Could a purpose built supercomputer play DEF CON Capture the Flag?

Mike Walker
Program Manager

November 14, 2013

Cyber Competition Challenges

Turing, Rice, & Undecidable Problems:

- Is the software correct & secure?
- If not, how incorrect or insecure is it?

Q: Can we *compete* when the answers required to name a victor are undecidable?

Competitive Programming: TopCoder

1: Construct

2: Challenge

```
bool find( const int x, const int* pBegin, const int* pEnd)
{
    int medel = (*pBegin +(( *pEnd-1) - *pBegin)/2) ;
    if(x == medel) return true ;
    else if( x > medel)
    { int begin = (medel +1);
      return find (x, &begin, pEnd); }
    else if( x< medel)
    { int last = (medel-1);
      return find(x,pBegin, &last); } }
```

```
public static int binarySearch(int[] a, int key) {
        int low = 0;
        int high = a.length - 1;
        while (low <= high) {
            int mid = (low + high) / 2;
            int midVal = a[mi
            if (midVal < key)
                low = mid + 1
            else if (midVal >
            else return mid; //
        return -(low + 1);  // key
```

```
binary_search(lo, hi, p):
   while we choose not to terminate:
      mid = lo + (hi-lo)/2
      if p(mid) == true:
         hi = mid
      else:
         lo = mid
   return lo
```

2^{31}

```
int mid = (low + high) / 2;
```

ArrayIndexOutOfBoundsException *

http://technorazzi.com/wp-content/uploads/2010/08/ctf_denmark2.jpg

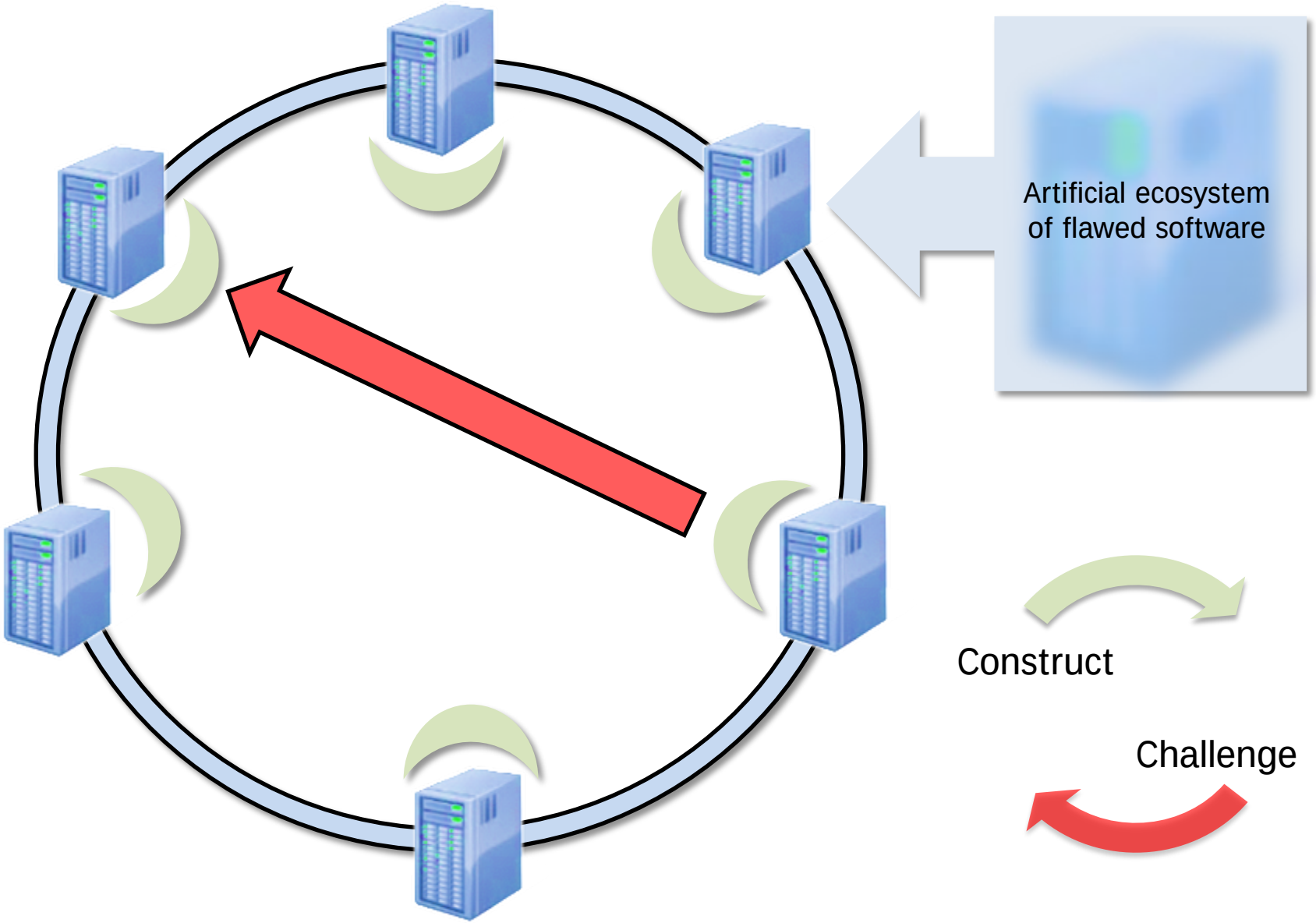
*http://googleresearch.blogspot.com/2006/06/extra-extra-read-all-about-it-nearly.html

Competitive Programming

Q: Can we *compete* when the answers required to name a victor are undecidable?

A: *consensus evaluation*

Competitive Computer Security: DEF CON CTF



Competition Paradigm

Harness consensus evaluation to identify breakthrough technology.

CYBER GRAND_CHALLENGE

A tournament for fully automated network defense

An alternative software ecosystem whose challenges and constraints mirror those imposed on real world network defenders.

