Roman LEONOV



Embedded Software Engineer

Berlin, Germany · leonovro@mail.de · +49 176 26006147

LinkedIn · GitHub

SUMMARY

Embedded Software Engineer with 13+ years of experience in C, RTOS, and bare-metal development, combining low-level software expertise with a hardware background in circuit design and PCB layout. Architected and shipped 11 flagship devices with more than 1M units in production. Built and led an embedded team of 5 engineers (3 direct reports), growing the function from a solo effort into a structured development group. Deep expertise in USB Host/Device, cryptography, and hardware-software debugging using JTAG/SWD, protocol analyzers, and oscilloscopes. Ranked #1 contributor to ESP-USB component development in Espressif's ESP32 IoT Development Framework in 2024–2025, with additional open-source contributions to the Zephyr RTOS USB Host stack.

SKILLS

Embedded Software & RTOS: Embedded C, Zephyr RTOS, FreeRTOS

CPU Architectures & Microcontroller Platforms: ARM Cortex-M series, Xtensa, RISC-V

Interfaces & Protocols: USB, UART, SPI, I²C, SDMMC, 1-Wire, CAN, NFC

Security & Cryptography: PKI, ECC, RSA, SHA, AES, DES

Hardware & Debugging: Circuit design (KiCad), hardware debugging and board bring-up, USB protocol analysis

Tools & Automation: GCC, Git, GitHub Workflows/Actions, Python, CI/CD pipelines

EXPERIENCE

Senior Software Engineer · Espressif Incorporated · Berlin, Germany (Remote) · 10.2022 – 11.2025

Espressif develops ESP32 microcontrollers and systems-on-chip (SoCs) with Wi-Fi/Bluetooth connectivity, along with software for connected and IoT devices.

Stack: Embedded C, ESP-IDF, FreeRTOS, TinyUSB, DWC2, USB protocol analyzers, Python, GitHub Actions/CI

Worked on the ESP-IDF USB subsystem from silicon bring-up through production software integration, designing stack architecture and public APIs and developing USB Host and Device functionality. Also owned Espressif's TinyUSB integration, including platform adaptations, upstream synchronization, CI, and release maintenance.

- Designed and implemented the first external USB hub support in the ESP-IDF USB Host stack while preserving the existing client API; implemented the hub driver and port state machine and added 10 dedicated test cases. The functionality was used without stack-specific modifications in a public Embedded World 2025 demo running two UVC cameras through a USB hub.
- Refactored legacy USB device enumeration into a dedicated queued state-machine driver, establishing the architectural foundation for hub topologies and handling multiple

concurrently discovered devices. Added 37 test cases, including failure-path scenarios using a reconfigurable TinyUSB mock device to inject errors at individual enumeration stages.
- Implemented teardown and reinitialization for the ESP-IDF TinyUSB Device stack, enabling automated DUT reconfiguration without power cycling; added Espressif-specific hardware-in-the-loop CI across ESP-IDF v5.1-v6.0 and ESP32-S2/P4 targets, with 23 automated hardware test runs covering device examples and integration test applications.
- Established and managed 6 milestone-based `esp_tinyusb` release cycles and maintained Espressif's TinyUSB fork across upstream upgrades, migrating platform-specific patches between release branches, resolving DWC2, API, and CI conflicts, and using staged synchronization to integrate validated upstream fixes without pulling in unfinished changes.
- Implemented ESP32-P4 cache support in TinyUSB and upstreamed the change into the main TinyUSB project, adding platform support directly to the upstream USB stack.

Career break · 05.2022 – 08.2022
Relocation to Germany.

Aladdin R.D. · Moscow, Russia · 12.2014 – 04.2022
Aladdin R.D. is a Russian cybersecurity company developing authentication and electronic-signature solutions, including the JaCarta product line. Ranked No. 5 in the TAdviser Security 100 by 2024 revenue.

Growth: Embedded Software Engineer → Embedded Software Team Lead

Led the technical evolution of the JaCarta 3 embedded platform from an initial R&D implementation into a reusable production architecture used across a family of USB security tokens and smart-card readers. Owned firmware architecture, platform development, provisioning and configuration infrastructure, and production programming processes for manufacturing runs of up to 500,000 devices.

Embedded Software Team Lead · 07.2017 – 04.2022
Stack: ARM Cortex-M, USB (CCID/HID/MSC), PKI (ECC/RSA/SHA/AES), JavaCard, Secure Element, NFC, JTAG/SWD, GRUB2

- Retained technical ownership of the JaCarta 3 architecture and led the continued development of the shared embedded platform, including architecture/code reviews, the boot/update subsystem, and migration of legacy functionality onto the common codebase.
- Scaled embedded development from an individual effort into a team: hired and mentored 5 engineers, distributed ownership across technical areas, and continued to directly manage 3 developers.
- Designed and implemented an x86 emulator for JaCarta 3, allowing the exact same C application code to run on both the emulator and ARM Cortex targets; the same test suite was used by the embedded team, QA, and adjacent teams without requiring physical hardware. Enabled the team to develop and validate platform applications, including the 3 major production PKI/RSA applications on the emulator/tooling infrastructure, separating application development from MCU and hardware integration.
- Designed the detailed architecture of a pre-boot authentication solution for a USB security device, including MSC storage / LUN layout, authentication protocol before loading of the OS, dynamic exposure volumes based on the authorisation roles, and

a cross-platform GRUB2 boot flow; the solution shipped in a 500K-unit production batch.
- Led smart-card reader development across firmware and hardware: designed a biometric authentication flow using the FingerCell library and JavaCard/Secure Element as secure storage, and performed bring-up and 13.56 MHz NFC antenna RF tuning for a contactless reader using Smith-chart measurements and matching-network optimization.

