TODD AUSTIN

PROFESSOR, UNIVERSITY OF MICHIGAN
CEO, AGITA LABS, INC.

DISTRIBUTION STATEMENT A. Approved for public release

MORPHEUS: ADAPTIVE DEFENSES FOR TOMORROW’S SECURE SYSTEMS

This research was, in part, developed with funding from the Defense Advanced Research Projects Agency (DARPA).
The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government.

SECURITY: THE BIG UNSOLVED CHALLENGE

- What we do well:
  - Finding and fixing vulnerabilities
  - Deploying system protections that stop well-known attacks

Valgrind

Synopsys' Coverity Tools

ARM's TrustZone

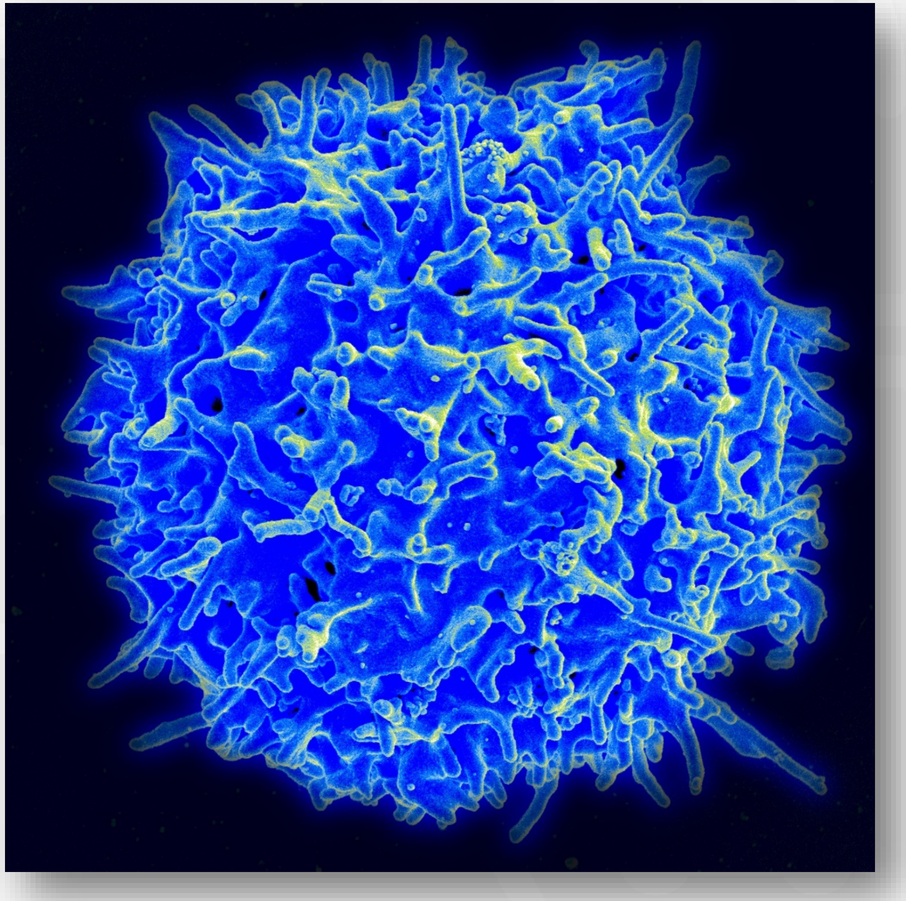
Intel's Control-Flow Enforcement

- Where we fail: ***identifying and stopping emergent attacks***

WHAT IF A SECURE SYSTEM COULD...

1. Respond lightning-fast against common attacks
2. Self-adapt quickly to unknown emerging threats
3. Learn and prioritize the most successful defense strategies
4. Utilize a self-protecting distributed implementation

T-Cell Adaptive Immunity



HUMAN ADAPTIVE IMMUNITY PRIMER

- T-cells receptors discern ***normal*** cells from ***malicious*** cells, via genetic markers