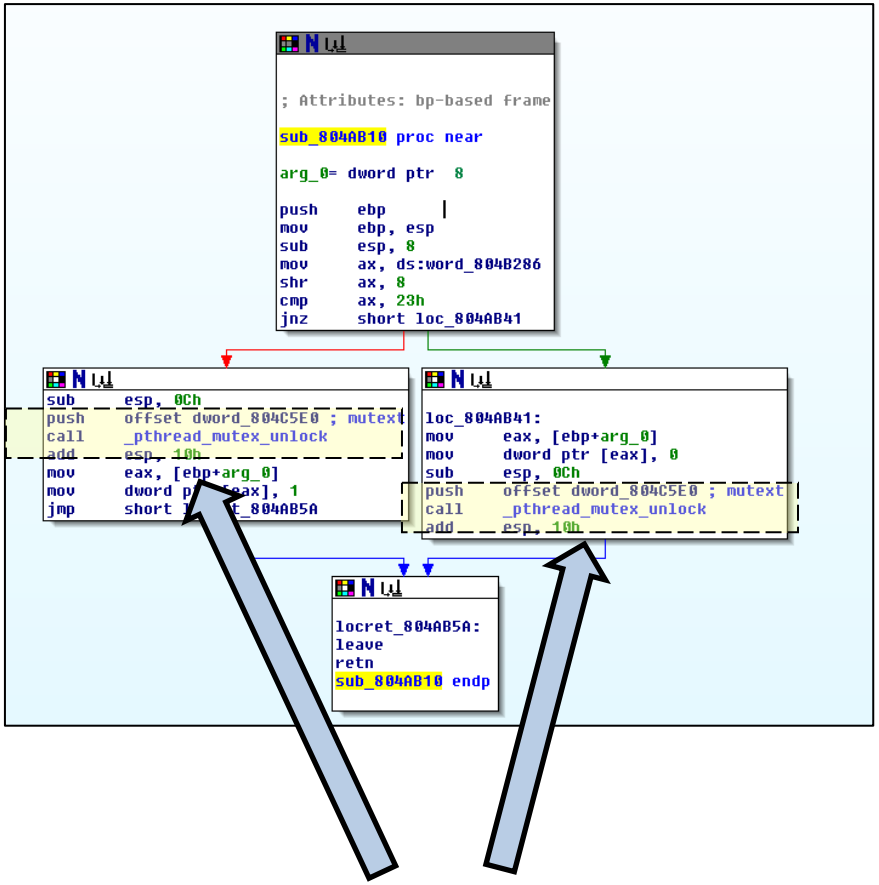
CTF: Alternative Software Ecosystem

Authentic Analysis Challenges

- Memory aliasing
- Race condition dependent memory corruption
- Randomized Initial State Dependent Flaws
- Hidden Interpreters
- Dynamic Network Utilization

Synthetic Programs

- Lightweight Network Services
- Used Only Once
- No A Priori Knowledge

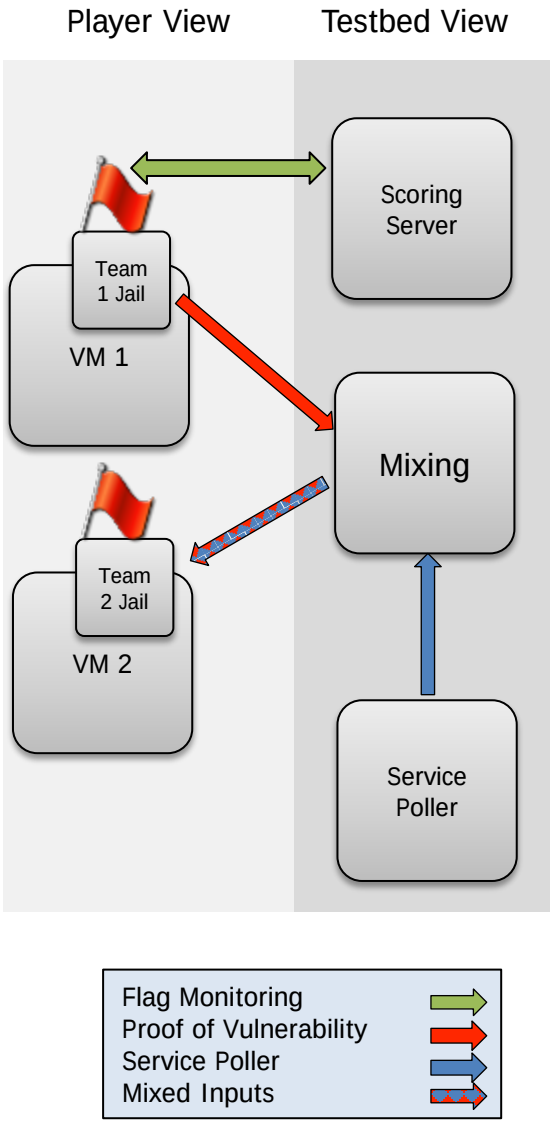


Defcon CTF Qualifiers 2007
Highest difficulty (500), network application flaw category
Hidden mutex unlock condition triggers timing specific memory corruption*

