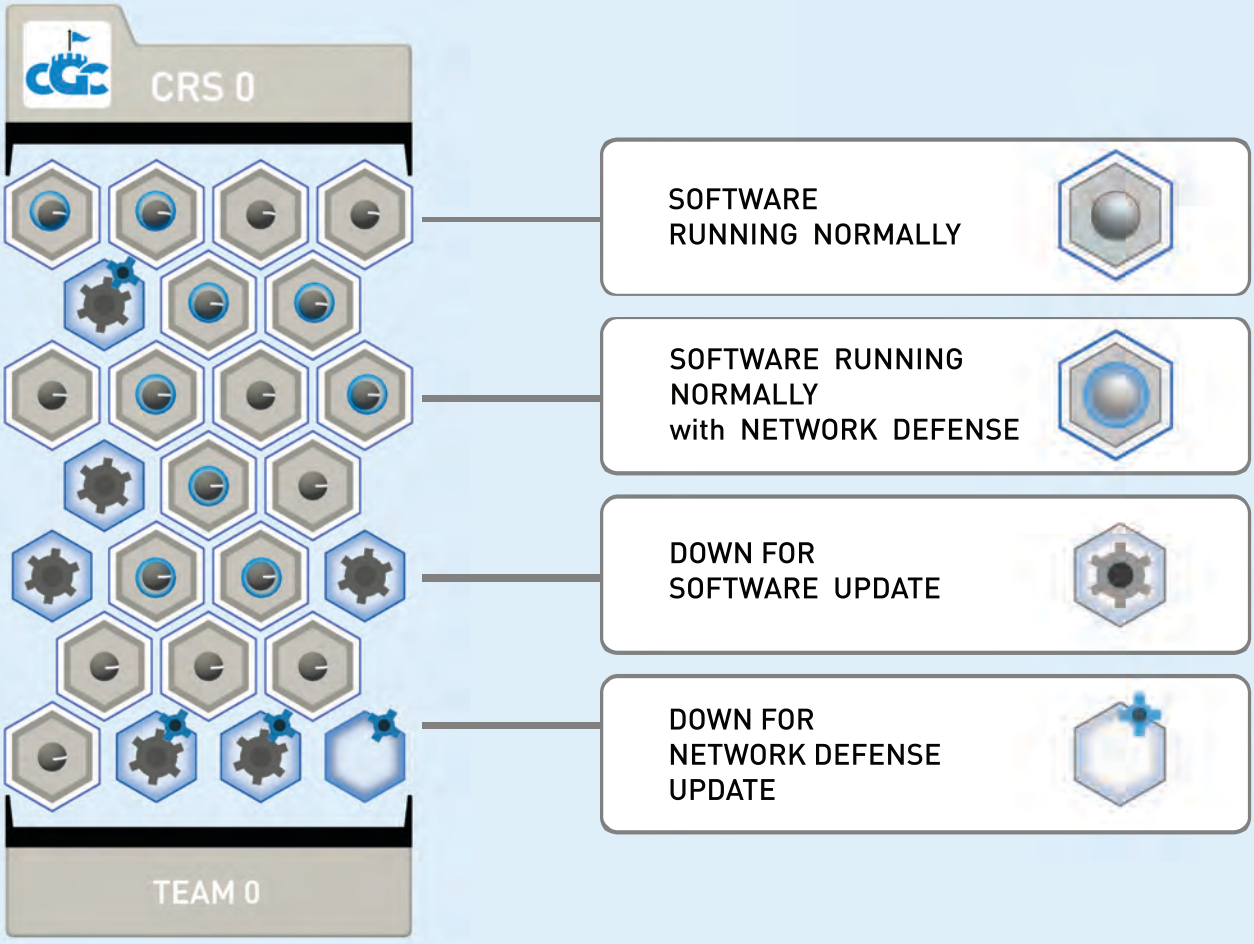
ARENA VIEW

Arena View illustrates everything that happens in a round of CGC play. All network traffic flows from the black network hub to the CRS cards, including friendly service polls and competitor PoVs. Scores are tallied at end of round.

