IEEE SecDev 2016: Prioritizing Secure Development

Robert Cunningham | MIT Lincoln Laboratory
Pamela Gupta | OutSecure
Ulf Lindqvist | SRI International
Stelios Sidiropoulos-Douskos | MIT
Michael Hicks | University of Maryland

Developing software in 2016 is different than it was when IEEE Security & Privacy magazine was founded in 2003. Developers now need to know about the constantly evolving threat landscape, the challenging complexity of systems security, and the accelerating pace of software and system development. Computer attacks in 2003 were rare enough that the term computer worms had to be defined when reported and taxonomies needed to be developed.1,2 Today’s threats are from well-funded militaries and companies with expertise in attacking systems, applications, and data, and the attacks are more varied and common. Back in 2003, Microsoft and Apple released a major OS update roughly every two years, and it took another year or two for it to be installed on the majority of systems. Today, a significant new OS version comes out almost every year, and the ability to share data and services across platforms like smartphones and smart watches is becoming ubiquitous.

It’s clear that developers, researchers, and practitioners need a venue to discuss design approaches and tools for building security in and significantly reducing the introduction of vulnerabilities. Great progress is being made in the academic security research community, but research results don’t transition to the engineering and development communities to the necessary extent and at the necessary speed. To address this critical need, the IEEE Cybersecurity Initiative is introducing a new event that aims to expand interactions and bridge the gap between cybersecurity research and development: the IEEE Cybersecurity Development Conference (IEEE SecDev). The inaugural IEEE SecDev 2016 Conference will be held on 3–4 November 2016 in Boston.

Conference Focus

Systems and software vulnerabilities continue to jeopardize intellectual property, consumer trust, and business operations and services. A broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depends on secure, reliable software. SecDev 2016 is designed to provide a proactive and innovative approach to the security challenges in systems of varying size, complexity, and functionality. It’s aimed at bringing different corners of the academic and business worlds’ engineering and security communities together to share the latest research, technical developments, and lessons learned from the front lines of security. Software systems can be built more securely when we understand and apply concepts coming out of research and development to real-world problems facing various areas of functionality and complexity.

SecDev is distinguished by its focus on how to build security in—not to simply discover the absence
of security. Its goal is to encourage, develop, and disseminate ideas for secure system development among both academia and industry. Developers have valuable experiences and ideas that can inform academic research, and researchers have concepts, studies, code, and tools that could benefit developers. We anticipate that attendees from academic conferences like the IEEE Symposium on Security and Privacy, the USENIX Security Symposium, the ACM SIGPLAN Programming Language Design and Implementation conference, the ACM SIGSOFT International Symposium on the Foundations of Software Engineering, the International Symposium on Software Testing and Analysis, the Symposium on Usable Privacy and Security, and many others will contribute ideas to SecDev, as will attendees of industrial conferences like the Open Web Application Security Project’s AppSec event, the RSA Conference, the Black Hat Conference, and ShmooCon.

In its inaugural year, the conference will run for two full days and will blend invited and proposed talks and hands-on tutorials by known experts and leading researchers from academia and industry.

Understanding Security Failures

The morning of the first day will address computer security failures and their implications for people, devices, companies, and the economy. Users feel the impact of security failures primarily because of the inconvenience they cause. When passwords are stolen, users need to reauthenticate and establish new ones. If users are unwise enough to reuse their password, then they need to do this for every site with the shared password. If data used for identity establishment (for instance, fingerprints, date or place of birth) is stolen too, then users might need to hire companies that monitor illegal use of identity.

Devices also need security, and with the rise of the Internet of Things, more and more people will be leveraging thermostats, door locks, lights, and many other devices that allow remote control via mobile devices. The ability to ensure that your door is locked from a remote location is a useful feature, but security vulnerabilities in these systems can result in property loss and even death. Early research on these systems have demonstrated significant problems with the design and implementation of security.3

For companies, the most valuable asset is often intellectual property; intellectual property theft can have catastrophic effects for a business. Failures in key resources, for example, power distribution systems and banking systems, can negatively impact entire economies. SecDev will try to cover portions of all these areas to give a sense of how important protecting intellectual property is.

Building Security In

The first day’s afternoon session will focus on solutions to commonly encountered security problems. IEEE SecDev members will start by looking at the state of software and hardware security: What are the best practices followed by industry, and what are the known good secure-design patterns? They will explore design and implementation of security. As Bruce Schneier wrote in the January/February 2016 issue of this magazine, “Complexity is the worst enemy of security.”4 We’ve known this for decades, yet we continue to invent complex protocols and applications in the hopes of delivering optimized implementations. Some companies incorporate metrics that capture important elements of security complexity and seek to design systems that are inherently more secure.5 Some go further and leverage formal methods to prove that critical software components or protocol designs are provably correct.

We know that tools and techniques exist to help build secure software. Random fuzzing has been surprisingly effective in uncovering errors and is heavily used by security researchers. But because of the state explosion problem, random fuzzing has been relatively ineffective at generating inputs that trigger errors deep inside applications.

By analyzing source code, static analysis tools can help find potentially all security bugs—even those deep inside complex applications—for certain error classes (for example, buffer overflows). Unfortunately, sound and complete analysis is shown to be undecidable. In practice, static analysis can be made practical by either adopting unsound techniques that lead to false negatives or reducing precision that leads to false positives.

Dynamic analysis techniques find bugs by analyzing code as it executes. By focusing on concrete execution traces, dynamic analysis avoids issues with precision (that is, false positives) but suffers from insufficient coverage, requiring inputs that trigger potentially vulnerable functionality. An effective development practice will combine these tools to find and fix software before it’s widely deployed.

SecDev is a venue for developers, researchers, and practitioners to discuss design approaches and tools for building security in.
Papers and Tutorial Sessions

The morning of the second day will cover more recent research in these areas. Papers will be selected from those submitted to the conference by the program committee assembled by Michael Hicks of the University of Maryland. On the afternoon of the second day, attendees will be able to select from among several parallel tutorial sessions. This mix of tools curated by the tutorial chair, Stelios Sidiroglou-Douskos, represents the core secure-development principles used in industry and academia today. Namely, there are tutorials representing the state of the art in random testing and fuzzing (for instance, Google’s libfuzzer), static analysis—both industrial (Coverity) and academic (DroidSafe)—and dynamic analysis (MIT’s Lincoln Laboratory’s PANDA framework). Together, these frameworks and tools form the foundation of secure development. Attendees will greatly benefit from understanding how to incorporate them in their development process.

The general chair for SecDev 2016 is Robert Cunningham, who also leads the IEEE Cybersecurity Initiative. For more information, please visit the SecDev website at www.secdev.ieee.org.

We hope to see you in Boston on 3 and 4 November!

References

Robert Cunningham is the leader of the Secure, Resilient Systems and Technology Group at MIT Lincoln Laboratory. Contact him at robertkcunningham@ieee.org.

Pamela Gupta is president and founder of OutSecure. Contact her at pamela.gupta@outsecure.com.

Ulf Lindqvist is a program director in the Computer Science Laboratory at SRI International. Contact him at ulf.lindqvist@sri.com.

Stelios Sidiroglou-Douskos is a research scientist in the Computer Science and Artificial Intelligence Laboratory at MIT. Contact him at stelios@csail.mit.edu.

Michael Hicks is a professor in the Department of Computer Science at the University of Maryland and is affiliated with the Maryland Cybersecurity Center. Contact him at mwh@cs.umd.edu.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

Subscribe today for the latest in computational science and engineering research, news and analysis, CSE in education, and emerging technologies in the hard sciences.

www.computer.org/cise