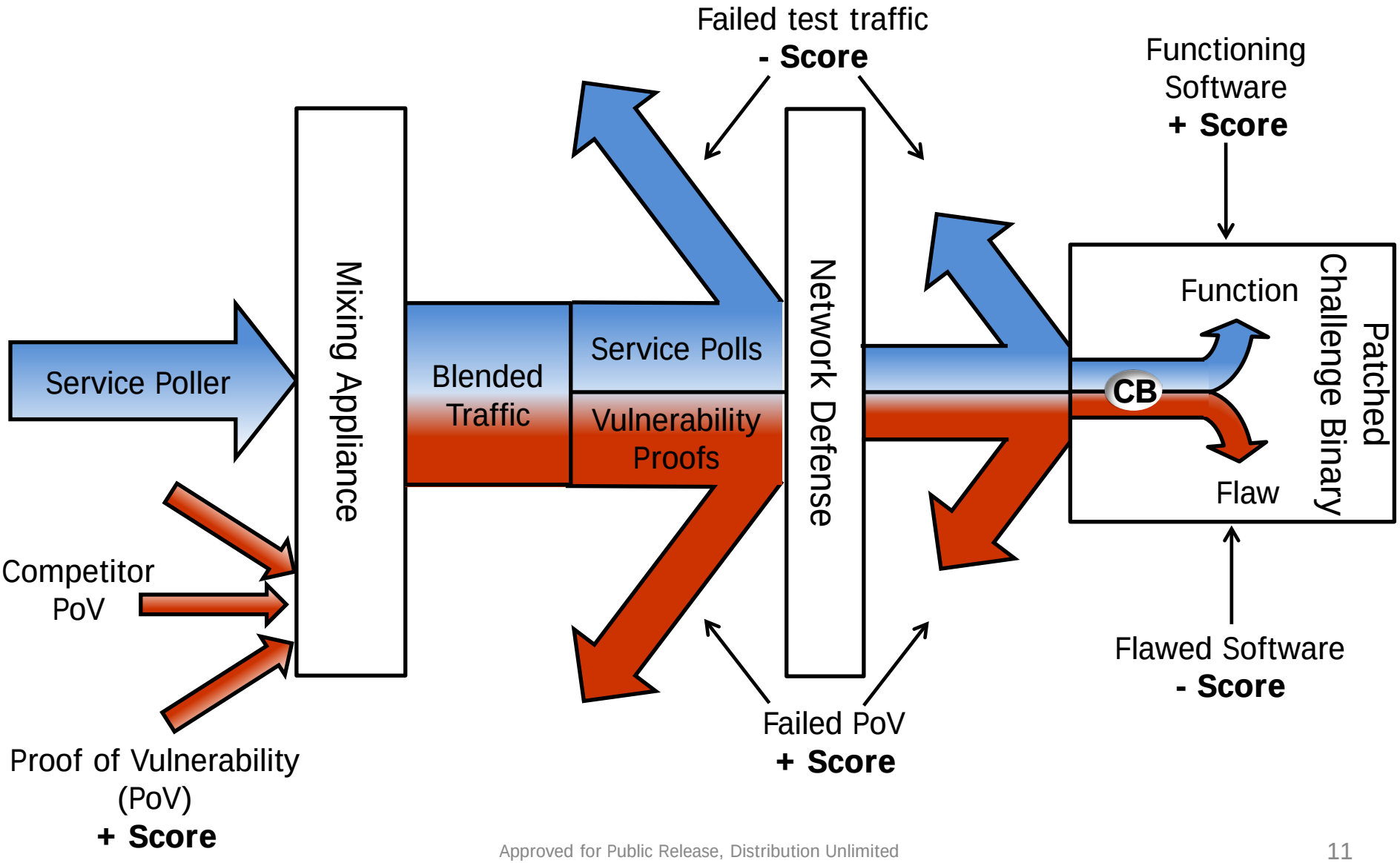
Authentic Skills, Synthetic Software

CTF: Real World Challenges

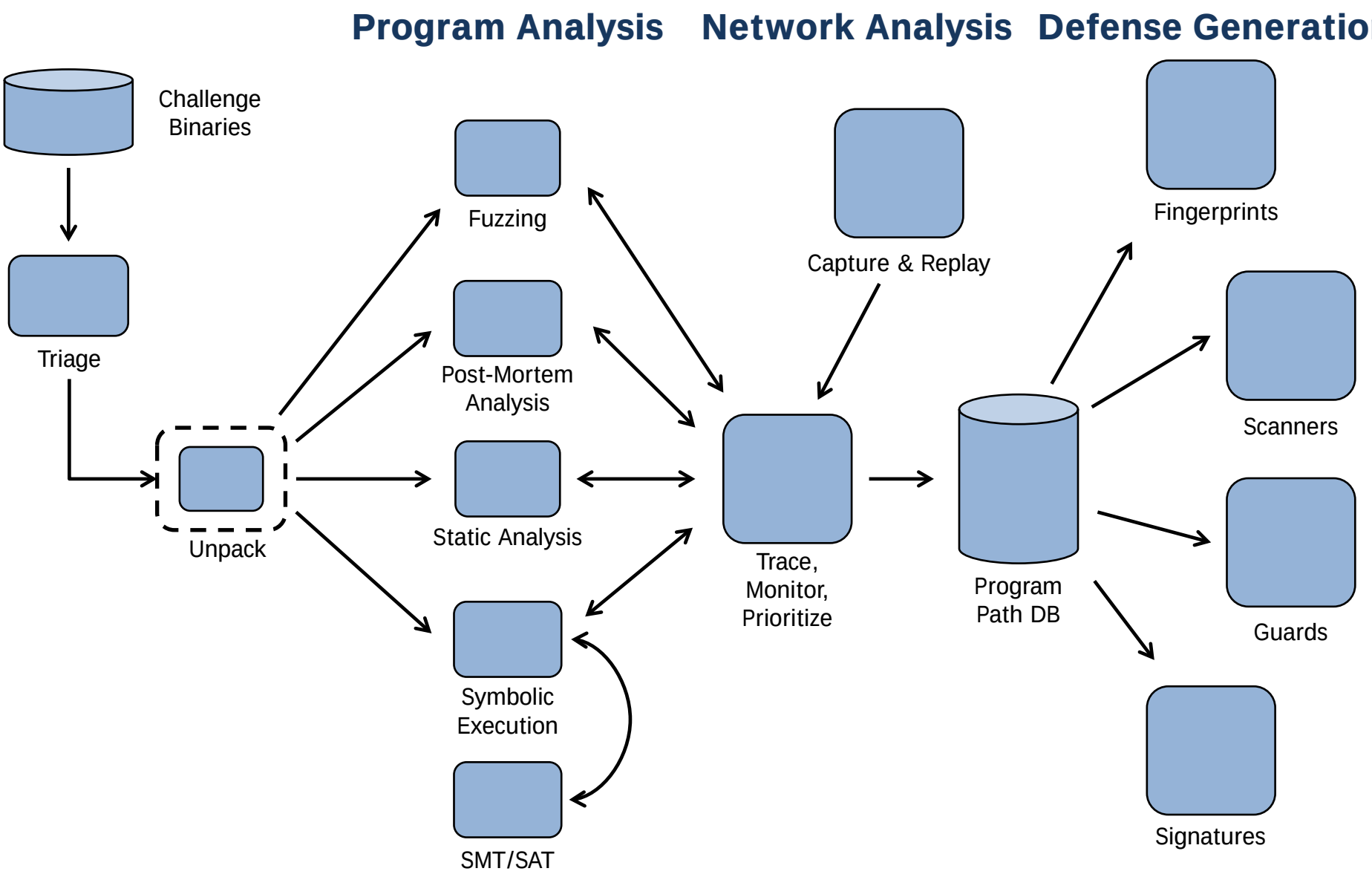
Challenges	CTF
Attribution & Reputation	Network Mixing
Resilience	New Flags Random Intervals
Availability	Service Poller