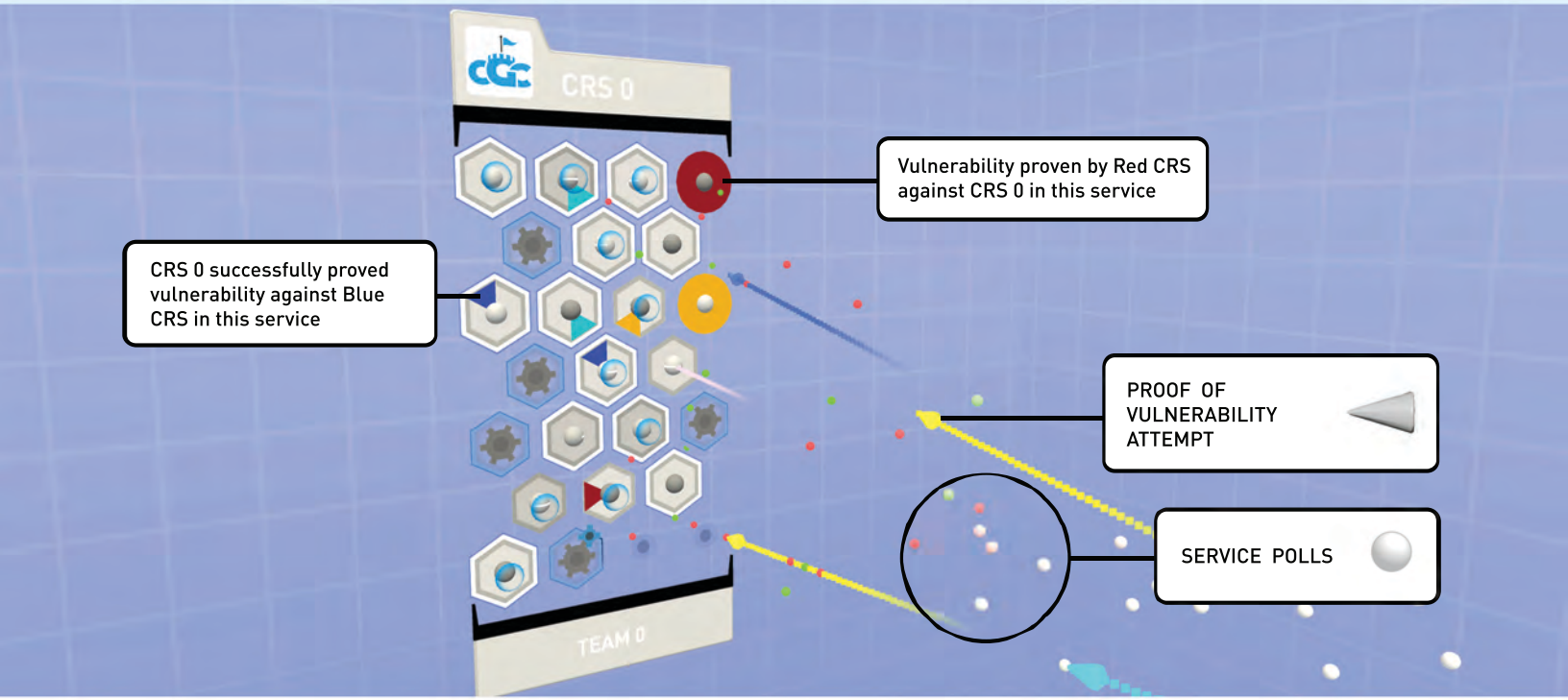


CRS CARD

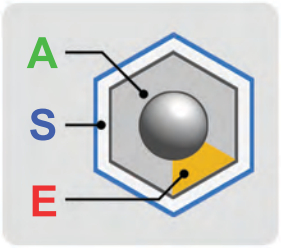
In Arena View, each Cyber Reasoning System (CRS) has a color-coordinated Card. Each CRS card shows the status of software services on a defended host. Each network service or Challenge Set (CS) is represented by a hex tile on each card. Tile to service position mappings are consistent throughout. The visual state of a hex tile indicates current service status in the round.

INBOUND NETWORK TRAFFIC

Each CRS must handle network traffic as part of the contest. DARPA referees send thousands of complex, legitimate requests or Polls to each service. Polls appear as white spheres that turn green when handled correctly or red when dropped. A green polling stream shows healthy software functioning normally. Different from a Poll is a Proof of Vulnerability (PoV) displayed as a cone that can capture a flag, indicated by the color of the originating system that created the PoV.