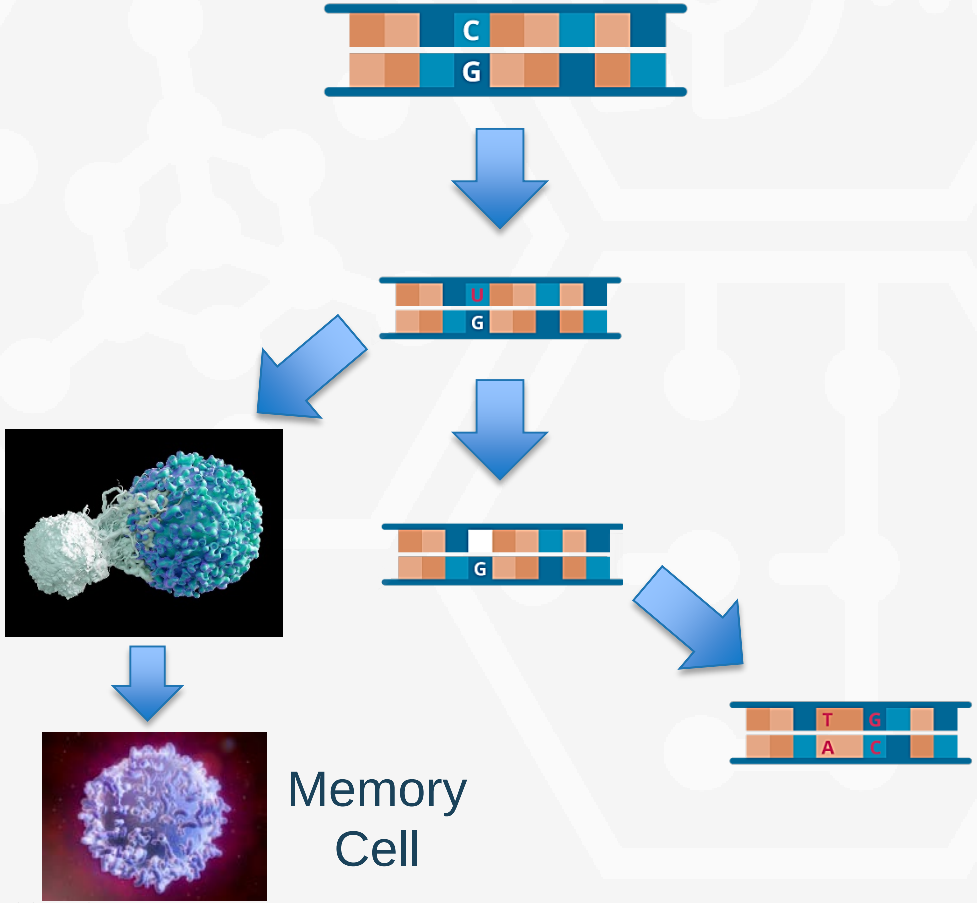
- To stop an unknown disease, T-cells undergo hypermutation that ***randomizes*** T-cell defense capabilities

- Boosted T-cell diversity will likely ***stop the pathogen attack***

- ***Immunological memory records successful T-cell variants*** to speed future recoveries

