# Austin Tyler Conn

user@austinconn:~$ resume --full

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 github.com/dynacylabs

**Active TS/SCI clearance.**

## ## SUMMARY

Cyber software engineer with 5+ years at Northrop Grumman, designing and delivering software for classified defense programs — including an object-oriented software-defined radio (SDR) payload emulator — alongside development test analysis and test automation. Background also spans IT management and database administration for a precision-instruments manufacturer, and embedded/low-level systems: bare-metal C on microcontrollers, firmware reverse engineering, and processor/ISA tooling, up to Python application and API-client development. Prolific open-source builder with a large portfolio of reverse-engineering tools, IoT device integrations, API-client libraries, and self-hosted infrastructure. Holds an active TS/SCI clearance.

## ## 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.
- Worked directly with clients to establish problem specifications and system designs; collected feedback across planning, development, and release phases and addressed concerns directly.
- Designed, built, documented, and tested 28 major internal projects (12 new, 16 existing) using VBScript, C#, Java, Pascal, and Delphi, consistently surpassing client expectations.

**Bugaboo Controls** — Cincinnati, Ohio

*Progressed from Specialist to a senior Foreman role; senior individual contributor rather than people manager.*

**Control System Specialist → Control Panel Foreman** 2013 – 2015

- Designed, laid out, machined, assembled, and wired high-voltage industrial control panels across a range of applications — industrial/factory automation, HVAC and building systems, water/utility systems, and custom OEM machine builds.
- Programmed and worked hands-on with Allen-Bradley / Rockwell and Siemens programmable logic controllers (PLCs), variable frequency drives (VFDs), and electromechanical and solid-state relay logic.
- Consulted with the Engineering Department on discrepancies in dimensions, wiring specifications, panel layout, and incompatible parts prior to manufacture.
- Performed load and functionality testing of control panels, documenting all test procedures, corrections, and errors in conformance with Underwriter Laboratories (UL) specifications.

## ## 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).

**Industrial Control Systems (ICS):** Allen-Bradley / Rockwell and Siemens programmable logic controllers (PLCs), variable frequency drives (VFDs), electromechanical and solid-state relay logic, high-voltage control-panel design, and UL-conformant panel testing.

**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

### ESP32 / ESP-IDF Reverse-Engineering Toolchain (Ghidra)

Built an integrated suite of tooling for reverse engineering ESP32 firmware in Ghidra — combining the Xtensa processor module, an ESP32 flash-dump loader, a firmware-image parser, a CMSIS-SVD peripheral loader, Ghidra Data Type (GDT) archives, and auto-generated function signatures (Rizzo / FunctionID) derived from ESP-IDF example binaries across IDF versions v2.0–v5.1.

Flash-dump loader · SVD loader · Image parser · GDT archives · Rizzo signatures

### Ghidra AI Auto-Analysis Scripts

A set of Ghidra scripts that drive AI-assisted auto-analysis of binaries — automating function identification, labeling, and annotation to speed up reverse-engineering workflows.

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

### Highlight — YoLink Smart-Home Reverse Engineering (Case Study)

Self-directed reverse-engineering deep dive into YoLink's ESP32-based smart-home ecosystem. Reverse engineered the hub/gateway and battery-powered LoRa sensors at the firmware level using ESP32 flash extraction, Ghidra static analysis (via the Xtensa/ESP32 toolchain above), and FCC teardown intelligence (YoSmart, FCC ID 2ATM7). Recovered the security keys governing the sensor → hub → ChirpStack (LoRaWAN) data path and mapped device onboarding. YoLink shipped official local control before the project reached that goal, so it stands as a deep technical exercise rather than a released integration.

RE write-up · yolink

### Automotive / Embedded

Set up comma.ai openpilot (open-source ADAS / driver-assistance) on a Volkswagen MK6 Golf — hands-on vehicle CAN-bus integration and embedded automotive hacking.

Repo

### IoT Device Reverse Engineering & Integration

A range of exploratory projects to reclaim control of consumer devices and their data — kept public for the open-source community rather than actively maintained: Python libraries and bridges for Blink cameras (including a Blink-to-RTSP bridge); tools for Ford (a FordPass widget and a downloader for Ford service manuals); a Node CLI to download VW/Audi erWin service documents (session-auth plus magic-byte file-type detection); and drone photogrammetry work that included reverse engineering the Dronelink protocol used to programmatically control DJI drones.

Blink bridge · Blink library · FordPass widget · Ford manuals · erWin downloader · Dronelink RE

### API Client Libraries (Python)

Authored several Python API clients, led by Pynab — a full-featured library for the YNAB (You Need A Budget) API and the most-starred project in the portfolio (~53 stars) — plus clients for Have I Been Pwned, LastPass, CPAP machine data, and voip.ms.

Pynab · Have I Been Pwned · LastPass · CPAP · voip.ms

### Software Tools & Automation

AIrganizer — an AI-powered file-organization pipeline that recursively scans files, extracts metadata (EXIF, binwalk, MIME), analyzes each file with the best-fit AI model (OpenAI, Anthropic, or local Ollama), then proposes names, tags, and a hierarchical taxonomy and physically reorganizes the files; features full resumability via a permanent cache, dry-run mode, and privacy-focused local-model support. Also built reusable dev tooling: a Python project template, a GitHub fork-syncer, and Backblaze B2 Docker backups.

AIrganizer · Project template · Fork-syncer · B2 backups

### Home Lab & Self-Hosting (software)

Runs a self-hosted software stack — bastion/jump host, Docker with automated image updates and container self-healing, an Nginx reverse-proxy manager, Cloudflare dynamic DNS, self-hosted wiki/docs, task management, and a personal/family medical-record aggregator — plus 3D-printing tooling (image-to-STL generation) and personal-data exporters.

jumpbox · watchtower · docker-autoheal · nginx-proxy-manager · cloudflare-ddns · docmost · tududi · fasten-onprem · AutoForge (3D→STL) · imessage-exporter

## HOME LAB (INFRASTRUCTURE)

- **Containerization** — Docker-based environment managed via Portainer.
- **Networking** — Managed networking gear (including WiFi HaLow), network segmentation, and reverse proxies.
- **Self-hosted services** — Docker-based services, backup/restore, DNS, wiki/docs, and monitoring.
- **Electronics bench** — Hardware-hacking / embedded workbench (soldering, debug and analysis gear) supporting firmware and IoT reverse-engineering work.

## 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).

## INTERESTS

Hardware and electronics (embedded tinkering, hardware hacking, home-lab bench work); automotive (openpilot / driver-assistance, VW and Ford tinkering, CAN-bus hacking); home automation and self-hosting (DIY IoT and reclaiming devices/data from vendor clouds); 3D printing and making.