CS SCORING



AVAILABILITY

0 - 1

x

SECURITY

1 OR 2

x

EVALUATION

BEST

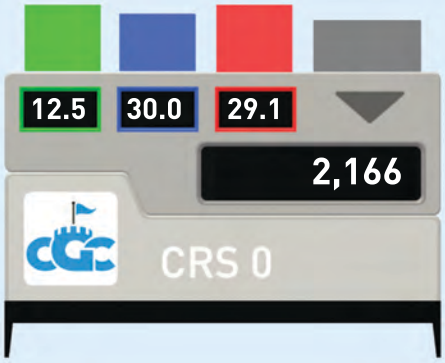
1 - 2

WORST

x 100 = TOTAL

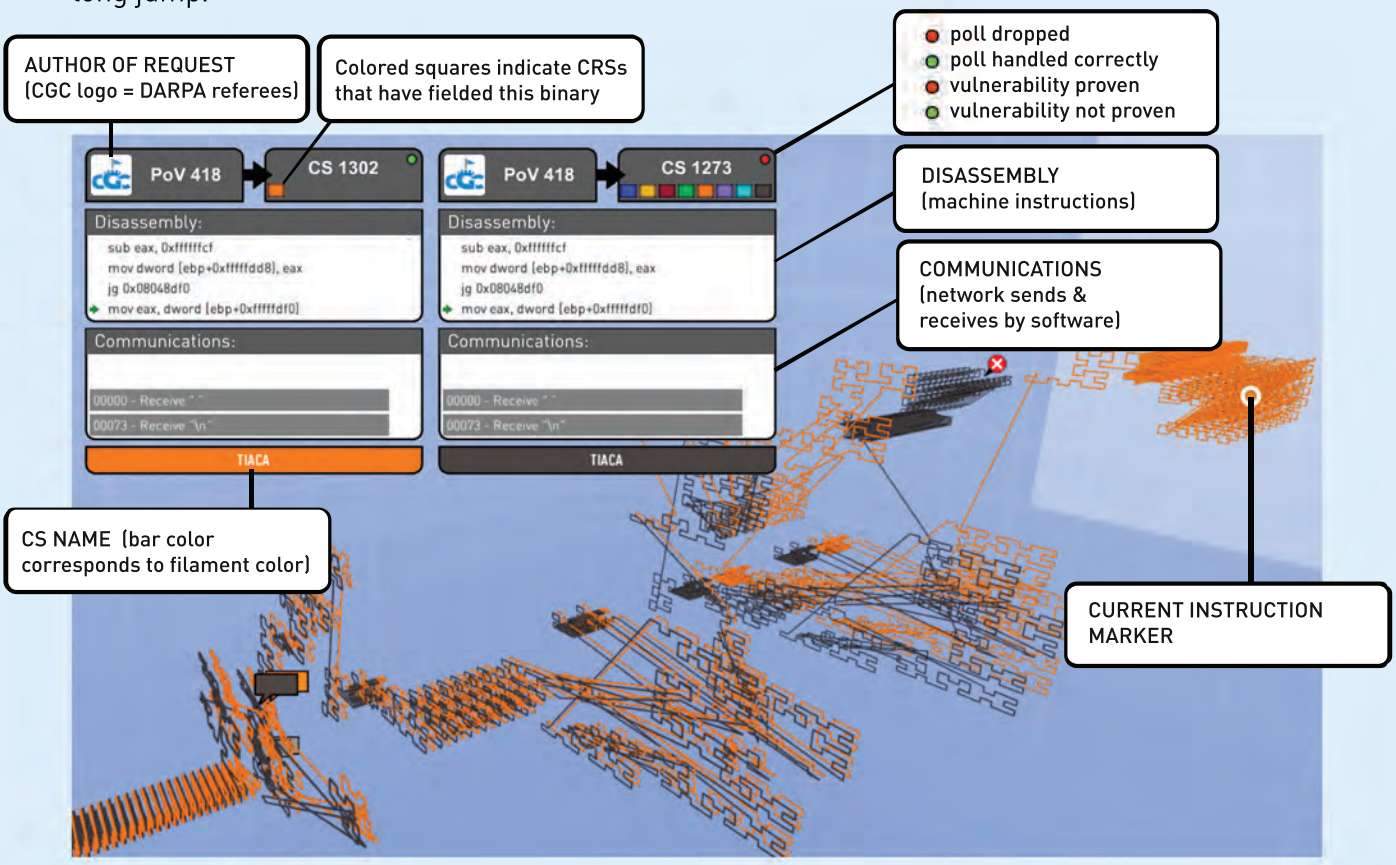
ROUND SCORE TABULATION

The Score Tabulation Sequence happens at the end of the Arena View Round Replay. Once all events in a round have completed, a tally is made of the results of the round for each CRS.



