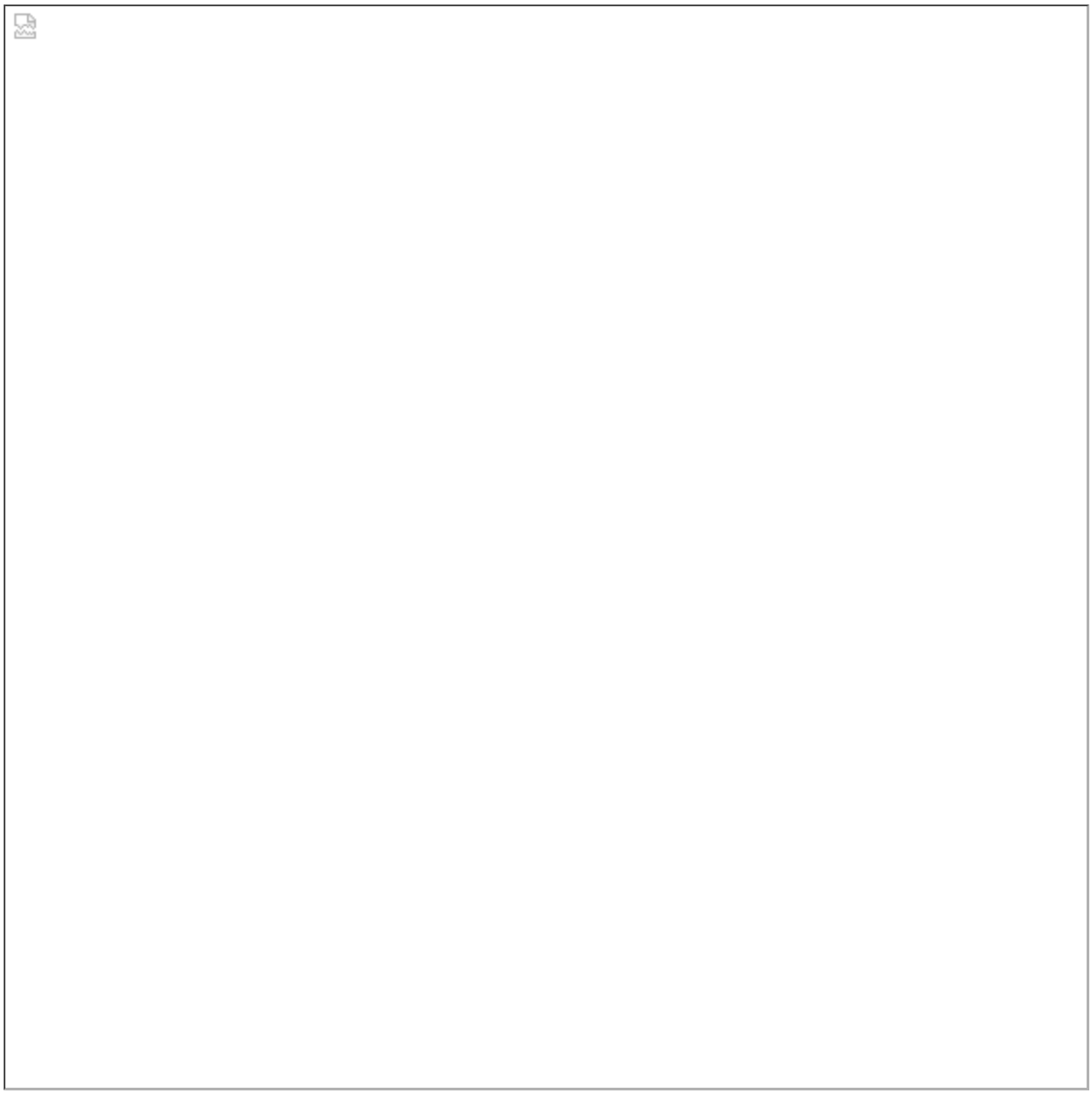
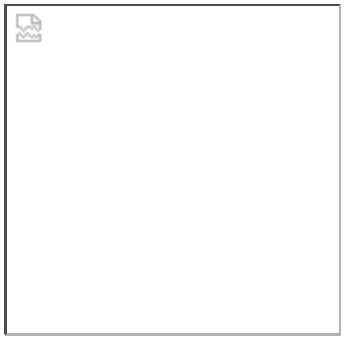


February / March 2014

News

It is beginning to feel like spring here in Pittsburgh: the temperature has not fallen below zero degrees for several days now, and it has even briefly stopped snowing. Many of the updates to the secure coding wiki have been in the CERT C Coding Standard space as Carol Lallier synchronizes changes from the manuscript of the upcoming Addison Wesley book. This project

is nearing completion-we are currently reviewing the page proofs, which are due back to the publisher on March 7. Overall, the project is on schedule and the books are still expected to be



available on or about April 18, 2014.

The SEI has launched a new version of the CERT website. The site has been redesigned to improve the user experience, to better represent the key capabilities and current research functions of the SEI's CERT Division, and to enable one-click access to the site's most in-demand resources (such as Secure Coding).

