SAND2017-9378C

Modeling and Analysis of the Impact of Diversity in Digital Circuits on Attackers

Jason Hamlet and Jackson Mayo, Sandia National Laboratories, USA

Diversity and redundancy in hardware and software systems have previously been studied as a means of enhancing the security of systems by limiting the impact of vulnerabilities in those systems. Diversity in implementation can eliminate some vulnerabilities and make it uncertain whether a given implementation will have a particular vulnerability [1]. We consider the more general scenario of an attacker purposefully inserting Trojans or other malicious artifices. Additionally, the presence of an active attacker may impact statistical assumptions about whether a particular implementation contains a particular vulnerability. Diversity is of interest because, while some properties of a system's design can be proved exhaustively [2], other "incidental" vulnerabilities still exist due to the particular way the system is implemented (and possibly subverted) at a lower level [3]. The only existing general technique to quantifiably mitigate such remaining, a priori unknown vulnerabilities is to disrupt adversaries' ability to analyze and attack a specific implementation at their leisure, by introducing design elements that are random or otherwise cannot be anticipated by the attacker. This is known as a moving target. The case we focus on here is voting several diverse implementations of the same function, so that a majority must be compromised simultaneously to successfully attack the system. There is broad evidence from previous work that moving target, including diverse voting systems, can increase the difficulty of attacks [4].

Our focus is on practical aspects of using diversity to reduce the utility of hardware Trojans. We place our emphasis on design-time constructs. Such approaches can be repeated from design to design and are relatively easily implemented and studied when compared to incorporating diversity during other portions of the lifecycle, such as fabrication. We also have broad control over our own design processes. It is also likely that design-time diversity can be automated, reducing the impact of diversity on system designers. To incorporate design-time diversity we need to identify frameworks for incorporating diversity into our systems and methods for creating that diversity.

We have developed formal models for abstractly studying the impact of various methods of incorporating diversity into circuit designs, and have used these to craft probabilistic expressions for studying the utility of the approaches over a range of conditions. We begin with a routing model in which data is processed from the input to the output of a circuit through several "tiers" of subcircuits. For example, tiers may represent pipeline stages or distinct processing units. If we permit several diverse implementations of each tier then we obtain a diversity of potential processing paths. A single path is realized by selecting one unit from each tier. The attack succeeds if any unit in the selected path has been subverted. Data can be

processed along more than one path in parallel to create a diverse voting system. By taking a majority vote on the output of the distinct paths we can ensure that the output of the voter is correct as long as fewer than half of the paths contain a subverted unit. This initial analysis assumes that only one node in the system is compromised. If two or more distinct processing paths pass through the same vulnerable node, then we interpret this as a common-mode failure in which insufficient diversity was applied to restrict the subversion to a single implementation. We present a probability relation that models this scenario.

We next present a model in which the circuit is again divided into a number of components, each of which can be diversified. We consider the scenario in which three diverse implementations of the circuit are constructed and the output of the circuit is voted on, which is conceptually similar to the previous model, in addition to the scenario in which individual subcircuits are diversified and the subcircuit outputs are voted on locally. We then generalize the second scenario to one in which only a subset of the subcircuits is diversified. We present probability relations for these models.

Finally, we consider a moving target model in which the attacker must be successful at least m times within n tries for the attack to succeed, and in which the system is modified after each attacker attempt. We present a broadly applicable probability relation to model this scenario.

For each of these models, we provide abstract hardware architectures that realize the modeled system. Future work will implement these architectures so that we can augment our probabilistic understanding of their benefits with an experimental understanding of the cost, speed, and power overheads required to implement them.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

1. Allan, Benjamin A., et al. "The Theory of Diversity and Redundancy in Information System Security: LDRD Final Report." (2010). SAND2010-7055.
2. Jean-Francois Monin. Understanding Formal Methods. Springer, 2003.
3. Robert C. Armstrong and Jackson R. Mayo. Leveraging complexity in software for cybersecurity. In Proc. 5th Cyber Security and Information Intelligence Research Workshop, 2009.
4. Daniel Williams., et al. Security through diversity. IEEE Security & Privacy, 7(1):26–33, 2009.