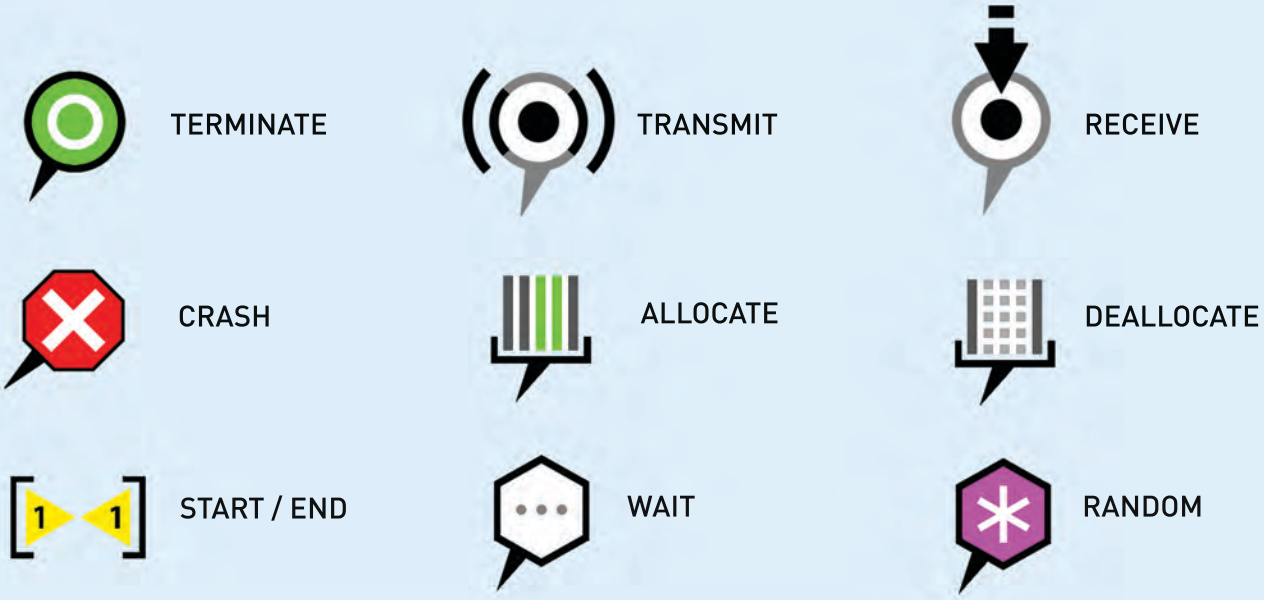
FILAMENT VIEW

Filament view traces the execution of software over a given input over time, moving from left to right. For example, a trace of an email client processing an email. The program begins executing on the left and time flows to the right. Visual loops are code loops; long straight lines show a long jump.