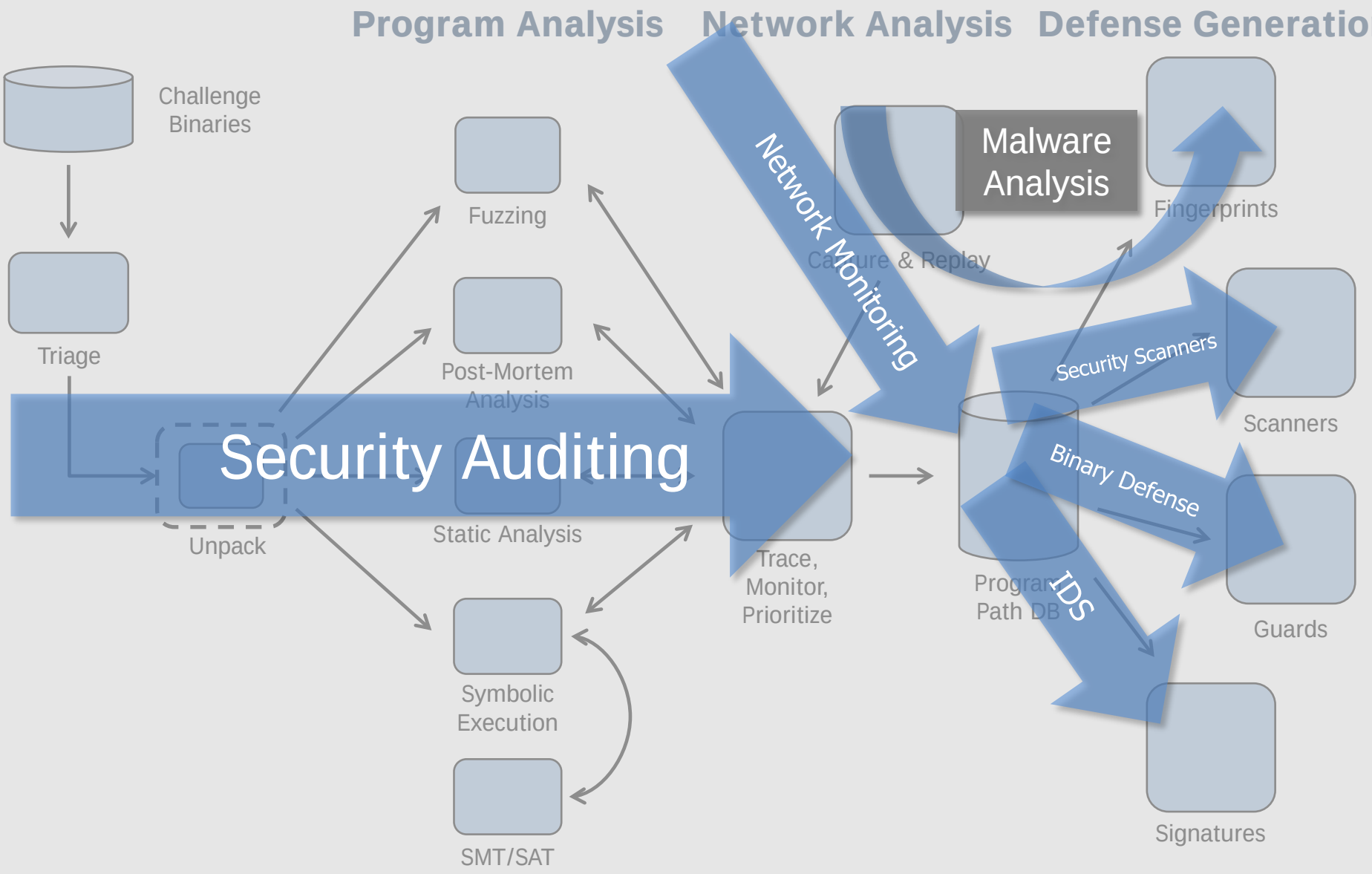
CTF: Real Time Defense



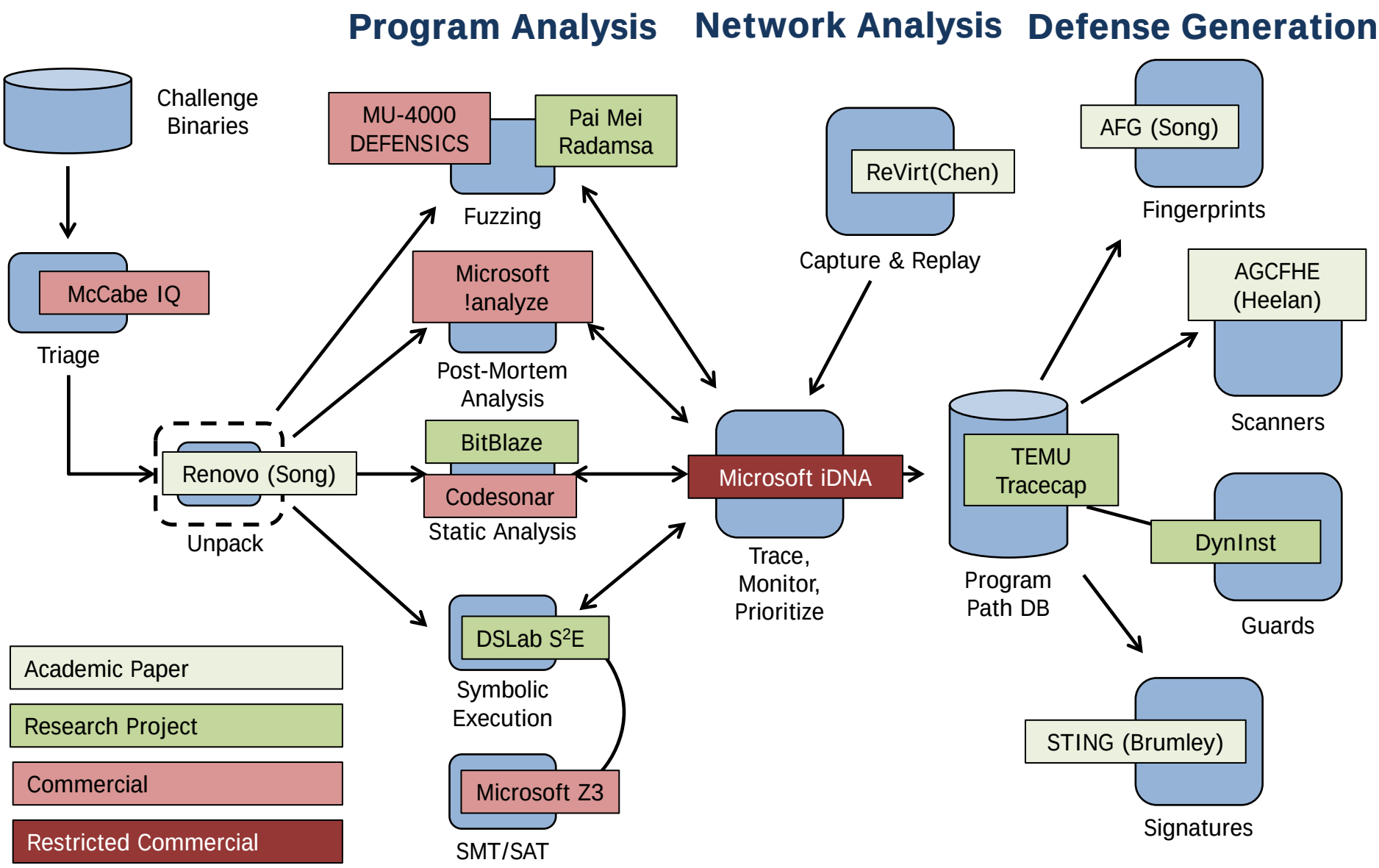
CTF: Human Reasoning Workflow



CTF: Representative Microcosm

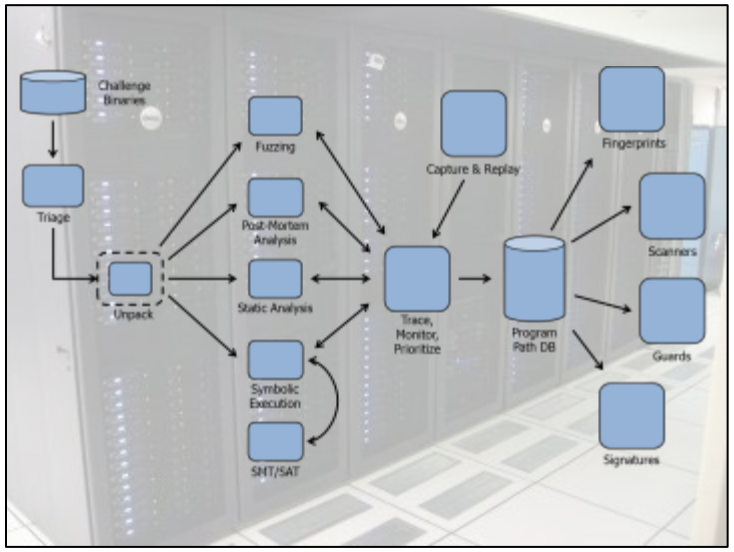


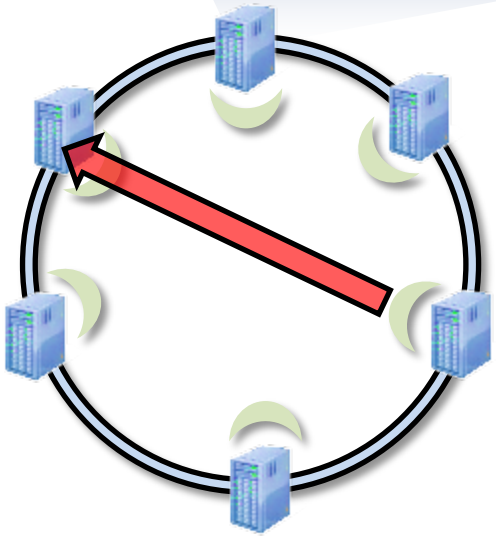
CTF in 2013: Seeds of Automation



Cyber Grand Challenge

Photo courtesy US Air Force Academy Cyber Competition Club





- Using the competition format which measures analyst cyber reasoning ability...
- A Grand Challenge for *automated defenders:*
- Systems that can detect and repel novel threats from networks

We've Been Here Before

Chess Grandmasters

Dedicated Systems

World Class CS

© IBM Research

Deep Blue

http://blog.pontiflex.com/2010/05/13/ibm-enters-social-media/

http://technorazzi.com/wp-content/uploads/2010/08/ctf_denmark2.jpg

Can We Do It Again?