10^7 T-cell variants

10^{15} possible diseases



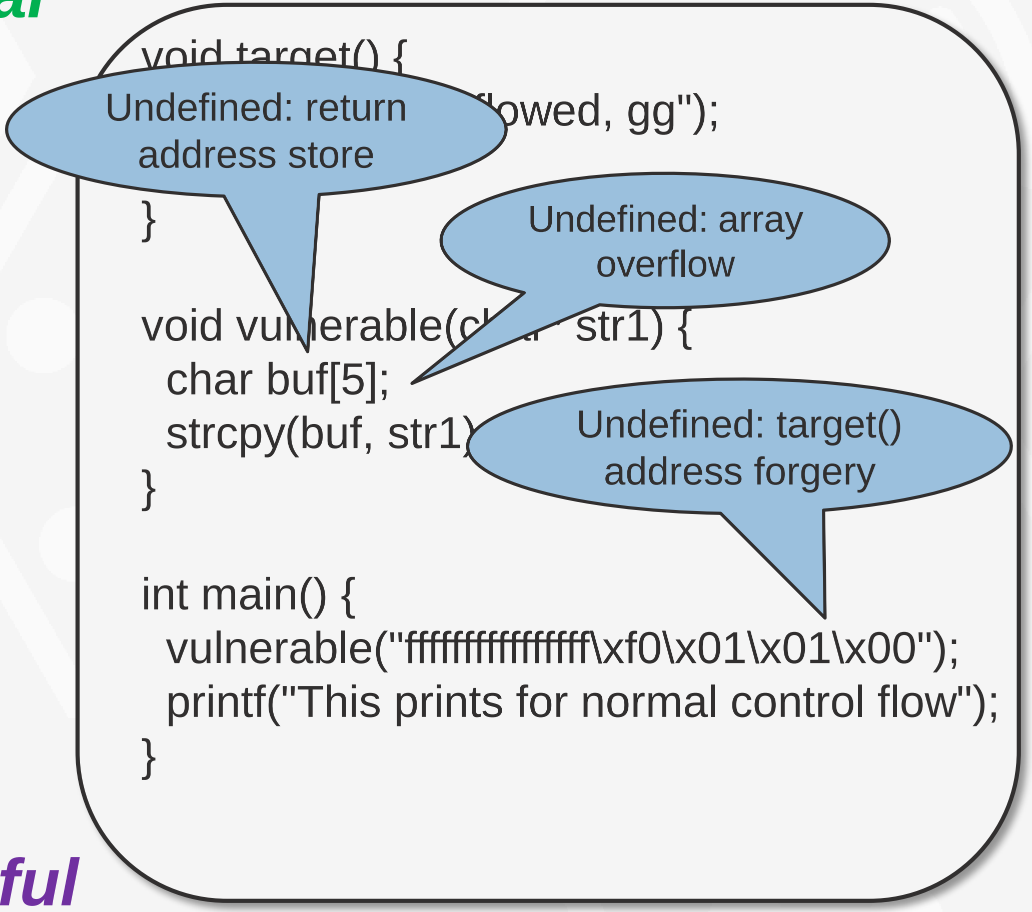
MORPHEUS MIMICS ADAPTIVE IMMUNITY

- Morpheus attack detectors discern ***normal*** code from ***malicious*** code, via undefined semantics

- To stop an unknown attack, Morpheus ***randomizes*** a system’s undefined semantics, a process called “churn”

- Churning undefined semantics ***stops security attacks***

- ***Learning mechanisms record successful defenses*** and stop future attacks quicker

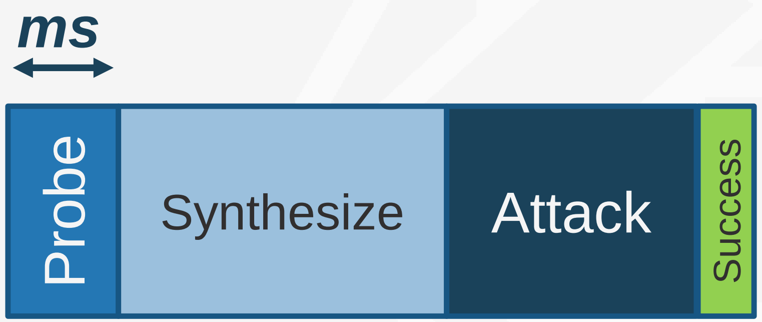


```
void target() {
                    lowed, gg");

}

void vulnerable(char* str1) {
  char buf[5];
  strcpy(buf, str1)
}

int main() {
  vulnerable("ffffffffffffffff\xf0\x01\x01\x00");
  printf("This prints for normal control flow");
}
```

Undefined: return address store
Undefined: array overflow
Undefined: target() address forgery