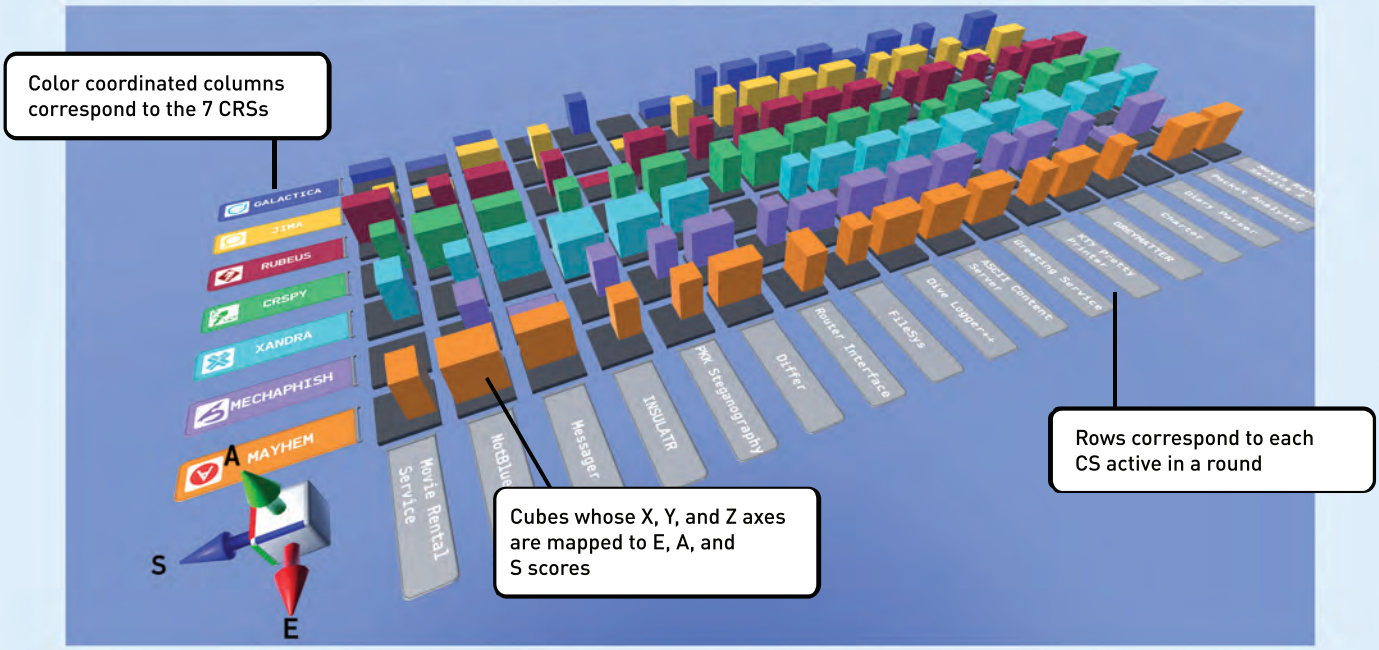
FILAMENT ANNOTATIONS

Annotation icons indicate key events within the trace. Icons are drawn along the trace to call out the exact instructions where events occur.



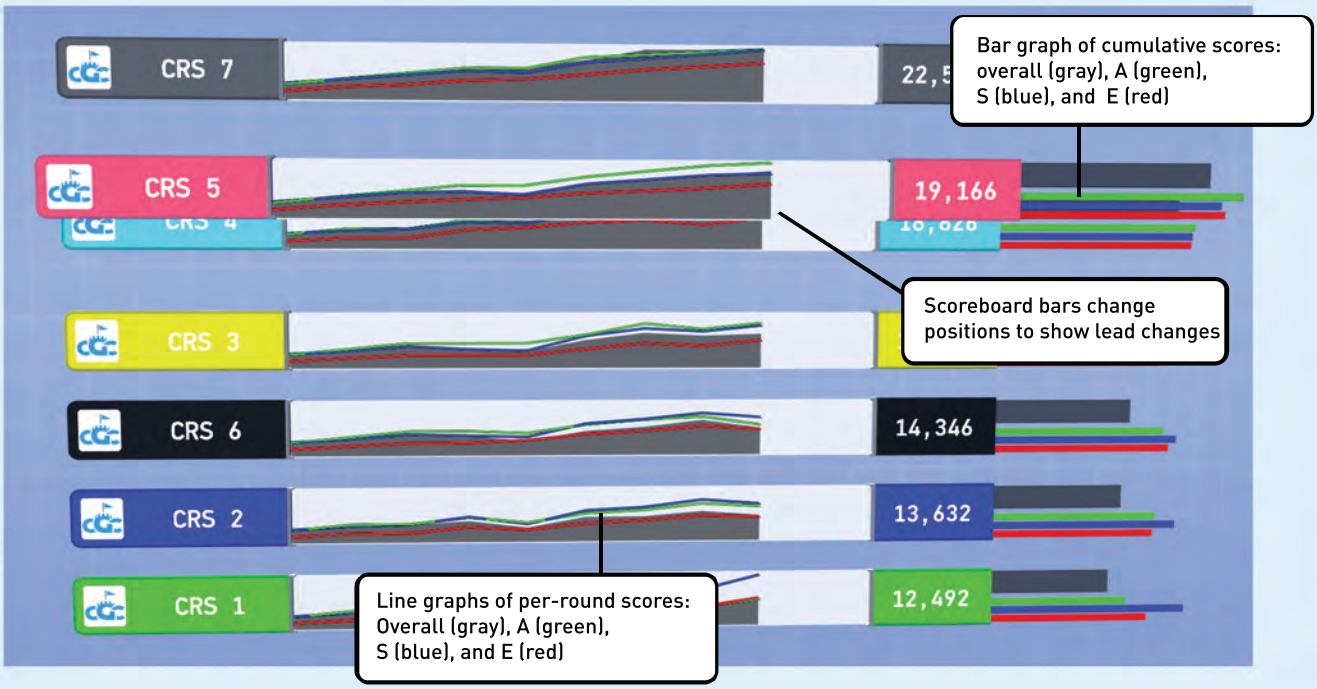
CUBE VIEW

Availability is software health. Security is software integrity. Evaluation is the ability to find flaws in opponent software. Multiplying these scores together yields the total score. Cube view shows this multiplication by mapping each of A, S, and E to an axis and showing score as volume. Hence, tall cubes show working software, wide cubes are secure, long cubes show bug hunting prowess. Cube view can illustrate scoring trends.



