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

Sandia National Laboratories

Jason Hamlet, Jackson Mayo

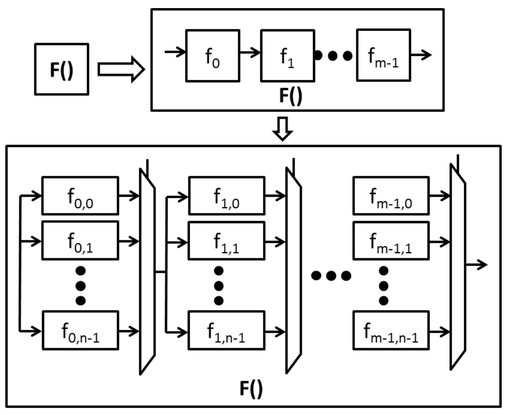
Sandia National Laboratories, Albuquerque, New Mexico and Livermore, CA, USA

Introduction

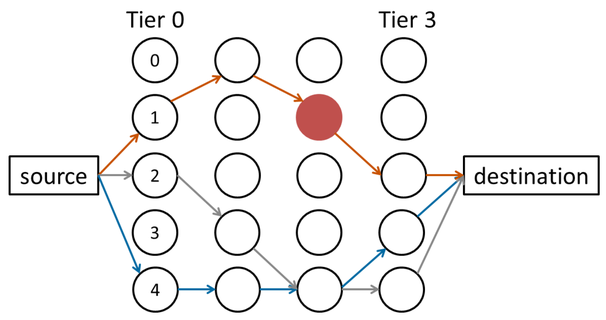
- Diversity in implementation can eliminate some vulnerabilities and make it uncertain whether a given implementation will have a particular vulnerability [1].
- The only general, quantifiable technique for eliminating a priori unknown vulnerabilities is to introduce design elements that cannot be anticipated by the attacker.
- We focus on voting amongst diverse implementations of the same function
- We have developed formal models for studying diversity, and have crafted probabilistic expressions for studying the utility of the approaches

Routing Model

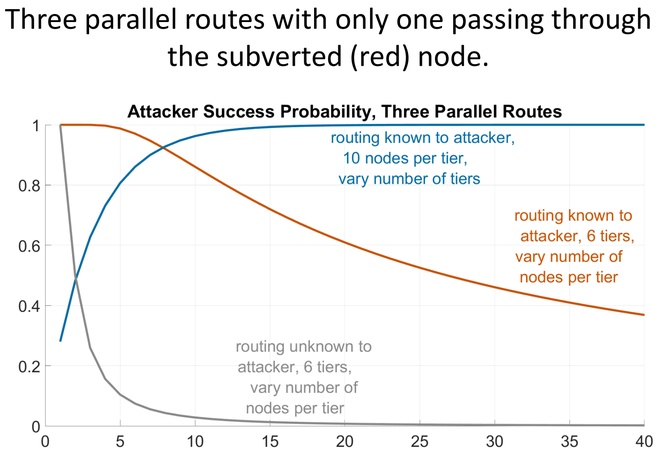
- Data is processed from source to destination through tiers of subcircuits. Several diverse implementations of each tier are available, and a subset of these is used to implement the circuit.
- A single route is realized by selecting one unit from each tier. The attacker succeeds if any unit in the path is subverted. We assume that the attacker can subvert only one node.
- We can also process along several parallel paths and vote on the output.



In hardware we find a disjoint decomposition of the circuit, create diverse versions of each subcircuit, and choose a subset of these to implement the function



Three parallel routes with only one passing through the subverted (red) node.