Cyber Grandmasters

Dedicated Systems

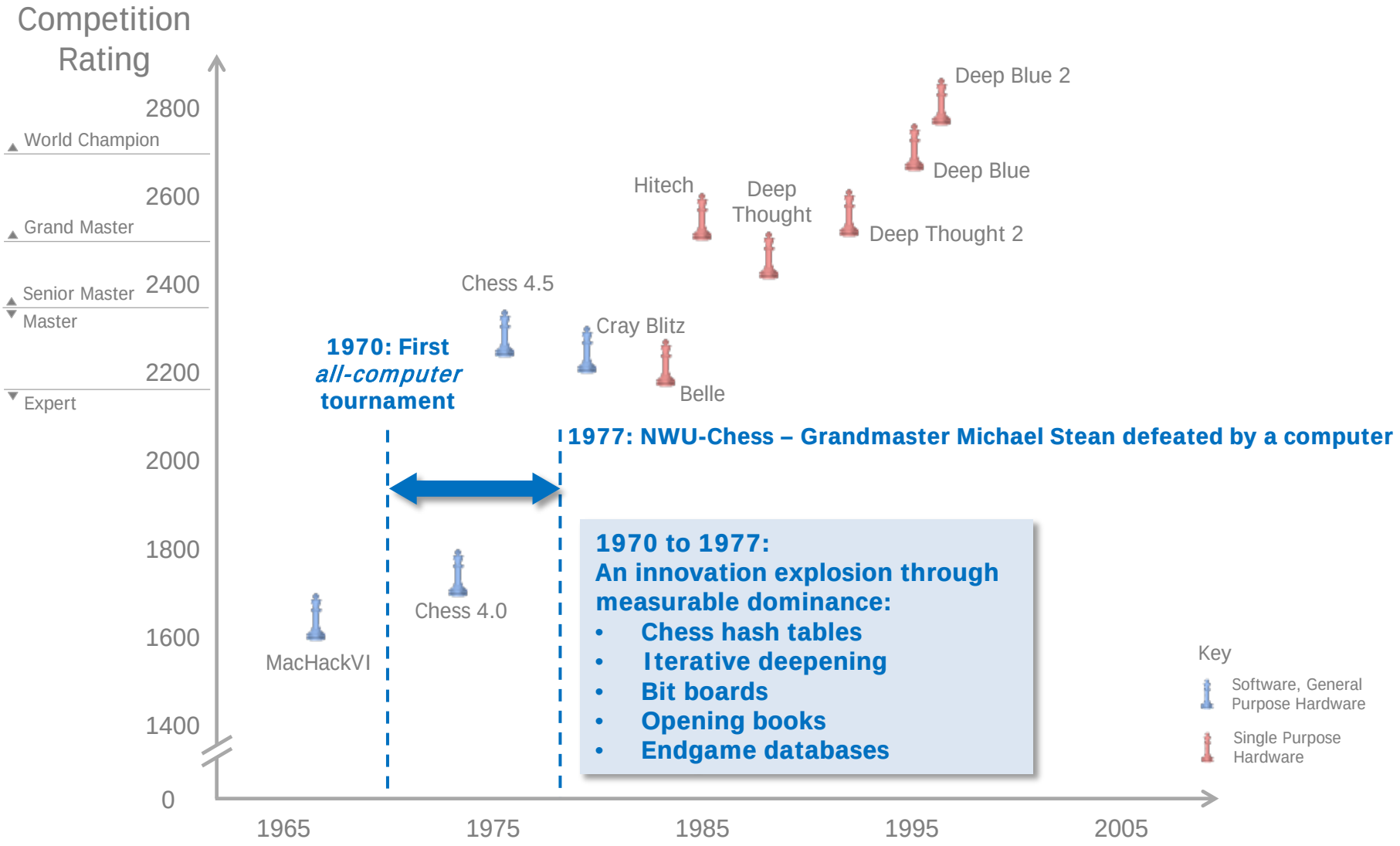
Program Analysis

dailyheadlines.uark.edu

Deep CTF?

