John R. Graham

Winder, GA, USA | Phone (678) 777-6321 | [john@graham-family.org](mailto:john@graham-family.org) [https://www.linkedin.com/in/john-r-graham2](https://www.linkedin.com/in/john-graham-75b4431)

Principal Security Architect

An accomplished and innovative leader with extensive cross-disciplinary engineering experience in software, electrical, embedded systems, operating systems, security, manufacturing, continuation engineering, and overall architectural design, gives a unique ability to envision and architect extremely efficient, secure, and cost-effective systems that minimize costs over the cradle-to-grave product lifecycle. Experienced in designing products for very high volume, very low cost. Comfortable interfacing with large customers, vendors, and standards organizations. Strong on-going active interest in science, mathematics, technology, and industry provides a broad tool set to apply to problems.

Key Skills

* Experienced in a wide variety of programming languages, including C, C++, Python, Perl, AWK, RPL, PL/I, FORTRAN, and about half a dozen assembly languages including x86, 8051, MIPS, 8080, Z-80, TI MSP430, IBM 370, and (learning) ARM.
* Extensive Linux development experience on both desktop and embedded systems, including build systems, toolchains, tools languages, device drivers, build automation systems, and distribution maintenance tools (Gentoo Linux developer).
* Extensive bare-metal embedded systems development experience, including using in-circuit emulators / JTAG debuggers, logic analyzers, oscilloscopes, schematic evaluation, and RTOS integration.
* Experience with embedded systems communications protocols, including I2C, SPI, asynchronous serial / multi-drop, and USB.
* Expert in cryptographic algorithms including symmetric (e.g., AES, DES) and asymmetric (e.g., RSA, ECC) ciphers, key agreement protocols, Public Key Infrastructure / X.509, digital signatures, revocation, authentication, and secure boot / trusted boot.
* Knowledge of SQL databases (e.g., MySQL, MariaDB, SQLite) and the LAMP stack.
* Broad experience with CP/CA/DRM (Content Protection, Conditional Access, Digital Rights Management) systems including HDCP, DTCP, DOCSIS, Nagravision, Irdeto, Mediaroom, PlayReady, Widevine, NDS/Synamedia, Netflix.
* Comprehensive experience in point-of-sale technology and industry requirements:
* Electronic check conversion, electronic signature capture, online debit, credit, EBT, ACH, smart card.
* Payment security (both physical and logical) and industry standards (ANSI X9-TG-3, Visa PED / PCI PED, INTERAC.
* Excellent communications skills; good communicator across multiple layers of management.
* Adept team leader with experience managing full development teams.

Work Experience

**Vantiva** Norcross, GA 2022 – 2024  
**Technicolor SA** Lawrenceville, GA 2016 – 2022  
**Scientific Atlanta / Cisco Systems, Inc.** 2006 – 2016  
In 2006, *Scientific Atlanta* was acquired by *Cisco.* In 2016, our division was acquired by *Technicolor.* In 2022, *Technicolor* spun off *Technicolor Creative Studios* into an independent company, renaming the remainder (where I continued to be employed) *Vantiva.*

**Staff Embedded Software Engineer (Scientific Atlanta / Cisco)** 2006 – 2010

* Worked on Linux and Windows CE IP Set Top Boxes for delivery of high-definition video to the home over the Internet.
* Designed, implemented, and delivered cryptographic key provisioning “Black Box” systems to securely provide unique per device secrets to be burned onto our integrated circuit dies in chip fabs (principally ST Microsystems and Broadcom).
* Chinese contract manufacturing partner liaison (principally with Asus, Pegatron) for manu­facturing yield and cryptographic key provisioning systems.
* Established formal key management procedures (“ceremonies”) and systems for secure symmetric and asymmetric key material handling within our group.
* Designed in-group HSM-based key management and code signing system that allowed hardware-enforced split knowledge and dual control of all code signing key material.
* Participated in the adoption and evolution (although not the initial design) of Cisco’s Abraxas code signing system, which replaced the above in our group.
* Developed the hardware-specific bootloader code signing utilities and procedures for almost every trusted boot capable SoC (System on a Chip) that was used by our group.

**Technical Leader / Security Architect (Cisco)** 2010 – 2016

* Participated in the architecture development of a redundant, hardened, unique per device key package production facility and the secure transport mechanisms for delivering those keys to our factory partners. The key packages, once they’ve left the hardened production facility, could only be decrypted within the security envelope of the target SoC on the factory floor.
* Produced design documents and prototypes for myriad cryptographic key packages. Key packages were then produced in volume by our hardened production facility.
* Security architecture consultant to the bootloader teams through the evolution of two different internally-developed bootloader architectures:
* BL2.x, the first group bootloader that supported a cryptographically authenticated boot chain of trust, all the way from the hardware to the running application suite.
* BL3.x, added standards-based certificate chains for code authentication keys, conditional signing based on flexible criteria, granular hardware-anchored revocation, and key diversity (com­ponent-based and roles-based signing keys).
* Promoted signing key lifecycle processes, utilizing the above­mentioned hardware-anchored revocation capability, to min­imize the exposure of fielded systems to undetected vulnerabilities in old signed images.
* Participated in security “deep dive” evaluations of new SoCs to verify compliance with internal security best practices, and external CP/CA/DRM requirements.
* Principal contributor to the development, maintenance, and promotion of key management best practices for the entire business unit.
* Designed a secure “beacon” system to ensure that factory software running on our products can only run within the confines of our factories.

