Building on the Success of Building Security In

Archer Batcheller | Northrop Grumman Corporation
Summer Craze Fowler | Carnegie Mellon University Software
Robert Cunningham and Dinara Doyle | MIT Lincoln Laboratory
Trent Jaeger | Pennsylvania State University
Ulf Lindqvist | SRI International

Large-scale cyberattacks continue to plague users, companies, and even countries. The WannaCry ransomware attack encrypted users' data and demanded ransom payments in exchange for returning access to the data. Dyn, a company that runs the Internet domain name system for many leading sites, was the victim of a distributed denial-of-service (DDoS) attack, resulting in large parts of the Internet becoming inaccessible. And, the recent Petya cybersabotage attack appears to be directed at systems in Ukraine but has spread to other countries.[1–3]

Software often meets functional requirements for consumer use but fails to build in security protections, leading to compromises and far-reaching unintended consequences.

Built In versus Bolted On

Much has been written about the impact of insecure software for everyday consumers.[4] For example, insufficient security protections have led to the "evilgrade" class of attacks against insecure software patching mechanisms, enabling the infection and weaponization of hundreds of thousands of everyday devices. These devices, such as webcams and DVRs, can then be deployed in attacks like the DDoS against Dyn.[5] Although there are many facets of these incidents, attacks like these highlight the need to shift to secure system and software design and implementation that build in appropriate security protections from the beginning.

The traditional software development lifecycle (SDLC) has often addressed security concerns in the testing phase, which results in very expensive fixes[6] or, worse, security issues that aren't uncovered until operation. Secure development practices integrate security-related activities in each phase of the SDLC, yielding benefits by making security a continuous concern rather than simply part of test procedures.

Many organizations including Microsoft (www.microsoft.com/en-us/sdl), NIST,[7] and the Open Web Application Security Project (www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project) offer secure SDLC models, and many advances have been made in secure coding practices such as penetration testing, secure code tools and analyzers, and exploit mitigation techniques. Yet these security advances run the risk of being underutilized. For security advances to be "built in" from the beginning, rather than "bolted on" at the end, security researchers must work with industry practitioners to learn the challenges of security in the engineering trenches and to build partnerships that mature and transition innovations from research to practice.

Despite secure SDLC models and advances in secure development techniques, there are many open areas of research. Further, there's a gap between secure development research and secure development practices that must be addressed with both community building and new innovations. IEEE is tackling this problem through its Secure Development Conference (SecDev), now in its second year.

The Inaugural Conference

In fall 2016, 167 researchers, practitioners, and students convened near Boston for the inaugural IEEE SecDev conference.[8] The two-day event was a blend of invited talks, accepted papers, and tutorials on topics ranging from secure design to secure enforcement techniques to secure defenses. Three experts on secure development provided thought-provoking research and shared their experiences. These experts highlighted the importance

Copublished by the IEEE Computer and Reliability Societies

of considering usability when designing secure systems, emphasized that implementing cryptography remains hard, and proposed several ideas to improve the current state of practice. They also provided an update on the latest efforts in developing automated analysis tools. Each talk highlighted both cutting-edge research and practical guidance for participants to implement in their own studies and projects.

In addition to the accepted presentations and enlightening talks, participants were able to learn more in hands-on tutorials on the security of web design, static analysis techniques, secure development operations, and dynamic testing techniques. The inaugural conference was a resounding success, and attendees were pleased with the level of participation and, most especially, with the high-quality content.

IEEE SecDev 2017

This year, IEEE is building on the success of this building security in–focused event and providing even more opportunities for participation and practical learning. Expanding to two and a half days, the IEEE SecDev event will convene in Boston on 24 September 2017, beginning with a half day of tutorials. This year, it's also adding poster presentations to broaden participation and provide a forum in which research and practices to be discussed in a less formal setting.

Following the tutorials and poster presentations, there are two days of presentation content spanning academic and industry research and practices. Topics will include machine learning approaches to secure development, addressing hardware vulnerabilities with software, securing databases, cryptography implementations for security, and advances in programming languages. Check the website at secdev.ieee.org for more information on our exciting keynote speakers who will kick off each day of the conference, including Christoph Kern from Google, who will discuss his work in security APIs.