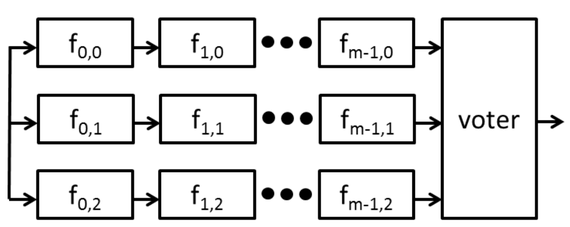
- If the attacker knows the routing, the probability of attacker success, *P(s)*, for a single route is 1 and for three routes is

$$P(s) = 1 - \left(1 - n\left[\binom{3}{2}\left(\frac{1}{n}\right)^2\left(1-\frac{1}{n}\right) + \left(\frac{1}{n}\right)^3\right]\right)^m$$

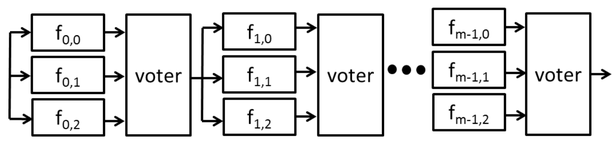
when there are *m* tiers and *n* nodes per tier. If routes are unknown to the attacker then *P*(*s*) for one route is $\frac{1}{n}$ and for three routes is $\binom{3}{2}\left(\frac{1}{n}\right)^2\left(1-\frac{1}{n}\right) + \left(\frac{1}{n}\right)^3$.

Composition Structures

- The system is decomposed into subcircuits, each of which must operate correctly for the system to operate correctly
- Components are vulnerable to some fraction of the input space. We assume that the composition itself does not introduce vulnerabilities. Under this assumption the "composition of voters" architecture is more secure than the "voter of compositions", but at the cost of more voters

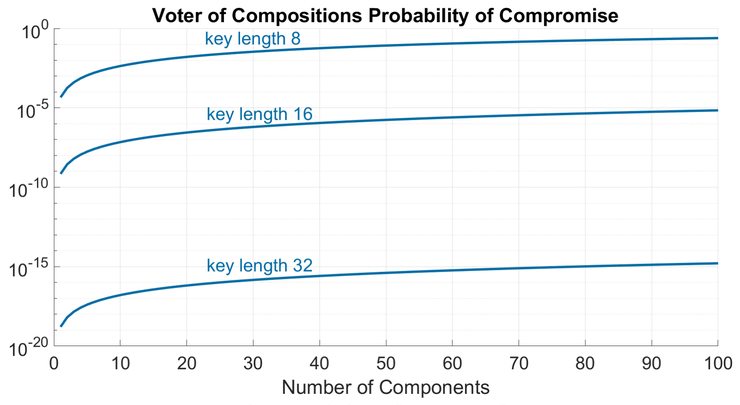


In a "voter of compositions" diverse implementations of the circuit are combined with a majority voter.

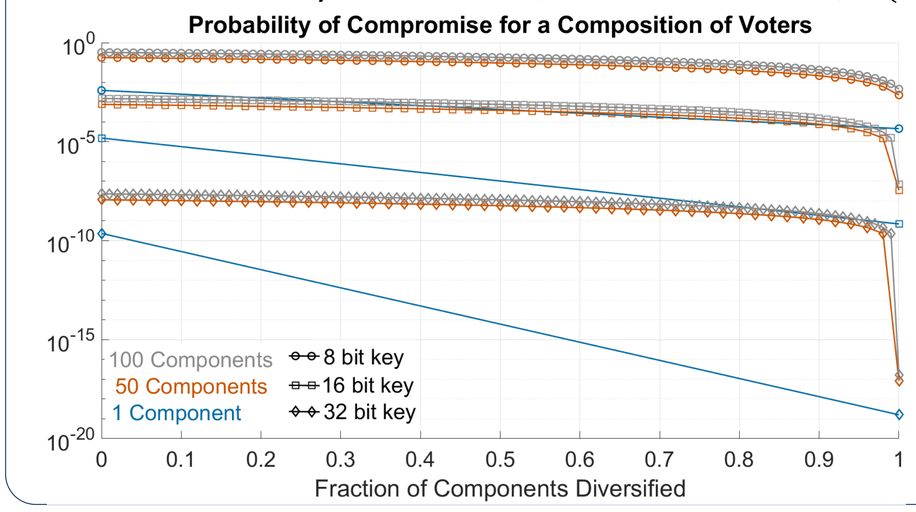


In the "composition of voters" structure diverse realizations of components are voted on locally.

