Case Study:
U.S. Department of Defense (DoD) Chooses Mayhem for Critical System Security

Learn how the DoD hand-picked Mayhem as the best solution to autonomously test their critical weapon systems applications for vulnerabilities, formulate patches, and deploy them in real time on network.
The Challenge

As DoD weapon systems became increasingly software dependent and networked, the challenges in protecting the associated applications from increasingly sophisticated attacks grew.

The DoD’s delayed prioritization of weapon system security created a critical need to recognize cyber warfare as a new domain of conflict.

Once the need for additional software security testing was identified, it was difficult to find automatic defense systems capable of identifying vulnerabilities, formulating patches, and deploying them in real time on network.

The DoD was left with a pressing need to find an autonomous software security solution with an accelerated time-to-value to address emerging weapon system security issues within select critical missions.
The Problem:

The U.S. Department of Defense (DoD) is responsible for billions of dollars in safety-critical equipment and missions. A single flaw in a system not only costs money, but puts their mission and lives at risk.

In 2018, the U.S. Government Accountability Office (GOA) reported that there were mounting challenges in protecting DoD weapon systems from increasingly sophisticated attacks: “This state is due to the computerized nature of weapon systems, the DoD’s late start in prioritizing weapon systems cybersecurity, and DoD’s nascent understanding of how to develop more secure weapon systems. DoD weapon systems are more software dependent and more networked than ever before.”

The DoD has moved to embrace cyber as a new domain of warfare, with that comes the requirement to check weapon systems’ applications dynamically. An expansion of a comprehensive software security solution into some of the most critical systems was needed across multiple branches of the DoD.

DoD organizations buy separately and have different missions. Between multiple organizations and missions, there was an aligned need to create automatic defensive systems capable of reasoning about flaws, formulating patches, and deploying them on the network in real time with an accelerated time to value.

The Solution:

The Defense Innovation Unit recognized a potential solution to the weapons system security problem in the original version of Mayhem featured in the Cyber Grand Challenge in 2016. They moved to apply Mayhem to select critical missions within the DoD.

DARPA Cyber Grand Challenge

Originally developed to participate in the 2016 DARPA Cyber Grand Challenge, Mayhem took first place amongst 110 teams that were competing. The competition, from the Defense Advanced Research Projects Agency (DARPA), focused on automatic cyberdefense systems and looked for a solution that created automatic defensive systems capable of reasoning about flows, formulating patches and deploying them on a network in real time.

Mayhem’s performance in the DARPA Cyber Grand Challenge showed fully autonomous security was possible. The key components that formulated Mayhem’s winning approach included:

- **Discovery/Vulnerability Identification**: Mayhem automatically found new vulnerabilities in commercial-off-the-shelf (COTS) software, even without developer participation.
- **Patching**: Mayhem automatically hardens programs.
- **Strategy**: The goal of cyber is to beat the attacker while still meeting mission and business objectives. Mayhem delivers by focusing on usability and integration into the development pipeline.

Mayhem “tests like a hacker” to find exploits. Mayhem is faster, more accurate, and less expensive than manual approaches and is truly automated, because it is not necessary for humans to double check the results.
Introducing Mayhem to The DoD

In 2020, Mayhem by ForAllSecure was awarded a contract of up to $45 million with the Defense Innovation Unit (DIU) for Project Voltron. The partnership was leveraged to design Mayhem after the DoD’s needs, allowing Mayhem to be rapidly and meaningfully iterated and improved upon using direct feedback from critical users, leading to a much accelerated time to value.

The Result

The DoD has expanded Mayhem’s software solution into some of their most critical systems. Over a dozen DoD organizations leverage Mayhem for either operational cybersecurity programs or to accelerate DevSecOps and comply with MDA or NIST guidelines. Mayhem has helped the DoD achieve its mission to test critical software, including weapon systems, both with and without developer participation.

Mayhem Beyond Federal

With its ability to automatically find exploitable bugs before attackers can, Mayhem is what modern application security looks like.

Since being contracted by the federal government, Mayhem has found other markets where software can make or break the mission, such as in aerospace, automotive, and core internet infrastructure.

Mayhem automatically generates and runs thousands of tests per minute to uncover defects in your code, while self-learning algorithms expand test coverage. Say goodbye to false positives with automated triage and reproduction. Our results are actionable, reproducible, and prioritized just for you. Discover how our developer-first app and API security testing solution can enhance your DevSecOps workflow.

Get a Demo