



May / June 2015

[News](#)

[Language Standards Updates](#)

[Upcoming Events](#)

[Our People](#)


[Secure Coding Resources](#)

News

Spring has finally arrived in Pittsburgh, Pennsylvania, as we are now mowing the snow from our lawns instead of shoveling our driveways. Major development work continues on the [CERT C++ Coding Standard](#). We have also received some funding to continue this work into the next fiscal year, although the scope of the work still needs to be defined.

We have completed some additional steps since the significant reorganization reported in the

last newsletter. We created a new public [Android Secure Coding Standard](#) space where we plan to continue to develop coding standards for the Android platform. The Android-only rules and recommendations now have categories, similar to the other CERT standards. Much of the reorganization is not yet completed, so please excuse our mess (and some missing content) as we reorganize. We plan to rename the Android-only rules and recommendations, which currently start with DRD, to have a "-A" suffix. CERT rules from other coding standards that are also applicable to Android app development will remain unchanged.

Robert Seacord recently recorded Part 1 of a training video, *Secure Coding Rules for Java LiveLessons*. It is currently available to [Safari Books Online](#) subscribers as a Sneak Peek. Robert is currently recording Part 2 of the video to be released later this year. In *Secure Coding Rules for Java LiveLessons*, he provides complementary coverage to the rules in *The CERT Oracle Secure Coding Standard for Java*. The rules for which LiveLessons are available (for example, [IDS00-J. Prevent SQL Injection](#)) now contain links to the corresponding LiveLessons; the links are listed in the Bibliography sections and marked with a  icon.

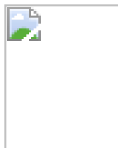
Robert Seacord just returned from Stuttgart, Germany, where he gave a keynote presentation on Automotive Vulnerabilities at the [Automotive Safety and Security Conference](#) and met with a number of industry executives. Perhaps the most interesting idea to come out of these meetings is a keen interest in developing a combined security/safety standard for C language programming. Please contact us if you are interested in being involved in or contributing to such an effort. Robert will also be speaking at the [ISO 26262 Functional Safety Seminar](#) sponsored by PRQA on May 12 in Detroit, Michigan.

Lori Flynn and Will Klieber published a new blogpost, [An Enhanced Tool for Securing Android Apps](#), which describes enhancements made to DidFail in late 2014 and an enterprise-level approach for using the tool.

Effective Programming Sale

Our [Java Coding Guidelines](#) book is now on sale as part of the [Effective Programming Promotion](#) from InformIT. You can buy 1 save 40% or buy 2 or more and save 50% on these books, eBooks, and video for experienced programmers in [C++](#), [Java](#), [Python](#), [Ruby](#), and [C#](#). Use discount code **EPSALE** during Checkout @InformIT.com through May 18, 2015.

How are you using the CERT Secure Coding Standards?



As a reader of this eNewsletter, your input is important to us. [Submit](#) your comments and let us know how you are using CERT Secure Coding Standards.

Language Standards Updates

CERT C Coding Standard

Editors: Martin Sebor and Aaron Ballman (SEI/CERT)

Changed

[ENV33-C. Do not call system\(\)](#)

Clarified susceptibility of `unlink()` function to symlink attacks.

CERT C++ Secure Coding Standard

Editors: Martin Sebor and Aaron Ballman (SEI/CERT)

Added

DCL59-CPP. Do not define an unnamed namespace in a header file

Changed

- [EXP54-CPP. Do not access an object outside of its lifetime](#)
Added a noncompliant code example/compliant solution (NCCE/CS) pair for reference-bound temporaries.
- [ERR54-CPP. Catch handlers should order their parameter types from most derived to least derive](#)
Added an automated detection entry for Clang's new -Wexceptions warning flag.
- [EXP53-CPP. Do not read uninitialized memory](#)
Added an NCCE/CS pair for reuse of moved-from objects.

Removed

No C++ rules were removed or deprecated.

CERT Oracle Secure Coding Standard for Java

Editors: Adam O'Brien (Oracle) and David Svoboda (SEI/CERT)

No Java rules were added, removed, deprecated, or substantively changed.

CERT Secure Coding Standard for Android

Editors: Fred Long (Aberystwyth University) and Lori Flynn (SEI/CERT)

No Android rules were added, removed, deprecated, or substantively changed.

CERT Perl Secure Coding Standard

Editor: David Svoboda (SEI/CERT)

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

Upcoming Events

Seminar: ISO 26262 Functional Safety Seminar

Sponsored by PRQA

May 12, 2015, in Detroit, Michigan

Details at <http://www.programmingresearch.com/hidden/prqa-day/>

Virtual Event: CERT Secure Coding Alignment with Cyber COI Challenges and Gaps

Will Klieber and Lori Flynn will be presenting "Using DidFail to Analyze Flow of Sensitive Information in Sets of Android Apps", as part of the day's lineup of topics.

June 23, 2015

Details at <https://www.webcaster4.com/Webcast/Page/139/8133> (registration required)

Workshop: Third International Workshop on Mobile Development Lifecycle (MobileDeLi 2015)

Organizers: Lori Flynn (CERT), Aharon Abadi, and Jeff Gray

October (26 or 27), 2015 in Pittsburgh, Pennsylvania, United States

Details at <http://sysrun.haifa.il.ibm.com/hrl/mobiledeli2015/index.shtml>

Collocated with the the ACM SIGPLAN conference on Systems, Programming, Languages and Applications: Software for Humanity (SPLASH)

We hope you will consider submitting to the workshop! Submission deadline is August 7, 2015.

Our People

In the eNewsletter, we highlight staff members behind our secure coding research. This month we feature Dan Plakosh.



Prior to joining the SEI, **Dan Plakosh** was the lead software engineer for the Systems Engineering Department at the Naval Surface Warfare Center (NSWCDD). Plakosh has over 15 years of software development experience in defense, research and industry. Plakosh's principal areas of expertise include; real-time distributed systems, network communications and protocols, systems engineering, real-time 2D and 3D graphics, and Unix OS internals. Much of Plakosh's recent experience has been redesigning legacy-distributed systems to use the latest distributed communication technologies.

Secure Coding Resources



Read the Blogpost [An Enhanced Tool for Securing Android Apps](#) by Lori Flynn and Will Klieber



Watch Fred Long's talk on [Secure Coding](#) to the British Computer Society Mid-Wales Branch, Monday, March 9



Watch Anatomy of [Another Java Zero-Day Exploit](#), presented by David Svoboda and Yozo Toda of JPCERT, now available at [JavaOne's website](#)

Subscribe to Our eNewsletter

Join the SEI CERT Secure Coding Community

