Acronis SCS

Balancing Innovation & Secure Software Development in a Globalized Economy

THE SOFTWARE STATE-OF-PLAY

From power grids and advanced weapons systems to the telework-enabling apps connecting us during COVID-19, software sits at the heart of nearly all that keeps America and the world running. But in the words of a 2020 Atlantic Council report, "society has a software problem." As more and more products and services rely on the use of unvetted third party code and open source software (OSS) libraries, cyber risks and opportunities for exploitation have surged. In fact, cyberattacks targeting OSS projects have grown 430% year-over-year, according to Sonatype's 2020 State of the Software Supply Chain report, with an average of 38 known OSS vulnerabilities per application.

The SolarWinds breach, which hit headlines at the end of 2020, is the clearest real-world demonstration of the need to evaluate and better secure software supply chains in order to maintain America's national security. Though that breach is perhaps the most noteworthy code exploitation in recent history, it is certainly not the only example. Attacks of this nature are becoming more frequent – and the potential impact for American interests more devastating.

MOVING IN THE RIGHT DIRECTION

Despite this trend, there is positive momentum to celebrate. Last year spurred several steps forward for cybersecurity policy. The Cyberspace Solarium Commission's original 2020 report discussed supply chain security issues and prompted the introduction of numerous pieces of legislation designed to help shore up our nation's cyber hygiene, nearly thirty of which were adopted under the FY2021 NDAA. In addition, the National Telecommunications and Information Administration continues to make progress in compiling a Software Bill of Materials (SBOM), an effort that promotes transparency and reduces risk for vendors and government alike.

America is moving in the right direction when it comes to balancing software supply chain security and innovation in today's globalized economy. Yet more work and collaboration amongst public and private stakeholders is required. To successfully serve our nation's software needs, vendors need access to clearly defined polices, processes, and practices for objectively assessing software code risk.

AN APPEAL ON BEHALF OF SMALL BUSINESSES

Hiring developers or outside firms to manually validate product source code can cost companies hundreds of thousands of dollars per review. That cost is simply unsustainable for most small and medium-sized businesses – even those dedicated to helping protect and preserve America's national security. As you read this memo, companies with exciting software ideas and solutions are being pushed out of the market simply because they cannot afford such expensive vetting requirements. All of America suffers when that happens: government, individuals, and the economy. It is time to forge a way ahead that prioritizes national security without sacrificing innovation or small business opportunity.

AN AI-BASED MODEL FOR SOURCE CODE ANALYSIS

Both companies and government need an affordable way to score software risk that relies on repeatable, objective processes and quantifiable results. Acronis SCS's research and development team has partnered with leading academics in the field of artificial intelligence (AI) at the University of California - Riverside to develop and train an AI-based model designed to do just that.

Speaking on the government's own software development strategies in September 2020, the driver of the Defense Department's Cybersecurity Maturation Model Certification (CMMC) effort, Katie Arrington, urged developers to "focus on the highest risk." Our model, which consists of a deep learning neural network, scans through source code (both open source and proprietary) to provide impartial quantitative risk scores that help IT administrators accurately determine whether and how to deploy new software packages, as well as update existing packages.

Our research team's first round of analysis, which focused on the Android Bluetooth module known as "Fluoride," resulted in a 41% improvement at detecting common vulnerabilities and exposures (CVEs) over random testing. The second round of testing, which studies the much larger Android kernel code base, is also tracking at 41% improvement over random testing.

THE FUTURE-PROOF APPROACH AMERICA NEEDS

Once research is complete, we hope to share the model with others to help all companies identify and remediate risks within their software code, and in so doing, help the US government hold industry accountable against a set of consistent, objective standards.

Our AI-based approach ensures software vendors – and the federal contractors and government agencies relying on their products – can take the uncertainty out of software supply chain validation, while spurring cutting-edge innovation and small business opportunity.

WANT TO KNOW MORE ABOUT OUR EFFORTS?

Contact members of our team today for more information!

POLICY CONTACTS

- **John Zanni, CEO** JZ@AcronisSCS.com
- **Lynndy Smith, Sr. Director of External Affairs** LS@AcronisSCS.com
- **Nicole Magney, Public Policy &Communications Manager** NM@AcronisSCS.com

RESEARCH CONTACTS

- **Neil Proctor, VP of Engineering and R&D** NP@AcronisSCS.com
- **Joe Barr, Sr. Director of Research** Joe.Barr@AcronisSCS.com

Acronis SCS