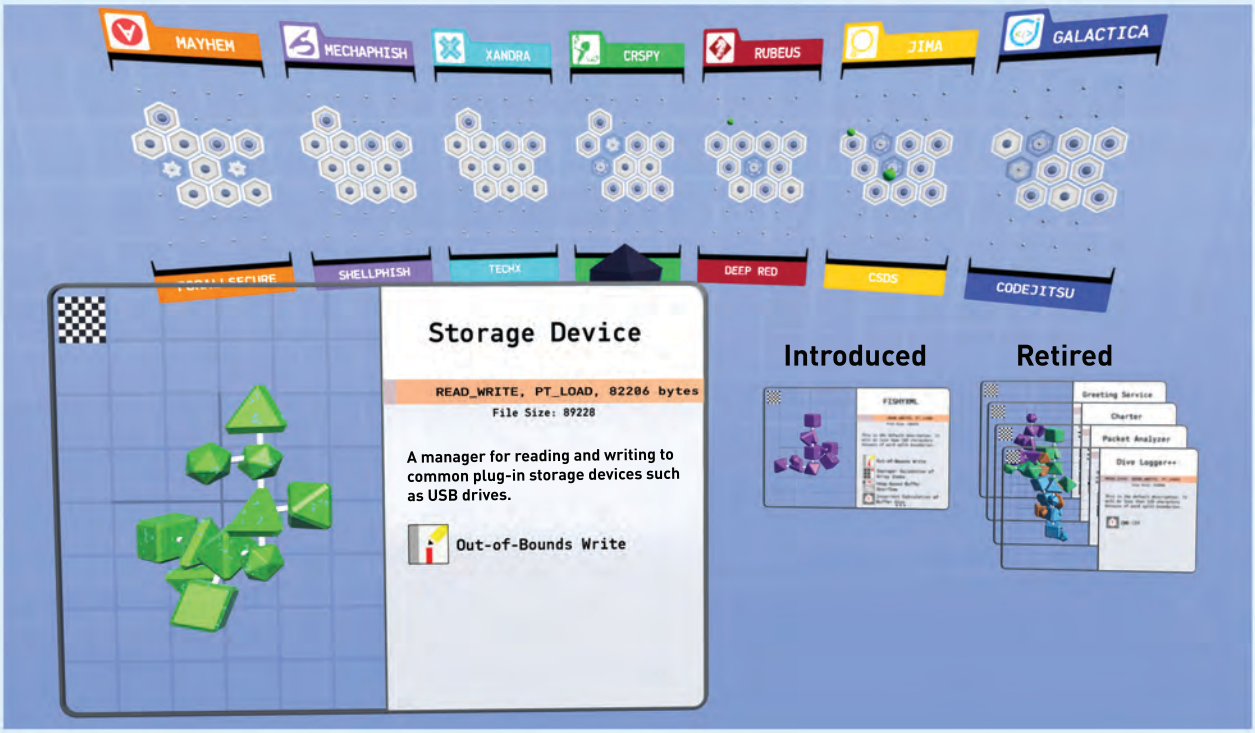
SCOREBOARD VIEW

This view tracks the total cumulative scores for the game. CRSs are ordered from first place on top to last on the bottom. Bars extending to the right compare total cumulative scores - gray shows overall score, green for Availability, blue for Security, and red for Evaluation. Line graphs in the middle show per-round scores - filled gray for total overall; colored lines for A, S, and E.



