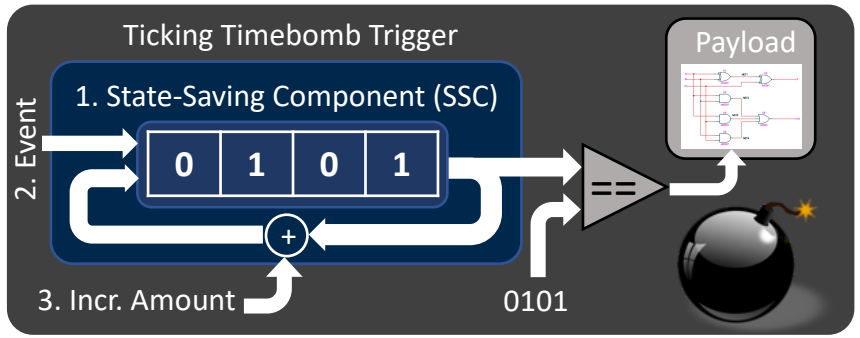
To cope with increased heterogenous on-chip parallelism, and minimize their time-to-market, most semiconductor companies *outsource* portions of the design process by purchasing 3rd party IP to include in their designs. *Outsourcing presents a security risk*: How do we know untrusted 3rd parties will not include hardware Trojans in their designs?

Vetting Untrusted 3rd Party IP



Existing design-time Trojan detection methods suffer from *false negatives* (i.e., Trojan designs that bypass these defenses). Bomberman strikes a balance in detection capabilities, *detecting a specific class of Trojans (Ticking Timebomb Trojans, or TTTs)* according to their behavior, not implementation.

Ticking Timebomb Trojans (TTTs)



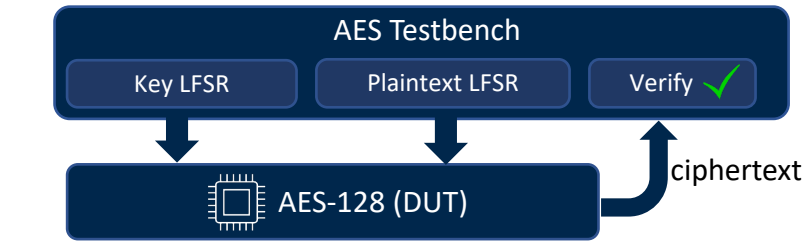
We define TTTs as Trojans with sequence counter Triggers that monotonically approach activation. Moreover, we define these counters by their behavior, namely they: ***1) never repeat*** and ***2) never complete***. Such Triggers are implemented using three components: 1) SSC, 2) Increment Event, and 3) Increment Amount. To identify any TTT design, all we must track are SSC values!

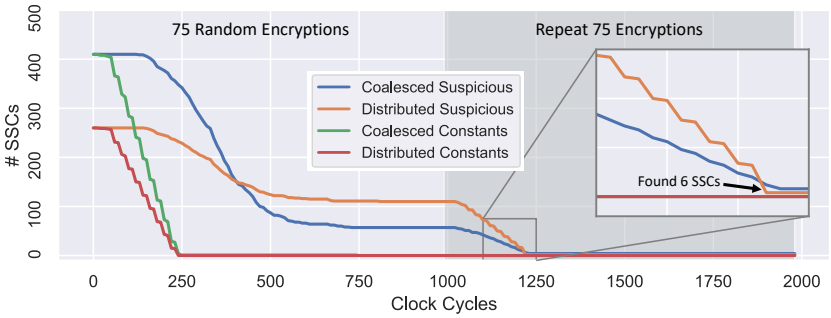
Bomberman

1. Enumerate all SSCs in the RTL
2. Assume all SSCs are *suspicious* (False negatives are impossible!)
3. Simulate the design
4. Check if SSCs violate either TTT invariant during sim.

Evaluation

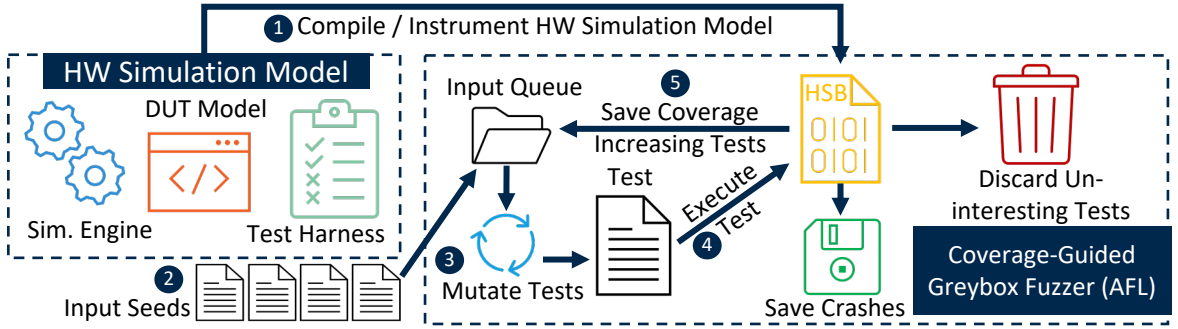
We implant six TTTs into an AES core and analyze it with Bomberman. We use a Constrained Random Verification (CRV) approach to exercise the core.





Future Directions (Fuzzing HW Like SW)

Minimizing false positives is ***manual***. We must tune test vectors to minimize false positives by causing repeated values. ***Could we automate this?***



DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work that was partially supported by: 1) the Under Secretary of Defense for Research and Engineering under Air Force Contract No. FA8702-15-D-0001, 2) the US National Science Foundation under Grant CNS-1646130, 3) the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE 1256260, and 4) the US Army Research Office under Grant W911NF-21-1-0057. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the funding agencies.