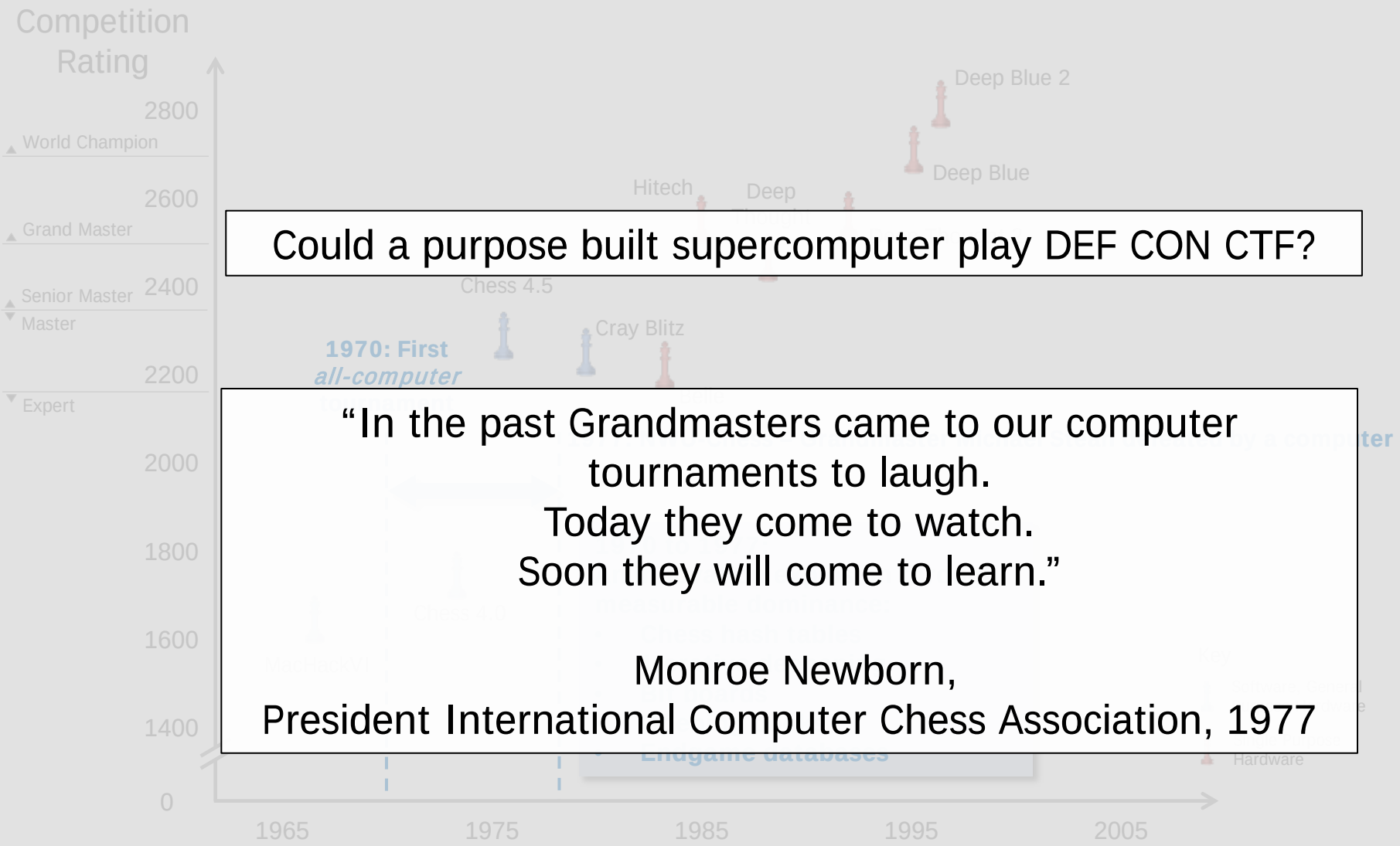
Photo courtesy US Air Force Academy Cyber Competition Club

A League of Their Own



Data Source: Computer History Museum
http://archive.computerhistory.org/resources/still-image/Chess_temporary/still-images/5.1a.%20Chess_Rating_Chart.L0623030076.jpg

A League of Their Own



Could a purpose built supercomputer play DEF CON CTF?

"In the past Grandmasters came to our computer tournaments to laugh.
Today they come to watch.
Soon they will come to learn."

Monroe Newborn,
President International Computer Chess Association, 1977

Data Source: Computer History Museum
http://archive.computerhistory.org/resources/still-image/Chess_temporary/still-images/5.1a.%20Chess_Rating_Chart.L0623030076.jpg

A new DARPA Challenge...

Open Track

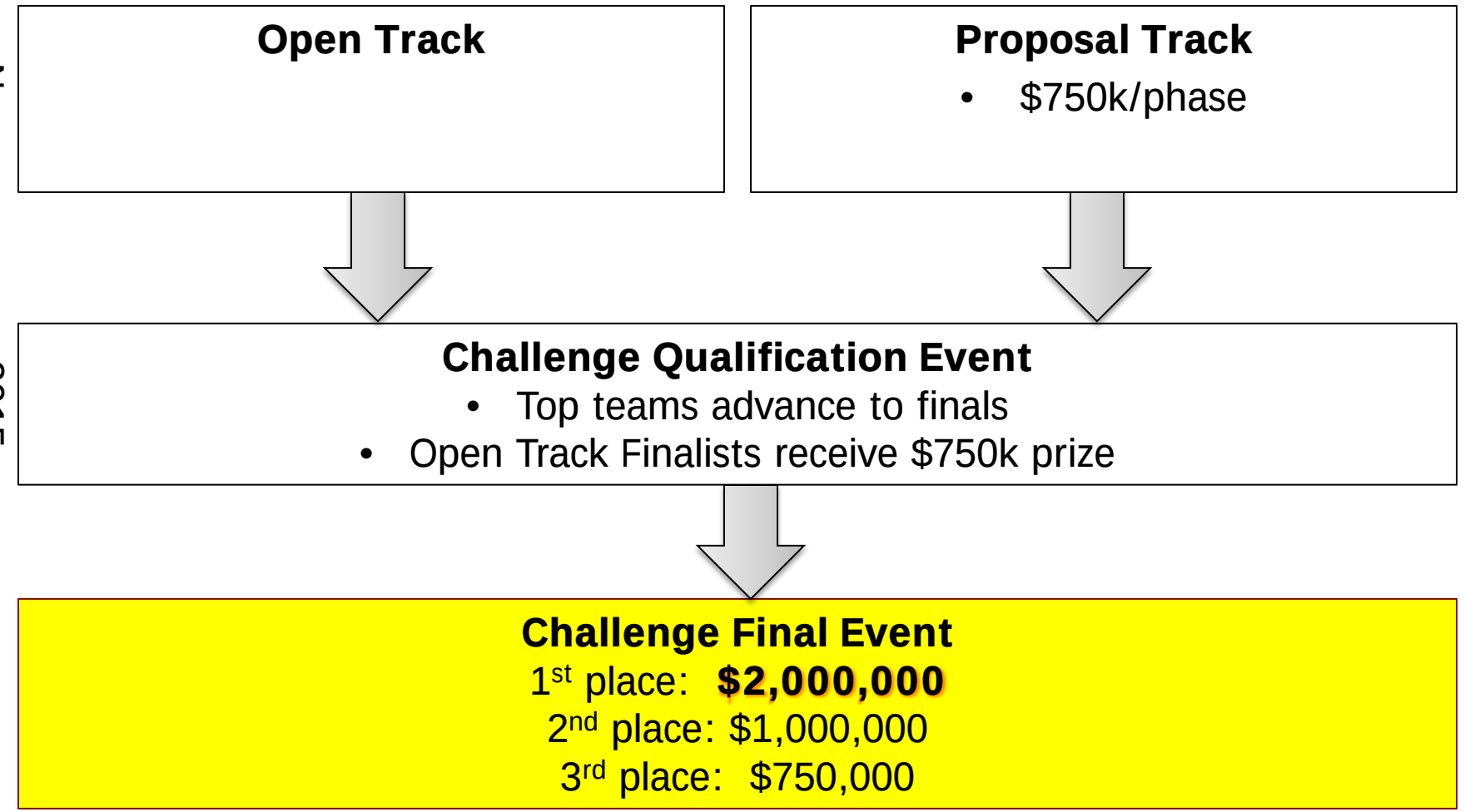
- Open to any eligible team
- No IP restrictions on entrant system

