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

ArrayIndexOutOfBoundsException *


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

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

Approved for Public Release, Distribution Unlimited
Q: Can we *compete* when the answers required to name a victor are undecidable?

A: *consensus evaluation*
Competitive Computer Security: DEF CON CTF

Artificial ecosystem of flawed software

Construct

Challenge
Harness consensus evaluation to identify breakthrough technology.
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

* Approved for Public Release, Distribution Unlimited
# CTF: Real World Challenges

<table>
<thead>
<tr>
<th>Challenges</th>
<th>CTF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribution &amp; Reputation</td>
<td>Network Mixing</td>
</tr>
<tr>
<td>Resilience</td>
<td>New Flags Random Intervals</td>
</tr>
<tr>
<td>Availability</td>
<td>Service Poller</td>
</tr>
</tbody>
</table>

---

**Diagram: Player View vs. Testbed View**

- **Player View**:
  - Scoring Server
  - VM 1
  - VM 2
  - Team 1 Jail
  - Team 2 Jail

- **Testbed View**:
  - Mixing
  - Service Poller

Legend:
- Flag Monitoring
- Proof of Vulnerability
- Service Poller
- Mixed Inputs

Approved for Public Release, Distribution Unlimited
CTF: Real Time Defense

Service Poller
Mixing Appliance

Failed test traffic
- Score

Functioning Software
+ Score

Flawed Software
- Score

Competitor PoV
Proof of Vulnerability (PoV)
+ Score

Blended Traffic
Service Polls
Vulnerability Proofs

Network Defense

Challange Binary
Patched
Function
Flaw

Approved for Public Release, Distribution Unlimited
CTF: Human Reasoning Workflow

Program Analysis  Network Analysis  Defense Generation

Challenge Binaries

Triage

Unpack

Fuzzing

Post-Mortem Analysis

Static Analysis

Symbolic Execution

SMT/SAT

Trace, Monitor, Prioritize

Program Path DB

Fingerprints

Scanners

Guards

Signatures

Approved for Public Release, Distribution Unlimited
CTF in 2013: Seeds of Automation

Program Analysis  Network Analysis  Defense Generation

Challenge Binaries

MU-4000 DEFENSICS  Pai Mei Radamsa

Fuzzing

Microsoft !analyze

Post-Mortem Analysis

BitBlaze

Codesonar

Static Analysis

Microsoft iDNA

Trace, Monitor, Prioritize

 TEMU Tracecap

Program Path DB

AGCFHE (Heelan)

Scanners

ReVirt(Chen)

Capture & Replay

Fingerprints

AFG (Song)

Guards

Unpack

Renovo (Song)

McCabe IQ

Triage

Microsoft Z3

SMT/SAT

Symbolic Execution

DSLab S^2E

Academic Paper

Research Project

Commercial

Restricted Commercial

Approved for Public Release, Distribution Unlimited
Cyber Grand Challenge

• 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

Deep Blue

Can We Do It Again?

Cyber Grandmasters

Dedicated Systems

Program Analysis

Deep CTF?

Photo courtesy US Air Force Academy Cyber Competition Club
1970: First all-computer tournament

1977: NWU-Chess - Grandmaster Michael Stean defeated by a computer

1970 to 1977: An innovation explosion through measurable dominance:
- Chess hash tables
- Iterative deepening
- Bit boards
- Opening books
- Endgame databases

Data Source: Computer History Museum

Approved for Public Release, Distribution Unlimited
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
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](http://www.darpa.mil/cybergrandchallenge) for full details
Cyber Grand Challenge: Scheduled Events

Open Track

Proposal Track
- $750k/phase

Challenge Qualification Event
- Top teams advance to finals
- Open Track Finalists receive $750k prize

Challenge Final Event
1st place: $2,000,000
2nd place: $1,000,000
3rd place: $750,000
Scheduled Final Event: Multi-Team Real Time Tournament

Scoring Server

Network Defense

Mixing

Flag Monitoring
Proof of Vulnerability
Service Poller
Mixed Inputs

Approved for Public Release, Distribution Unlimited
For more information:
www.darpa.mil/cybergrandchallenge

Questions?