Paul D. Martin, Ph.D.

Chief Scientist, Harbor Experts · Lecturer in Computer Science, Johns Hopkins University

Professional Background

I am the Chief Scientist at Harbor Experts, Inc. and a part-time Lecturer in the Department of Computer Science at Johns Hopkins University. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science.

I serve as both a testifying and consulting expert in complex litigation involving software, cybersecurity, artificial intelligence, embedded systems, and computer hardware. I have testified at trial, in evidentiary hearings, and at deposition in federal and state courts, before the International Trade Commission, and in inter partes review proceedings before the Patent Trial and Appeal Board. I have served as a testifying or consulting expert in more than one hundred matters, and I have personally led more than one hundred large-scale source code reviews involving systems ranging from thousands to billions of lines of code. In these engagements, I have reconstructed system behavior, development history, and technical provenance from source code, binaries, and forensic artifacts — including in matters where source code was lost or unavailable, requiring binary reverse engineering and forensic reconstruction. My engagements have included matters involving many of the world's largest technology companies.

Validation and testing of technical claims are a consistent part of my professional work, research, and teaching. In litigation, I design and execute custom experiments to verify how systems actually behave, rather than relying on how they are documented or intended to behave, and I have evaluated the reliability and validity of forensic software — including computerized DNA analysis software — in criminal proceedings. I am currently a member of the IEEE 7024 Working Group, which is developing the "Standard for the Procurement, Verification and Validation, and Life Cycle Management of Forensic Technologies." I hold Six Sigma Black Belt and Green Belt certifications, reflecting formal training in data-driven measurement, statistical analysis, root cause analysis, and quality management. In my teaching at Johns Hopkins, my students identify potential vulnerabilities in real codebases and validate their findings by writing working exploits.

Teaching

I am a part-time lecturer in the Department of Computer Science at Johns Hopkins University. I currently teach classes on computer and network security, applied cryptography, and C and C++ programming, including developer tools and Linux environments. In the past I have taught classes on the topic of hardware hacking, including analyzing, modifying, and repairing computer hardware and embedded devices and vulnerability analysis and exploitation. I also occasionally guest lecture and substitute in other classes.

My classes cover a diverse array of topics including hardware and software security design, analysis and reverse engineering for vulnerability assessment; hardware and software-based attacks on computer components including RAM and CPUs; applied cryptography; computer architecture; computer networking; and component-level analysis and modification. My classes also utilize hardware and software emulation and virtualization techniques in order to present students with a variety of real-world environments in which to learn and perform hands-on projects. My security courses have a significant source code analysis component: students read through real codebases to identify exploitable vulnerabilities and then validate their findings by writing working exploits that achieve code execution — the same discipline of testing and validation that I apply to source code review and experimentation in litigation.

Research

In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, where I researched computer security and privacy systems, both designing novel technologies for securing computing systems and bridging the interface gap between users and their technology. My research focused not only on developing technical solutions to novel security and privacy problems but also on presenting those solutions in a way that non-technical users could understand. Some of my projects also focused on non-deterministically generating virtualized computer networks in order to provide malware education environments for students. I also developed an emulator for analyzing malware code segments as part of a project with the NSA. This emulator was integrated into an IDA Pro plugin and was able to observe how binary instruction snippets taken from malware samples modified their computing environment.

During my tenure as a Ph.D. student at Johns Hopkins, I was fully funded as a research assistant and/or teaching assistant throughout all of my semesters. I was a member of the Upsilon Pi Epsilon computer science honor society, as well as its treasurer for the 2014-2015 school year. I was also a member of the Johns Hopkins chapter of the Association for Computing Machinery. I earned the Computer Science Department Outstanding Teaching Assistant Award in 2014. I co-instructed a short course called "Introduction to Hardware Hacking" with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification; network traffic analysis; and web-based vulnerability assessment and exploitation.

During my time as a student at Johns Hopkins, I also participated in numerous kinds of service to the department. I represented the university as a student speaker at numerous open houses and admitted student days to help introduce prospective students to the computer science department. I was selected to speak to the external advisory board for the computer science department to provide insight into the student experience in the department. I served the department as the faculty liaison czar for several semesters, in which I attended and documented faculty meetings, which I then summarized for the students in the department. I also mentored and supervised a high school student on a year-long independent study project in software design and I supervised a variety of undergraduate research assistants on some of my own research projects.

I finished my Ph.D. by successfully defending my dissertation, entitled "Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare," on February 12, 2016. My doctoral research was advised by Dr. Aviel Rubin. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation, and error-proofing of security controls.

During my doctorate and afterward, I have produced, peer-reviewed, and published research in areas such as fingerprinting, anomaly detection, multifactor authentication, and embedded systems security. My research has been published in peer-reviewed venues including the ACM/IEEE International Conference on Internet-of-Things Design and Implementation, the ACM Conference on Bioinformatics, Computational Biology, and Health Informatics, and Financial Cryptography and Data Security. In many of these cases, I focused not only on designing novel security systems but also on designing usable interfaces for controlling them and understanding their data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which was funded in

part by Accenture Labs, I developed a Hadoop-based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed a web application to automatically produce human-readable reports and graphs for use in consulting. Accenture subsequently patented this technology.

Similarly, in my research at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a smart grid network as well as to detect unexpected anomalies in the network. This dashboard was able to aggregate and visualize multiple data streams in real time. Applied Communication Sciences subsequently patented this work and continued to build on the project, integrating it into their SecureSmart Managed Security Service product offering.