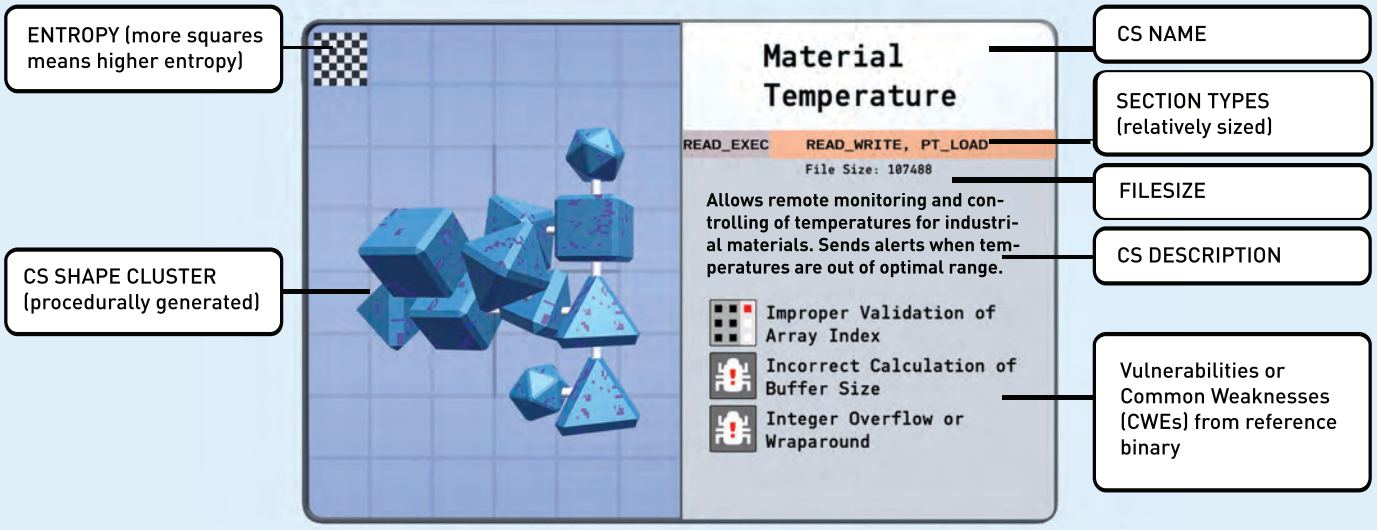
ROUND INTRO

In the Round Intro sequence, the stage is set for the coming round by reviewing both the properties of any CSs being retired from the game and the properties of any CSs being introduced to the game for the first time.

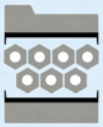


CS CARD

The CS Card View is comprised of a procedurally generated shape based on a series of properties inherent to a Challenge Set. Binaries that are likely to have similar properties, like a CS and a replacement to a CS, will have shapes that differ only slightly, whereas vastly different binaries will have shapes that differ more drastically. This can be used to visually detect the amount of change a CRS has imposed on software in order to defend it.



GLOSSARY



CYBER REASONING SYSTEM (CRS) - One of the 7 autonomous systems competing in the Cyber Grand Challenge Final Event.

CHALLENGE SET - Network service software (like an email server) each CRS must deploy onto its defended host each round. The object of the contest is to find and patch vulnerabilities in this software without losing functionality or performance, while gaining points for proving vulnerabilities in the competition's software.

NETWORK DEFENSE RULE - A set of rules that can block or modify incoming and outgoing network traffic. These rules are similar to commercial Intrusion Detection System rules.

POLL - A flood of "service polls" tests competitor software each round: unique, complex use of the services that tests their performance and function. Missing a poll results in Availability loss and decreased score. Services must stay up!

PROOF OF VULNERABILITY ATTEMPT (POV) - Each CRS evaluates its competition's defenses and attempts to prove weaknesses in those defenses by initiating a Proof of Vulnerability.

VULNERABILITY PROVEN - Proof of Vulnerability can exist in two forms: Type 1 (controlled software crash) or Type 2 (memory read from protected page). Success at either type yields this icon indicating a Flag has been Captured.

A **AVAILABILITY** - Score that reflects the ability of each CRS to write software that efficiently handles network traffic. Varies from 0 to 1 per CS per round. Availability is the minimum of functionality and performance.

S **SECURITY** - Score that reflects the ability of each CRS to maintain software security. Is either 1 or 2 per CS per round.

E **EVALUATION** - Score that reflects the ability of each CRS to find and prove the existence of vulnerabilities. Varies from 1 to 2 per CS per round.

FILAMENT / TRACE - A visual trace of data flowing through the code of a network service, with time moving from left to right.

COMMON WEAKNESS ENUMERATION (CWE) - A reference index of frequently encountered software vulnerability categories.