**Principal Security Architect (Technicolor / Vantiva)** 2016 – 2024

* Designed and implemented the secure transport protocols & procedures, to securely export our code signing keys from Cisco’s Abraxas HSMs in a form where they could be securely imported into Technicolor’s nascent TCH-SS replacement system’s HSMs.
* De facto systems and security architect for the TCH-SS code signing system, evolving it from a single host server to a globally redundant, high availability, fault-tolerant, ISO 27001-certified system.
* Led the ISO 27001 certification effort for TCH-SS from 2021 (its first certification year) to 2023, creating the documentation package and the requisite organizational structure with the required personnel redundancy and process reliability, achieving certification with no major corrective actions required by the auditor each year.
* Continued to produce design documents and prototypes for cryptographic key packages for Technicolor products.
* Continued to do security “deep dive” activities on new silicon and silicon vendors.
* Continued to participate in the maintenance and promulgation of security best practices.
* Developed and successfully pushed multiple silicon vendors to adopt generic signing call-outs, abstracting the signing primitives from the image signing software, to facilitate the use of our existing TCH-SS code signing infrastructure, ensuring that no production code signing key ever need be compromised.
* Security architect for BASE (Build Automation and Signing Eco­system). BASE provides a portal to select high volume customers to submit application images for automated signing for continuous integration, but implementing automated security controls to reject flawed or vulnerable images.
* To support evolving requirements and software migrations, designed systems to deliver new unique per device cryptographic key packages to set-top-boxes already deployed in customers’ homes.

**Inventech, Inc.** Lawrenceville, GA 2003 – 2006

**CTO and Principal**

A privately held corporation focusing on the development of ultra low cost secure authentication devices for Internet payment trans­actions.

**4Access Communications** Alpharetta, GA 2002 – 2003

A privately held corporation focusing on the development of a merchant terminal that would convert paper checks to electronic form at the point of sale.

**Vice President of Payment Technology**

* Set the technology direction, architecture, and contributed to the overall feature set of the *Orion* family of Linux-based all-in-one electronic check conversion payment terminals.

**Ingenico North America** Roswell, GA 2001 – 2002  
**IVI Checkmate, Inc.** Roswell, GA 1998 – 2001  
**Checkmate Electronics, Inc.** Roswell / Sandy Springs, GA 1990 – 1998

In 1998, *Checkmate Electronics* merged with *International Verifact* to form *IVI Checkmate.* In 2001, *IVI Checkmate* was bought by *Ingenico.*

**Vice President / CTO** 1995 – 2002

* Led a high profile, radical re-architecture and cost reduction effort on the fifth generation check reader design (the CMR-430). The most successful in the company’s history, this program realized over $4 million to the company’s bottom line annually.
* Defined a common architecture for the company’s product road map. Three products were ultimately built with the same underlying architecture, resulting in lower develop­ment and manufacturing cost. The product line ultimately achieved full chain roll-outs at Wal\*Mart, Kmart, Home Depot, and well over half of the 200 largest retailers in the US.
* After the merger, was named the chairperson of the company’s North American Architecture committee, recommending technology consolidation and architectural direction for the combined company’s product line.
* Wrote the *Architecture Manifesto,* advocating a larger role for global shared architecture con­sider­ations in the company’s product development process.
* Key advocate for incorporating Linux and an open systems architecture into the next generation of payment terminal products.
* Designed a security architecture that allowed an open system, touch screen based payment terminal, to be properly secure without onerously burdening the applications developer.

**Vice President of Software Engineering** 1992 – 1995

* Developed the software architecture for Checkmate’s first entry into the online debit payment terminal market: the CM2001.
* Led the software team that enhanced the company’s flagship check reader product line through six years and seven product generations.
* With the fifth generation check reader, the CMR-430, the product line crossed the 100,000-units/year manufacturing volume which peaked at 147,000 units/year, ultimately selling well over a million units.
* Major technical liaison with most of Checkmate’s flagship accounts such as Wal\*Mart, Kmart, J.C. Penney, and Federated Department Stores.
* Upon the untimely death of both the company’s CEO and VP of Engineering, became the company’s technical spokesperson with certain key accounts, convincing them that Checkmate still had the technical savvy to deliver on their product roadmap.

**Director of Software Engineering** 1990 – 1992

* Built the embedded software development team, including hiring and day-to-day management.
* Cost reduced and enhanced Checkmate’s flagship point-of-sale check reader.
* Reverse engineered over a dozen proprietary cash register interfaces in order to allow the check reader family to be seamlessly deployed.
* Managed all software development at Checkmate, managing a team of 7 developers.

Additional Relevant Experience

Resolution Systems Sandy Springs, GA 1989 – 1990  
Stanford Technologies, Inc. 1988 – 1989

Developed RS React, a combination software and hardware solution to analyze the causes of check misreads on large banking check reader / sorters. Successfully deployed at Bank South and Trust Company Bank.

Computer Consultants Athens, GA 1980 – 1988

Computer engineering consulting firm specializing in system software and device drivers for mini- and microcomputers.

Education

Program for Technical Managers, Georgia Institute of Technology Atlanta, GA

Math / Physics dual major, University of Georgia Athens, GA

Extracurricular Activities

* Avid reader of science fiction & fantasy, history of science & technology, and science & technology periodicals.
* Active volunteer developer on the Gentoo Linux distribution.
* Mountain biking, hiking, running, flying (private pilot), and chess.

Accreditations

* Certified ANS X9-TG-3 compliance auditor.