I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies, especially in healthcare settings. In one project, my co-authors and I designed an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of in order to be used as a secondary authentication mechanism for accessing patient medical records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical records of nearby patients. In another project, my co-authors and I designed an authentication bracelet that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. Upon use of other terminals throughout the hospital, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal in order to allow the user to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user.

My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection, and automated security enforcement. In one case, I designed Sentinel, a security system that can be soldered directly to the CPU of embedded devices in order to perform control-flow integrity for purposes of profile building and enforcement; this work was published at the ACM/IEEE International Conference on Internet-of-Things Design and Implementation. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices in order to build a software profile of the platform configuration of the device, which can then be cross-referenced with a vulnerability database. I personally wrote the patent specification for this technique, and I am the named inventor on the resulting patent. My current research includes the use of large language models for technical research and analysis, the use of multimodal large language models for diagnosis of disease progression, automated analysis of vulnerabilities in containers and virtual appliances, and large-scale comparison of the nature and kind of firmware vulnerabilities across and within product classes.

In 2023 and 2024, I served as a member of the program committee for the IEEE Symposium on Security and Privacy. As a member of this committee, I peer reviewed research that was submitted for publication at the Symposium, including research on memory forensics, side channel attacks, password vaults, differential privacy, computational theory, memory module design, and hardware security.

Patents

I am a named inventor on five U.S. patents. A full listing of these patents can be found on my curriculum vitae.

Industry

In 2007, I developed my first Linux distribution and an associated LiveCD build system, called PJAMAS. The Linux distribution was built on Gentoo, a source-based Linux distribution, and compiled from scratch to be a minimal desktop image that could fully boot and run on low-performance desktop computers that primarily ran the Windows operating system, and that could run Windows binaries under the WINE libraries. The ultimate goal of the distribution was to identify and remove malware from infected Windows computers. To achieve these goals, I tuned the kernel and operating system configuration, including performance-critical subsystems, to minimize RAM footprint, reduce runtime overhead, and constrain binary size, allowing the software to run on the widest possible range of Windows-era hardware. As an artifact of this process, I also produced a general-purpose build system for creating Gentoo-based Linux LiveCDs that could be custom-designed for any purpose.

This early work focusing on Linux, systems, and security became the focal point of my career and led me to select security, operating systems, and embedded systems as core areas of my professional work and research.

I began working in the software industry in 2008, when I obtained my first independent consulting client — Brandeis University. I created a program for their computer repair shop's ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets in order to easily identify customers' devices.

Shortly after finishing my engagement with Brandeis University, I began working for the Johns Hopkins University Digital Research and Curation Center as a student programmer. There, I created a batch importer for a digital archiving system called DSpace in order to enable hundreds of digitally archived works per week to automatically be added to the repository. I next ported a web interface for statistics tracking and visualization to the same digital archiving system in order to allow library staff to more easily visualize and understand data about how the digital archiving system was being used through a common web-based interface.

In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for iOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. Of note, I designed automation systems to create and restore virtualized snapshots of Windows machines on which I tested antivirus software on actual malware samples as part of a project for Consumer Reports. I worked for ISE throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy.

In February 2016, I joined Harbor Labs full-time as a research scientist. In 2018, I was promoted to Director of Firmware Security. In December 2023, I was promoted to Vice President of Applied Research and Technology. In October 2024, the division of Harbor Labs that I managed became Harbor Experts, and I became its Chief Scientist. At Harbor Experts, I manage client engagements related to all of the analysis work that Harbor Experts performs. I also lead Harbor Experts' research projects.

A substantial portion of my role at Harbor Experts is in managing source code review engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling in the millions or billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms, virtualization platforms, and numerous other products. I have also authored whitepapers on source code comparison, source code quality assessment, and the source code review process in litigation.

Prior to joining Harbor Experts, I was also the technical and development lead for a firmware security analysis engine for a product developed at Harbor Labs called Firmware IQ. Firmware IQ is designed to analyze the firmware of embedded devices for security vulnerabilities in an automated fashion. In one configuration of the product, a developer uploads a firmware image to a web-based portal which uses a broker to forward the firmware to an engine for analysis. The engine unpacks the firmware, breaks it into its constituent components, and then performs more than a hundred automated security checks in order to find vulnerabilities in the firmware image, including cross-referencing identified software components against NIST's National Vulnerability Database. The results are then reported through JSON to a web-based presentation system which displays them in an interactive fashion.

Since Firmware IQ, I have devoted a substantial portion of my time to incorporating lessons learned from analyzing large numbers of firmware images into my own Linux distribution, which I am currently in the process of releasing. This distribution is designed to address several gaps in the current market and to provide improved stability, reliability, and performance relative to existing Linux distributions.

Beyond my analysis work, I have written production code deployed in FDA-regulated medical devices, identified and demonstrated remote code execution vulnerabilities in life-critical medical systems, and designed cryptographic protocols implemented in production healthcare environments. I have hands-on experience across sixteen CPU architectures — from 8-bit microcontrollers through embedded processors to server-class systems — and I maintain a hardware analysis laboratory equipped with oscilloscopes, logic analyzers, microscopes, soldering and rework stations, and other diagnostic equipment used for component-level hardware investigation, firmware extraction, and forensic analysis. I also design, build, and operate virtualization and hosting infrastructure for security research, AI inference, and expert witness work, drawing on more than twenty years of hands-on performance measurement and tuning across embedded systems, network infrastructure, and datacenter hardware.

In addition to my litigation work, I have provided technical analysis, design, and development services to organizations across the medical device, telecommunications, semiconductor, and security industries.

A more detailed list of my engagements can be found on my curriculum vitae.