
Austin Tyler Conn

user@austinconn:~\$ resume --role defense

Cyber Software Engineer · Reverse Engineer / Vulnerability Researcher · Embedded Engineer · Software Engineer
Hamilton, Ohio 45013 austin@austinconn.org 513.432.5631 [linkedin.com/in/austin-conn-3030](https://www.linkedin.com/in/austin-conn-3030) github.com/dynacylabs
Active TS/SCI clearance.

▣ Tailored view – Defense / Cleared

SUMMARY

TS/SCI-cleared cyber software engineer with 5+ years at Northrop Grumman supporting multiple classified defense programs and 25+ customer deliveries. Experience across software development, reverse engineering, and test automation (internal test frameworks and GitLab CI), plus security research. Recognized with a BRAVO award for a rapid, quick-turnaround customer delivery that fulfilled urgent warfighter needs. Background also spans IT management and extensive open-source reverse-engineering tooling.

WORK HISTORY

Northrop Grumman Corporation – Cincinnati, Ohio

Program names and mission specifics omitted; descriptions generalized to releasable technology and skills only.

Cyber Software Engineer 02/2023 – Present

- Serve as a software engineer across multiple classified defense programs, with a focus on reverse engineering and low-level embedded development.
- Designed and implemented a software emulator for a software-defined radio (SDR) payload, implementing TCP/UDP and serial communication protocols using object-oriented design (inheritance and polymorphism).
- Delivered design and implementation of new product features; contributed to 25+ major customer deliveries across programs over tenure.
- Collaborated within program teams and coordinated across multiple teams and programs; mentored and helped onboard teammates.

Associate Cyber Software Engineer 08/2020 – 02/2023

- Test-automation engineer across defense programs, using an internal test framework and GitLab CI runners in support of multiple customer deliveries.
- Maintained and extended large program-specific automated test suites and GitLab CI pipelines (across multiple runners), and contributed upstream fixes to a shared internal test-framework repository used across programs.
- Received a BRAVO award for a rapid, quick-turnaround customer delivery that fulfilled urgent warfighter needs (in support of multiple quick-reaction capabilities / QRCS).
- Performed security research and reverse engineering of widely used software and hardware, including GPS and RF technologies and microcontroller-based systems (notably ARM and PowerPC).

Cincinnati Precision Instruments – Cincinnati, Ohio

Information Technology Manager 02/2019 – 05/2020

- Managed all IT operations and a \$300,000 IT budget, streamlining processes to cut operating costs by \$50,000.
- Led an IT department of 3 employees, recruiting, hiring, and conducting performance reviews for 2 college co-op / intern positions.
- Liaised with vendors and team members to promote ongoing network design; reevaluated and optimized systems and software to scale with company growth.
- Analyzed network security and infrastructure, recommending and installing upgrades across 55 workstations.
- Performed detailed risk/constraint assessments, identifying 6 major areas of unaccounted risk, and developed mitigation strategies and upgrades.
- Built and maintained a production virtualization environment of 12 business-critical virtual machines; streamlined processes using IndySoft and QuickBooks.

Software Developer / Software Engineer 01/2016 – 02/2019

- Analyzed, designed, administered, and supported 8 Microsoft SQL databases, including backup and migration strategies, with rigorous pre-deployment testing and post-deployment issue resolution.
- Designed, built, documented, and tested 28 major internal projects (12 new, 16 existing) using VBScript, C#, Java, Pascal, and Delphi, consistently surpassing client expectations.

TECHNICAL SKILLS

Programming Languages: Python, C, C++, C#, Java, Assembly, VBScript, Pascal, Delphi (plus shell scripting; JavaScript/TypeScript and Go via open-source work).

Reverse Engineering & Vulnerability Research: Binary and firmware reverse engineering (static and dynamic analysis); Ghidra (custom processor modules, loaders, and scripting); fuzzing / vulnerability discovery (libFuzzer and harness development) and crash triage; custom/proprietary protocol analysis and emulation (TCP/UDP, serial, TDLs). Tooling: Ghidra, Fireflight, TAU, Nmap, Metasploit, OpenVAS, Wireshark, Snort, sguil, libFuzzer, SonarQube.

Processor Architectures / ISAs: Xtensa (incl. ESP32/Tensilica), ARM (32- and 64-bit / AArch64), MIPS, PowerPC.

Embedded & Low-Level: Bare-metal C/C++ on microcontrollers (register-level programming); RTOS-based development; bus and I/O protocols (GPIO, UART/serial, SPI, I2C, TCP/UDP); hardware debug/programming interfaces (JTAG, SWD); firmware extraction and parsing (e.g., ESP32 flash dumps).

SDR / RF & Signals: Software-defined radio payload emulation and integration; SDR hardware (HackRF, RTL-SDR, BladeRF); Universal Radio Hacker (URH) for wireless-protocol reverse engineering.

Databases: Microsoft SQL Server (MSSQL), MySQL.

Systems, Networking & DevOps: Ubuntu Server 14.04 and later, macOS 10.8 and later, Windows 7/10/11, Windows Server 2008+, Cisco, GitLab CI runners, Docker, Nginx/reverse proxies, self-hosted infrastructure, virtualization.

Tooling & Other: LaTeX, Git/GitHub, IndySoft, QuickBooks.

EDUCATION

University of Cincinnati – Cincinnati, Ohio

- Master of Science, Computer Science (May 2025)
- Bachelor of Science, Information Technology — Cybersecurity Track (2020)

Cincinnati State Technical and Community College – Cincinnati, Ohio

- Associate of Applied Science, Software Engineering

OPEN-SOURCE & NOTABLE CONTRIBUTIONS

Ghidra – Xtensa Processor Support

Developed a Tensilica Xtensa processor module for Ghidra (the architecture behind the ESP8266/ESP32) and contributed it upstream to the NSA's open-source Ghidra project. Xtensa support is now included in Ghidra as of version 11.0.

[Upstream PR](#) · [Repo](#)

PERSONAL PROJECTS

Flagship – ESP32 / ESP-IDF Reverse-Engineering Toolchain for Ghidra

Built a complete toolchain for reverse engineering ESP32/ESP8266 firmware in Ghidra: a Tensilica Xtensa processor module (register windowing, MAC16, loop options) contributed upstream and now in Ghidra 11.0; an ESP32 flash-dump loader and firmware-image parser; a CMSIS-SVD peripheral loader; Ghidra Data Type (GDT) archives for the ESP-IDF SDK; and auto-generated Rizzo/FunctionID function signatures across IDF v2.0–v5.1.

[Xtensa module](#) · [Flash-dump loader](#) · [Image parser](#)

VOLUNTEER & AWARDS

Ohio Cyber Reserve (OhCR) – Southwest Ohio Region

- 02/2020 – 08/2021
- 08/2022 – 11/2023

BRAVO Award (Northrop Grumman)

For a rapid, quick-turnaround customer delivery that fulfilled urgent warfighter needs (in support of multiple quick-reaction capabilities / QRCs).

Tailored resume – full resume & project portfolio at resume.austinconn.org