MORPHEUS BREAKS EMERGENT ATTACKS

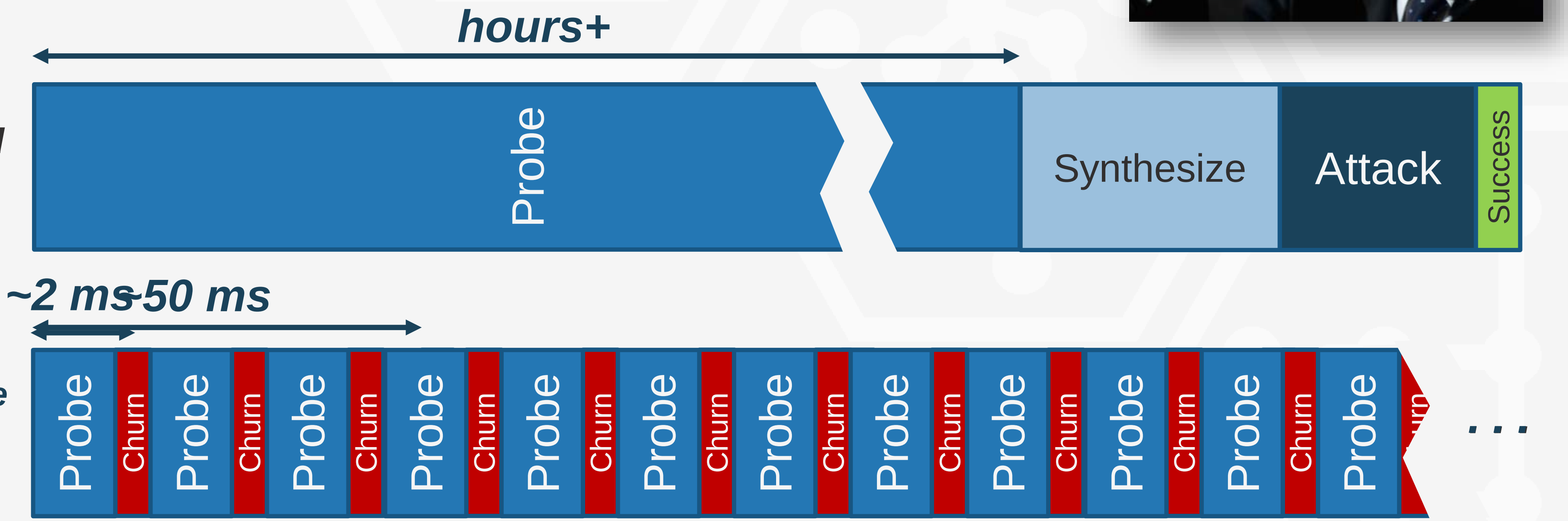
Conventional Attack



With Randomized Undefined Semantics

With Adaptive Churn and Memory

With Churn



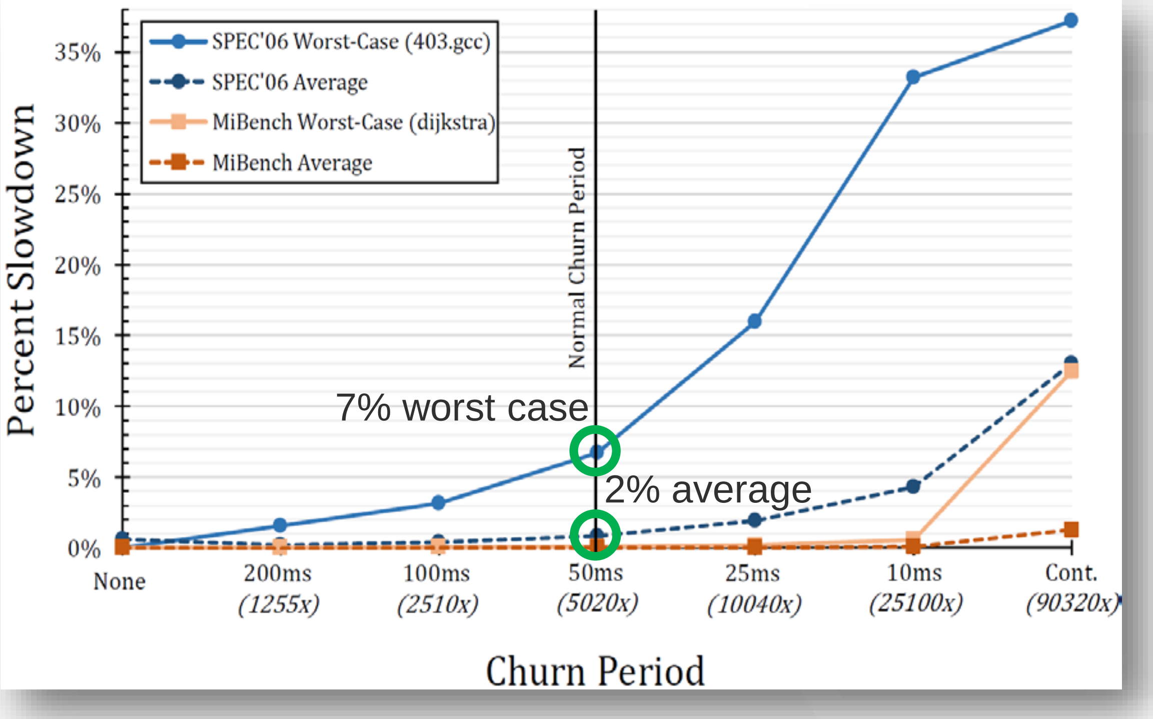
DISTRIBUTION STATEMENT A. Approved for public release

THE EARLY RESULTS LOOK PROMISING

Morpheus ***secure CPU*** developed in the DARPA SSITH Program with PM Linton Salmon. Team includes researchers from Michigan, Princeton and UT Austin

Early results:

- Performance cost: ***2% average slowdown*** with 504-bits of entropy and 50ms churn
- Power cost: ***2.5% power***
- Area cost: ***8% area*** increase
- Developer cost: ***No impact on normal applications***



COMMERCIALIZATION IS UNDERWAY

- ***Agita Labs*** is commercializing Morpheus
  - Integrated into the RISC-V ecosystem
  - Initially targeting ***server*** and ***IoT*** markets
  - Building ***FPGA & ASIC based secure CPUs***

- Two technology demos are in development
  - Secure ***voting machine hacking*** event at DEFCON
  - A second ***national-defense oriented demonstration*** is soon to start

- Visit http://www.agitalabs.com for more info

ERI ELECTRONICS RESURGENCE INITIATIVE

SUMMIT

2019 | Detroit, MI | **July 15 - 17**