Lujo Bauer (Carnegie Mellon University, Department of Electrical and Computer Engineering), Lori Flynn, Limin Jia (Carnegie Mellon University, Department of Electrical and Computer Engineering), Will Klieber, Fred Long, Dean F. Sutherland, and David Svoboda published an SEI technical report, Mobile SCALe: Rules and Analysis for Secure Java and Android Coding, describing Android secure coding rules, guidelines, and static analysis developed as part of the Mobile SCALe project. This is work is also being performed in collaboration with Masaki Kubo and Yozo Toda of JPCERT, both of whom have just completed their yearly pilgrimage to Pittsburgh to meet with the secure coding team.

Finally, David Svoboda and Robert Seacord have both been asked to join the security review team to review submissions for the JavaOne Security Track. The call for proposals should be out soon, so it's not too early to begin thinking about submissions. Dan Plakosh and Robert Seacord are also running a Software Security for Mobile Platforms Minitrack at HICCS-48, January 5-8, 2015. See the events section below for details.

Mobile SCALE

In March, we kick off the first post in a series on the SEI blog about our work on Android Secure Coding rules and guidelines. The first post focuses on the initial development of our Android rules and guidelines, done in 2013. The next post in this series will focus on the development of two tools that analyze information flow within and between Android apps. Later this year, we will publish a third post about our ongoing Android secure coding work: expanding the coding rules and guidelines beyond Java and further development of our newest static analysis tool. The posts may be viewed at blog.sei.cmu.edu.

How are you using the CERT Secure Coding Standards?

As a reader of this eNewsletter, we want to hear from you. Submit your comments about how you are using CERT Secure Coding Standards.

Language Standards Updates

CERT C Secure Coding Standard

Editors: Martin Sebor (Cisco Systems), Aaron Ballman (SEI)

No C rules were added, removed or deprecated last month

Changed

MEM05-C. Avoid large stack allocations
Updated to contain information about the recent findings regarding the Toyota unintended acceleration bug
MSC07-C. Detect and remove dead code
EXP19-C. Use braces for the body of an if, for, or while statement
Updated to contain information about the recent Apple OpenSSL "goto fail" bug
Updates were applied to most rules based on wording changes found while copy editing *The C Coding Standard*

CERT C++ Secure Coding Standard

Editors: Martin Sebor (Cisco Systems), Aaron Ballman (SEI)

No C++ rules were added, removed, deprecated, or substantively changed last month.

CERT Oracle Secure Coding Standard for Java

Editors: Adam O'Brien (Oracle), David Svoboda (SEI)

Added

DRD14-J. Check that a calling app has appropriate permissions before responding
DRD15-J. Consider privacy concerns when using Geolocation API
MSC08-J. Do not store non-serializable objects as attributes in an HTTP session

Changed

OBJ03-J. Do not mix generic with nongeneric raw types in new code
Now contains a definition for heap pollution.

CERT Perl Secure Coding Standard

Editor: David Svoboda (SEI)

No Perl rules were added, removed, deprecated, or substantively changed last month.

Upcoming Events and Training

Mini-Track Announcement | Hawaii International Conference on Systems Sciences

Software Security for Mobile Platforms

January 5-8, 2015
Grand Hyatt Kauai, Hawaii

This Minitrack focuses on the research and automation techniques that can be applied to mobile platforms that will ensure that developed software on these devices are secure while not compromising other system properties such as performance or reliability. Security on mobile devices has not kept pace with traditional computer security, and mobile phone operating systems are not updated as frequently as those on personal computers. In both the personal computer and mobile platform arenas, current security engineering methods are demonstrably inadequate at identifying software vulnerabilities. These vulnerabilities are caused by software designs and implementations that do not adequately protect systems and by development practices that do not focus sufficiently on eliminating implementation defects that result in security flaws. This is especially true in the area of mobile platforms where one study found that, from 2010 to 2011, the number of new vulnerabilities in mobile operating systems jumped by 93 percent. Additionally, according to Symantec Corp, 2011 was the first year that mobile malware presented a tangible threat. An opportunity exists for systematic improvement that can lead to secure mobile software applications and implementations.

Research topics include, but are not limited to:

- Static analysis tools and techniques for detecting security flaws and software vulnerabilities in source or binary code
- Dynamic analysis tools for detecting security flaws and software vulnerabilities in source or binary code
- Model-checking tools for detecting security flaws and software vulnerabilities in software systems
- Software architectures and designs for securing against denial-of-service attacks and other software exploits
- Coding practices for improved security and secure library implementations
- Other tools and techniques for reducing or eliminating vulnerabilities during the development and maintenance

Author Deadlines

- June 15: Submission of manuscripts. The review is double-blind; therefore, this initial submission must be without author names.
- Aug 15: Notification of acceptance.
- Sept 15: Submission of final papers.
- Oct 15: Registration deadline for accepted papers.

Co-Chairs

Daniel Plakosh (primary contact)
CERT
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213
Tel (412) 268-7197
Cell (412) 427-4606
Fax: (412) 268-6989
dplakosh@cert.org

Robert C. Seacord

CERT
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213
Tel: (412) 268-7608
Fax: (412) 268-6989
rcs@cert.org

Secure Coding Resources

Listen to *Raising the Bar: Mainstreaming CERT C Secure Coding Rules* by Robert C. Seacord http://www.cert.org/podcast/mp3/2/20140107seacord-full.mp3

Watch Robert Seacord discuss *Secure Coding - Avoiding Future Security Incidents,* http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=54982

Subscribe to Our eNewsletter

Join the SEI CERT Secure Coding Community