Embedded Software Engineer · 12.2014 – 06.2017
Stack: C, ARM Cortex-M, Nordic nRF51/nRF52, USB (CCID/HID/MSC), Flash/EEPROM, FatFS, RexOS, JavaCard, ISO7816, ISO14443A/B, NFC

- Architected the JaCarta 3 embedded platform, replacing product-specific monolithic firmware with a modular architecture built around a reusable platform layer and product-specific applications; the platform was later used across 11 production security devices.
- Designed a fault-tolerant dual-slot firmware update architecture: new images were written to the inactive Flash slot, cryptographically validated, and made bootable only after a final commit, keeping the previous firmware operational in case of power loss or interrupted updates.
- Strengthened firmware update security by replacing CRC-based integrity checks with a 32-bit keyed cryptographic MAC, adding encrypted firmware packages, version/downgrade validation, and a secure update flow over CCID/APDU.
- Redesigned persistent storage for embedded workloads by replacing FAT-oriented semantics with an EEPROM-like abstraction using 32-bit object IDs and 128-byte sectors, reducing unnecessary Flash erase/rewrite operations and adding transparent encryption for stored data.
- Developed 6 product-specific applications on top of JaCarta 3 Platform, all of which reached production devices, including functionality for OTP, U2F, and secure Data Storage.
- Implemented composite USB security devices combining CCID, HID, and Mass Storage, including support for up to 4 LUNs and dynamic removable-media switching after authentication by remapping SD-card regions.
- Ported the open-source RexOS to Nordic nRF51/nRF52, implementing MCU/platform support for UART, RTC, WDT, RNG, ADC, Flash, timers, power management, and RF; multiple pull requests were accepted upstream.

Firmware Engineer · WWPass Corporation · Moscow, Russia · 02.2012 – 11.2014 (part-time 02.2012 – 02.2013, then - full-time)
WWPass is a cybersecurity company developing hardware and software authentication solutions, including USB/NFC security tokens and smart cards. The company has 151-200 employees and is headquartered in Nashua, New Hampshire, USA.

Stack: C, ATmega32U2, USB, NFC (13.56 MHz), KiCad, SolidWorks

Developed firmware and hardware for PassKey and SecurityKey. PassKey and SecurityKey were USB/NFC hardware security tokens for cryptographic authentication. The devices combined embedded firmware, secure credential storage, and NFC/USB communication. Developed firmware and hardware for NFC/USB smart-card readers, designed the enclosure in SolidWorks, and manufactured prototypes using CNC machining.

- Designed hardware for ATmega32U2-based USB/NFC authentication tokens, including schematics, PCB layout, and 13.56 MHz NFC antenna matching using an antenna analyzer and Smith chart; the designs were used in production runs of approximately 10K PassKey and 15K Security Key devices.
- Improved USB enumeration reliability on ATmega32U2 by implementing watchdog-based recovery around a third-party USB stack, eliminating intermittent hangs during a 150-cycle compliance test and enabling the full test sequence to complete successfully.

Firmware Engineer · NIIRET BMSTU · 09.2011 – 02.2013
Research unit within the RL1 Department at Bauman Moscow State Technical University, working on engineering and applied research projects that also involve students in research, coursework, and thesis projects. The unit has approximately 10-15 research staff.

Stack: C (bare-metal), STM32F100, STM32F200, CC1101, UART

- Developed a distributed time-synchronization mechanism for a network of 200 CC1101-based wearable devices built on an STM32F200-based microcontroller, using time-slot allocation and reference-time propagation from a base node; achieved network-wide synchronization within ~5–10 seconds and reliable operation across a ~2-hectare forest field site during a three-day event.
- Designed and built an STM32F100-based antenna positioning controller for remote laboratory work, including schematic and PCB design, bare-metal firmware, and a custom UART protocol for PC-controlled azimuth and elevation; integrated the controller with the host software and brought the system to a working prototype.

EDUCATION

Engineer Degree · Bauman Moscow State Technical University · 09.2007 – 07.2013

Anabin status: H+.

WES evaluated equivalent degree certificate: Master’s Degree in radio and electronic systems development.

VOLUNTEERING

The Zephyr Project · USB area collaborator · 06.2026 – present
Collaborator in USB area on The Zephyr Project: a small, scalable open source RTOS for IoT embedded devices.

OTHER

- Authorized to work in Germany
- English (C1), German (B2), Russian (native)