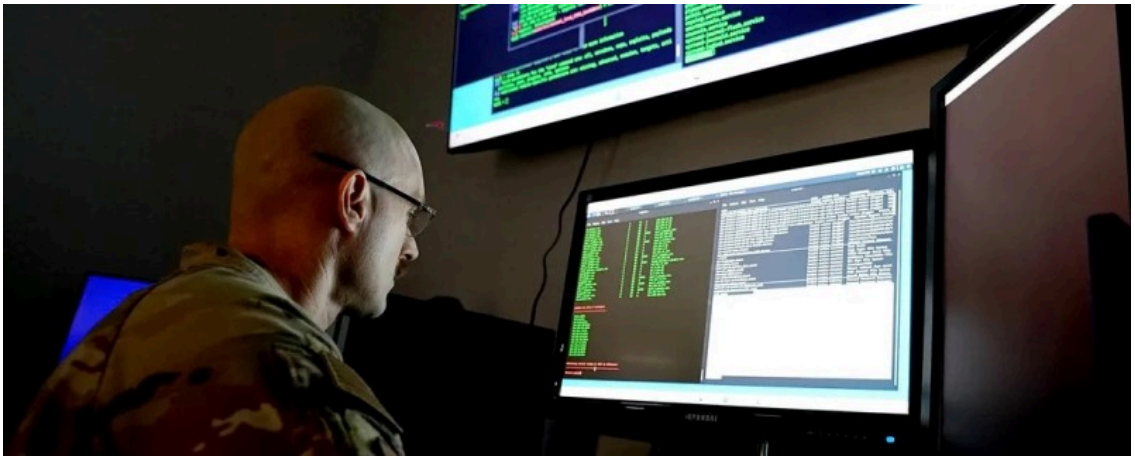
SEI Bulletin 40 years



SEI Parser Demystifies Firmware to Fight Vulnerabilities

January 7, 2026 — Most computer firmware is based on the Unified Extensible Firmware Interface (UEFI) standard. Largely invisible to users, critical to basic computer functionality, and sparsely documented, UEFI-based software is an inviting target for attackers. To make UEFI and other low-level, opaque software more accessible to vulnerability researchers, the SEI's CERT Division recently released the CERT UEFI Parser, an open source tool that enables inspection and analysis of UEFI software.

The opaque anatomy and workings of UEFI software greatly slow independent security analysis, which is critical when widespread firmware vulnerabilities emerge, such as the one targeted by the BlackLotus malware. "Firmware exploits against sensitive environments give attackers two major advantages: invisibility and persistence," said SEI vulnerability analysis team lead Vijay Sarvepalli. "Our goal is to combat both by making firmware far more inspectable at scale."

The CERT UEFI Parser can currently recover around 600 data structures, giving researchers a map of an entire firmware ROM. Researchers are

invited to use the tool, build on it, and report unsupported elements to enhance UEFI security analysis.

Read more »

SEI News

New Guidance Helps Defense Programs Get on the Software Acquisition Pathway
The guide is the first release in the Software Acquisition Go Bag series of resources for defense software programs seeking to advance acquisition practices.

SEI and Accenture Partner to Develop AI Adoption Maturity Model
Organizations can use the maturity model to establish a baseline for adopting artificial intelligence and roadmap future investments, according to a new SEI paper.

See more news »

Latest Blogs

Analyzing Partially Encrypted Network Flows with Mid-Encryption *(Steven Ibarra, Mark Thomas)*
Encrypted traffic has come to dominate network flows, which makes it difficult for traditional flow monitoring tools to maintain visibility. This post looks at a new feature added to CERT's Yet Another Flowmeter (YAF) tool to capture the attributes of encryption when it occurs after the start of the session.

Tailoring 9 Zero Trust and Security Principles to Weapon Systems
(Christopher Alberts, Timothy Morrow, Rhonda Brown, Charles Wallen)
This post outlines how 9 zero trust and security principles might apply to weapon systems.

See more blogs »

Latest Podcasts

Orchestrating the Chaos: Protecting Wireless Networks from Cyber Attacks
Joseph McIlvenny and Michael Winter discuss common radio frequency (RF) attacks and investigate how software and cybersecurity play key roles in preventing and mitigating these exploitations.

From Data to Performance: Understanding and Improving Your AI Model
Drift in data and concept, evolving edge cases, and emerging phenomena can undermine the correlations that AI classifiers rely on. Linda Parker Gates, Nicholas Testa, and Crisanne Nolan discuss a new tool to help improve AI classifier performance.

See more podcasts »

Latest Publications

SWP Essentials Kit
This collection of assets focuses on understanding the Software Acquisition Pathway (SWP).

A Preliminary Report on a Model for Maturing AI Adoption: From Hype to Achieving Repeatable, Predictable Outcomes *(Ipek Ozkaya, Anita Carleton, Matthew Butkovic, Sebastián Echeverría, Robert Edman, John Haller, Erin Harper, Michael Konrad, Natalie Schieber, Carol Smith, Shawn Wray)*
This report introduces the key concepts of a model for AI adoption, which will provide organizational leaders with guidance on overcoming the challenges that arise as they try to realize the promise of AI.

A Practitioner's Guide to Designing and Developing Hands-On Cybersecurity Skilling Continuation Labs *(Richard Weise, Christopher Herr, Nicholas Giruzzi)*
This report describes Skilling Continuation Labs that provide novel, relevant, and unique hands-on immersive training for the federal cybersecurity workforce.

See more publications »

Latest Videos

For those on the Software Acquisition Pathway (SWP), how do we catch problems before they escalate?
Brigid O'Hearn explains how to catch problems before they escalate for those on the Software Acquisition Pathway (SWP).

How do we scope and sequence an MVP, MVCR, and subsequent releases?
Brigid O'Hearn explains how to scope and sequence MVP, MVCR, and subsequent releases.

See more videos »

Upcoming Events

Webcast - Right-Sized DevSecOps: How Tooling Complexity Breaks Modern Pipelines, January 7
Joseph Yankel, Vaughn Coates, and David Shepard discuss how right-sizing DevSecOps restores velocity and reliability.

Webcast - Software Acquisition Pathway: Ready, Set, Go!, January 12
Julie Cohen, Brigid O'Hearn, and Eileen Wrubel walk through the new Tactical Guide for the Software Acquisition Pathway.

See more events »

Upcoming Appearances

Hawaii International Conference on System Sciences (HICSS), January 6-9
SEI researchers are chairing the mini-track "AI-Driven Program Analysis and Software Synthesis" in the HICSS 59 Software Technology Track.

AIAA SciTech Forum 2026, January 12-16
Visit the SEI at booth 106.

AFCEA WEST 2026, February 10-12
Visit the SEI at booth 817.

See more opportunities to engage with us »

Upcoming Training

Insider Risk Management: Measures of Effectiveness
February 18-20 (SEI Live Online)

Insider Threat Program Manager: Implementation and Operation
February 24-26 (SEI Live Online)

E-learning - CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate

E-learning - Introduction to Artificial Intelligence (AI) Engineering

E-learning - Effective Communication of Technical Concepts

Online registration is now available for 2026 public courses, both live online and in person.

See more courses »

Employment Opportunities

Principal Financial Analyst

Senior Financial Analyst

Reverse Engineer Researcher

All current opportunities »

Carnegie Mellon University
Software Engineering Institute