Analysis of Composition Structures



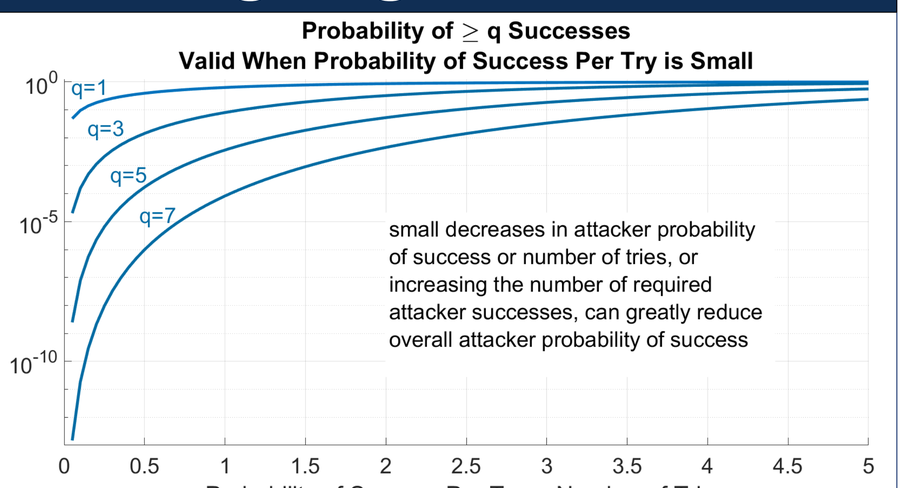
- Consider a system of *m* components that are, on average, vulnerable to a fraction *v* of the system inputs. Assuming the vulnerabilities are triggered by some *k* bit input, $v=2^{-k}$ where *k* is the key length.
- A circuit is vulnerable if any of its components is, so the attacker succeeds with $p=1-(1-2^{-k})^m$. In majority-3 voters, if the failure probability of one realization is *q* then the system fails with $p=3q^2-2q^3$. Combining these, the failure probability for a voter of compositions is $3\left(1-\left(1-2^{-k}\right)^m\right)^2 - 2\left(1-\left(1-2^{-k}\right)^m\right)^3$
- In a composition of voters, let *d* be the fraction of diversified components. Again using the majority voting formula, the probability of incorrect behavior in a diversified component is $3v^2 - 2v^3 = 3\times 2^{-2k} - 2\times 2^{-3k}$ so at least one component behaves incorrectly with $p = 1-(1-3\times 2^{-2k}+2\times 2^{-3k})^{dm}\left(1-2^{-k}\right)^{(1-d)m}$

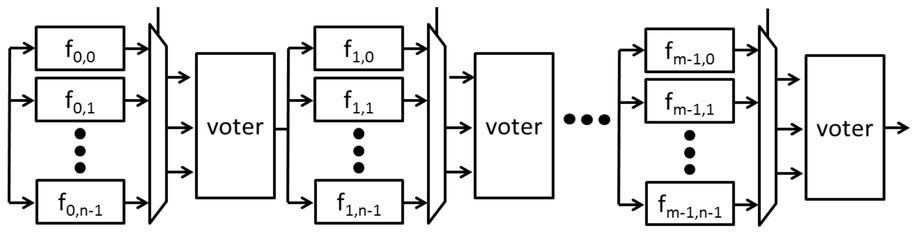


- Particularly when *k* is large, the strongest benefits result from diversifying all components. Even a single undiversified component is the weakest link and reduces the benefit.

Moving Target

In the moving target scenario, the attacker must be successful at least *q* times, and the system is re-randomized after each attacker try. If the attacker tries *N* inputs, each with probability of success *p*, then the number of successes follows a binomial distribution *B*(*N*,*p*). Since *p* is small, we approximate this as a Poisson with parameter $\lambda=Np$. Then the attacker has at least *q* successes with probability $1-\sum_{i=0}^{q-1}\frac{\lambda^i}{i!\,e^\lambda}$





We create a moving target system by providing many diverse implementations of the subcircuits and then changing which of these are used over time. Here, we show a dynamic composition of voters.

Future Work

We are currently implementing these approaches in hardware at different levels of coverage to understand the cost in area, operating frequency, and power required to achieve these reductions in attacker probability of success.

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

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.

SAND2017-12698 C