**Andrew Lilley Brinker** alilleybrinker@gmail.com • (951) 836-8902

**Securing critical infrastructure for software trust across supply chain security, artifact identity and dependency tracking, vulnerability management, and memory safety.**

## Roles

Principal Cyber Security Engineer (2015–present), Group Lead (2019–present) / MITRE

- Hipcheck: Founded and leading development of Hipcheck, an automated supply chain risk assessment tool adopted across the Department of War; manage $2M in funding from multiple federal sponsors. Redesigned the architecture from a fixed analysis pipeline into an extensible plugin system supporting custom data sources, analyses, and policy rules.
- Group Lead: Leading groups ranging from 5 to 14 staff. Advanced staff careers, including promotions to Senior Principal level.
- OmniBOR Core Team: Co-leading the OmniBOR standard for reproducible software artifact identity and fine-grained dependency tracking, cited in CISA's 2023 Software Identification Ecosystem analysis; built and maintain its Rust reference implementation.
- Common Vulnerabilities and Exposures (CVE): Leading authn/authz redesign for the CVE Services API — the backbone of the world's largest vulnerability-tracking system, serving 530 international CNAs. Introduced Package URL (PURL) support in the CVE Record Format. Redesigned the CVE Quality Working Group's processes for broader public engagement.
- Advisor, Office of the Undersecretary of War for Research & Engineering: Advise on DoW software bill-of-materials (SBOM) policy, including evaluation of investment in "XBOM" (eXtensible BOM) concept.
- White House RFI: Contributed to MITRE's federal RFI response on open source security that helped shape the White House directive on memory-safe programming languages.
- OSS Policy Jam: Organized event on open source software security featuring representatives from Apple, Microsoft, Cisco, Red Hat, Google, Linux Foundation, CISA, and more.

## Teaching

Course Creator & Instructor, “Introduction to Rust” (2019, 2026) / MITRE

Adjunct Lecturer, “CSE 320: Introduction to Programming Language Theory” (2017) / CSUSB

## Editing

Pre-Publication Reviewer, “C++ Safety, in Context” by Herb Sutter, ISO C++ Chair (2024)

Technical Editor, “Write Powerful Rust Macros” (2023–2024) / Manning Publications

## Writing

“Memory Safety for Skeptics,” ACM Queue (2025), republished Communications of the ACM (2026)

“Conditional Impls,” Possible Rust (2026)

“Open Source Software and Corporate Influence” (2025)

“C++ Must Become Safer” (2024)

"What Can Coerce, and Where, in Rust," Possible Rust (2021)
"3 Things to Try When You Can't Make a Trait Object," Possible Rust (2021)
"Non-Generic Inner Functions," Possible Rust (2020)
"AI & National Security: A Primer," Instick Media (2019)

### Speaking

"Memory Safety and the Future of Vulnerabilities," Cal Poly Pomona SWIFT Tech Symposium (2025)
"Software Identity in the Vulnerability Management Ecosystem" panel, VulnCon (2025)
"A Tale of Teaching Rust," Rust Conf (2017)
"Hello and Welcome: Documentation in the Rust Ecosystem," Rust Belt Rust (2016)

### Skills & Technologies

Rust (Expert. Writing Rust since 2014, pre 1.0. Taught to undergraduates and MITRE employees)
Software Identification (OmniBOR, Package URLs, CPEs)
Common Vulnerabilities and Exposures (CVE) (CVE Automation Team, CVE Quality Working Group)
Software Bills of Material (SBOMs) (SPDX, CycloneDX, SBOM Policy)
Supply Chain Security Analysis (Hipcheck)
Supply-chain Levels for Software Artifacts (SLSA)

### Education

Master of Computer Science, Rice University (2021–2023) 4.0 GPA
B.S. Computer Science, Math Minor, CSUSB (2011–2015) Magna Cum Laude