Proposal Track

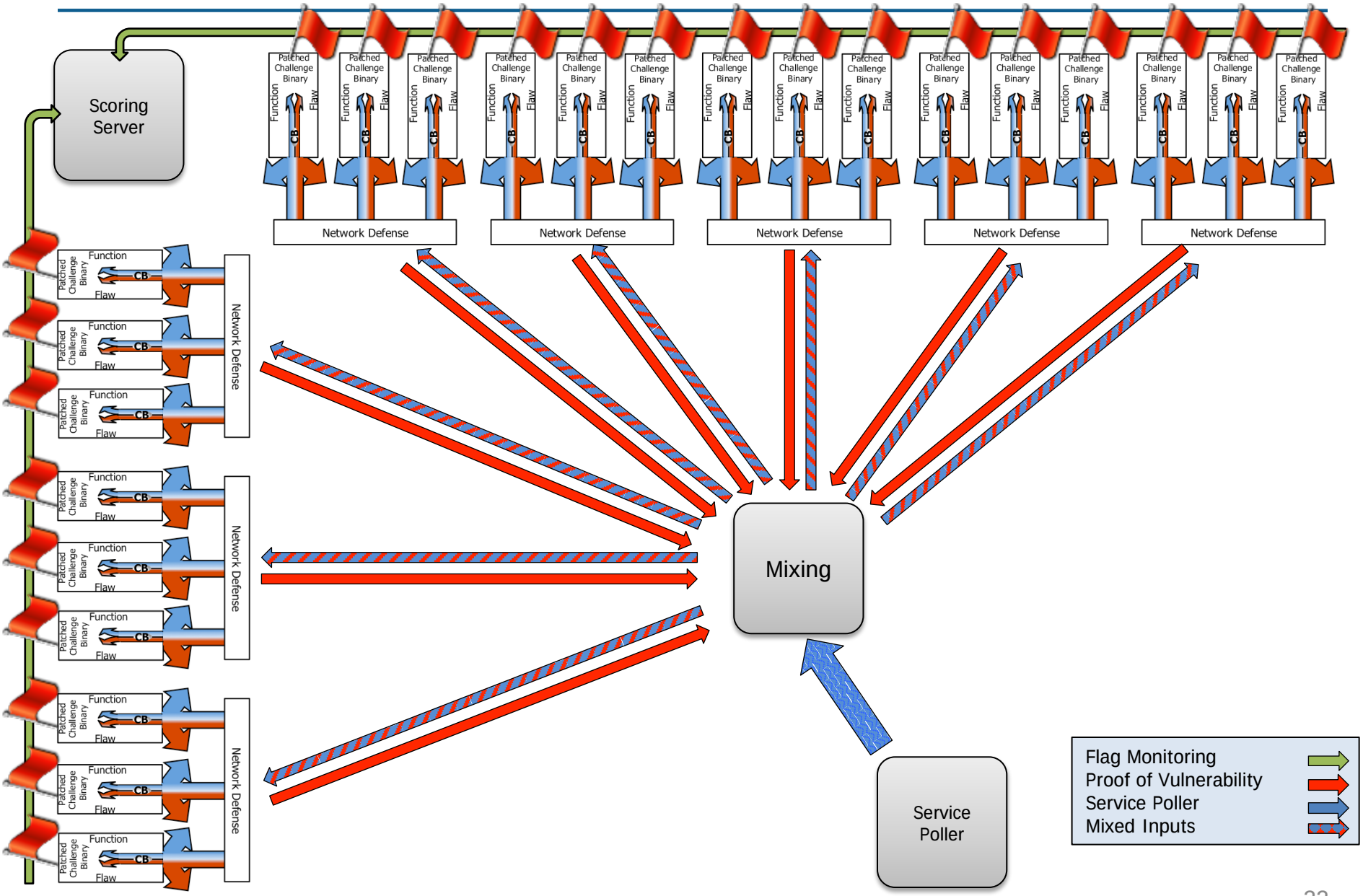
- DARPA Scientific Review Board
- Funded $750k/phase
- Government Purpose Rights to funded development

See rules at www.darpa.mil/cybergrandchallenge for full details

Cyber Grand Challenge: Scheduled Events



Scheduled Final Event: Multi-Team Real Time Tournament



For more information:

www.darpa.mil/cybergrandchallenge

Questions?