In addition to a full program of accepted presentations and lightening talks, this year's program includes a panel of industry secure development experts who will discuss building a business around secure development. This panel includes Nadia Carlsten, program manager for the Transition to Practice program in the US Department of Homeland Security's Science and Technology Directorate, Reed Sturtevant of the MIT Engine, Andreas Kuehlmann of Synopsys, and Chris Wysopal of Veracode. The members of this esteemed group have funded research, supported new start-ups, created companies, and defined entirely new sectors of secure development practices. They will share wisdom about settling on (and funding development of) a great new idea, challenges involved in building a useful product, taking that product to market, and building a tool useful to developers everywhere.

For a second year, IEEE SecDev has been awarded a student travel grant from NSF, so we're thrilled to offer this grant money (up to $1,300 per student), with preference given to students studying privacy and security and to students from diverse backgrounds. Applications are due by 11 August 2017. Students will be notified of the award decisions by 18 August 2017. Details about the process for applying for student grants are available at secdev.ieee.org/2017/student-travel.

IEEE SecDev is a venue for presenting ideas, research, and experience about the development of secure systems, and we've created a program that brings together experts in the field to focus on building security in. The general chair for IEEE Sec Dev 2017 is Summer Craze Fowler, technical director at Carnegie Mellon University's Software Engineering Institute CERT Division.

Please join us in Boston 24–26 September 2017 to contribute to and learn from the secure development community! For more information, please visit the IEEE SecDev website at secdev.ieee.org. ■

References

1. S. Hilton, "Dyn Analysis Summary of Friday October 21 Attack," *Oracle+ Dyn*, 26 Oct. 2016; dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack.
2. B. Chappell, "WannaCry Ransomware: What We Know Monday," *NPR*, 15 May 2017; www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.
3. R. Brandom, "The Petya Ransomware Is Starting to Look like a Cyberattack in Disguise," *The Verge*, 28 June 2017; www.theverge.com/2017/6/28/15888632/petya-goldeneye-ransomware-cyberattack-ukraine-russia.
4. W. Dormann, "The Consequences of Insecure Software Updates," *The CERT/CC blog*, 30 June 2017; insights.sei.cmu.edu/cert/2017/06/the-consequences-of-insecure-software-updates.html.
5. S. Misra, M. Maheswaran, and S. Hashmi, "Security Challenges and Approaches in Internet of Things," *SpringerBriefs in Electrical and Computer Engineering*, Springer, Feb. 2016.
6. M. Dawson et al., "Integrating Software Assurance into the Software Development Life Cycle (SDLC)," *J. Information Systems Technology & Planning*, vol. 3, no. 6, 2010.
7. R. Kissel et al., "Security Considerations in the System Development Life Cycle," *NIST Special Publication 800-64 Rev 2*, Oct. 2008; nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf.

8. R. Cunningham et al., "IEEE SecDev 2016: Prioritizing Secure Development," *IEEE Security & Privacy*, vol. 14, no. 4, 2016, pp. 82–84.

Archer Batcheller is a cyber systems engineer at Northrop Grumman. Contact him at archer.batcheller@ngc.com.

Summer Craze Fowler is the technical director of Cybersecurity Risk and Resilience at Carnegie Mellon University's Software Engineering Institute (CERT program). She's also a member of the faculty at Carnegie Mellon's Heinz College. Contact her at sfowler@cert.org.

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

Dinara Doyle is the DevOps and IT Services team lead at MIT Lincoln Laboratory. Contact her at dinara.doyle@ll.mit.edu.

Trent Jaeger is a computer science and engineering professor at The Pennsylvania State University and codirector of the Systems and Internet Infrastructure Security Lab. Contact him at tjaeger@cse.psu.esu.

Ulf Lindqvist is a program director in the Computer Science Lab at SRI International, vice chair of the IEEE Cybersecurity Initiative, and 2016–2017 chair of the IEEE Computer Society's Technical Committee on Security and Privacy. Contact him at ulf.lindqvist@sri.com.