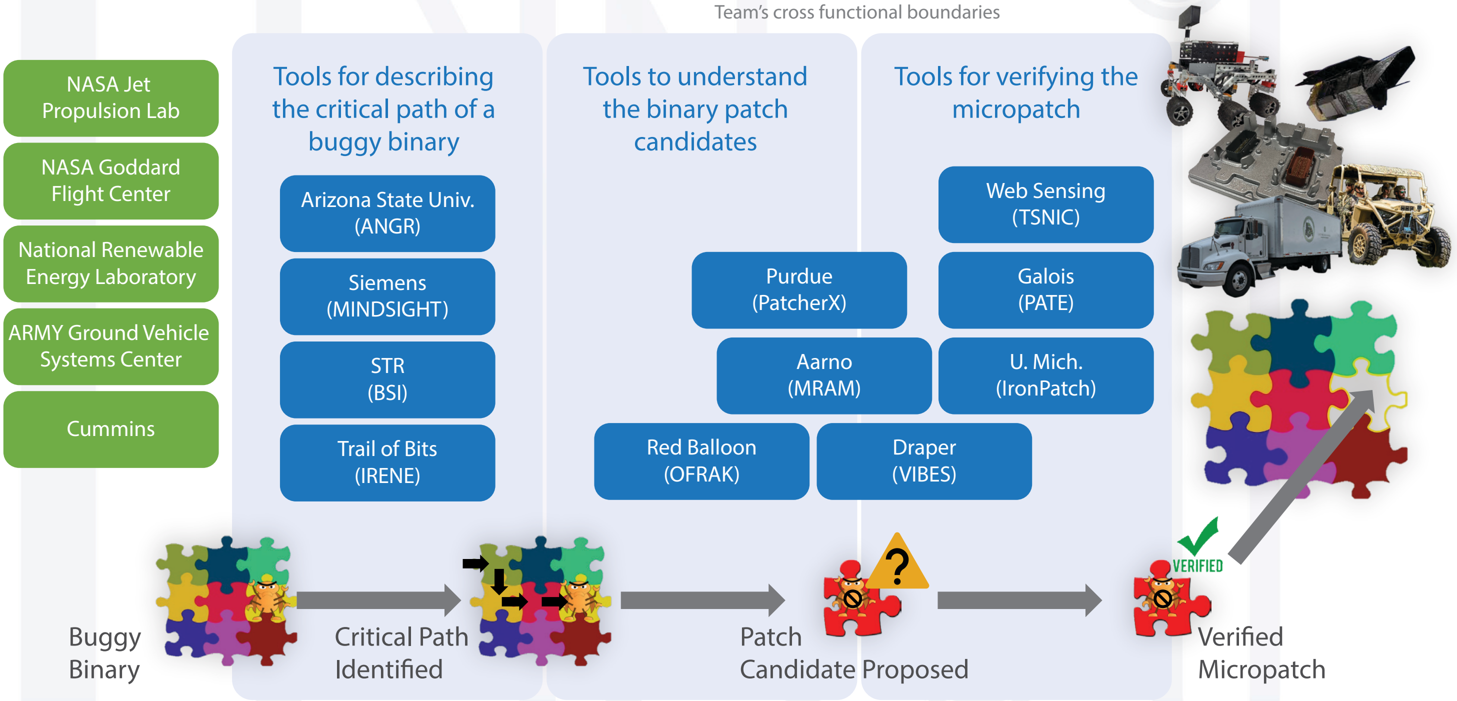
DARPA / I2O
Assured MicroPatching (AMP) Program

The Assured McroPatching (AMP) program produced targeted micropatches to repair legacy binaries of Department of Defense (DoD) mission-critical systems, with strong guarantees that the patch will not impact the functions of the system. It enables emergency patching of software in critical defense systems that are vulnerable to adversary attack. AMP created a capability to analyze, modify, and fix legacy software in binary form when the original source code version and/or build process is not available. AMP produced micro-patches for known vulnerabilities in embedded systems, with proofs that the patches will preserve the original functionality of the system. With these proofs, the time to test and deploy the patched system is reduced from months to days. National security depends upon the correct and trustworthy operation of its critical defense systems and the ability to rapidly update or patch systems in times of conflict. The technologies developed in this program can quickly and accurately patch legacy code in binary form when cyber-attacks occur in critical defense systems that our military forces depend on for planning and operational Command, Control, Communications, Computers and Intelligence (C4I). The diagram below depicts the AMP tools associated with the AMP program roles.



Team's cross functional boundaries

NASA Jet Propulsion Lab

NASA Goddard Flight Center

National Renewable Energy Laboratory

ARMY Ground Vehicle Systems Center

Cummins

Tools for describing the critical path of a buggy binary

Arizona State Univ. (ANGR)

Siemens (MINDSIGHT)

STR (BSI)

Trail of Bits (IRENE)

Tools to understand the binary patch candidates

Purdue (PatcherX)

Aarno (MRAM)

Red Balloon (OFRAK)

Draper (VIBES)

Tools for verifying the micropatch

Web Sensing (TSNIC)

Galois (PATE)

U. Mich. (IronPatch)

Buggy Binary → Critical Path Identified → Patch Candidate Proposed → Verified Micropatch

Distribution Statement A – Approved for Public Release, Distribution Unlimited

DARPA

AMP Open-source tools are changing the landscape

Tools for describing the critical path of a buggy binary:

Anger Management: Provides high-quality decompilation for binary code and offers unique capabilities, such as manual refactoring of decompilation output, viscous patching, and better decompilation output for compiler-optimized binary code

Integrated Reverse Engineering Environment (IRENE): Binary patching framework built on the **Ghidra** reverse engineering framework that produces patch definitions localizable to a minimal region of a binary

Binary Structure Inference (BSI): Matches binaries to source code in a target binary using **Binary Ninja** GUI

Tools to understand the binary patch candidate:

Open Firmware Reverse Analysis Konsole (OFRAK): Automatically unpacks, analyzes, modifies, and re-packs nested firmware binaries with an extensible Python framework

Patcherex: Binary patching tool, offering an easy-to-use Python interface to modify compiled code, even when the original source code or the original compilation tool-chain is unavailable - **integrated with angr**

Verified Incremental Binary Editing Synthesis (VIBES): From "Patch & Pray" to "Patch and Verify"!

CodeHawk: High assurance binary patching for the masses! – has a **Binary Ninja** plugin

Tools for verifying the micropatch:

PATE Verifier: Interactive verification of binary patch effects

Links:

AMP Tool Catalog
https://creative.spa.com/?s=amp-catalog-2

DARPA Resilient Software Systems Demo Day videos
https://www.youtube.com/playlist?list=PL6wMum5UsYvZhEOoP4YtAwtZdLSBIAltk

Resilients Software Systems
Stephen Kuhn
stephen.kuhn@darpa.mil

AMP Program Manager
Dan Wallach
daniel.wallach@darpa.mil

Distribution Statement A – Approved for Public Release, Distribution Unlimited