The IEEE Center for Secure Design Reveals Top 10 Most Significant Software Security Design Flaws

Experts from Cigital, Google, HP, Twitter and eight other organizations form IEEE Center for Secure Design

Piscataway, NJ August 27, 2014 — The IEEE Center for Secure Design, a cybersecurity initiative focused on the identification of software design flaws, announced the release of a report titled "Avoiding the Top 10 Software Security Design Flaws" based on real-world data collected and analyzed by experts at the world's leading technology companies.

In 2014, the IEEE Computer Society, the community for technology leaders, launched a cybersecurity initiative with the aim of expanding its ongoing involvement in cybersecurity. As part of that initiative, the IEEE Center for Secure Design (CSD) was formed, which welcomed experts from a diverse group of organizations to discuss software security design flaws that they had identified in their own internal design reviews. What resulted was a list of the top ten most significant software security design flaws and the design techniques to avoid them. Practical advice ranges from encouraging the correct use of applied cryptography to validating each individual bit of data.

Proper security design has been the Achilles' heel of security engineering for decades, mostly because it is difficult and requires deep expertise. More than just identifying implementation bugs, the IEEE CSD directly addresses today's most vexing security problem — security design.

Participants in the foundational workshop included Neil Daswani, Twitter; Christoph Kern, Google; Gary McGraw, Cigital; Jacob West, HP; Iván Arce, Sadosky Foundation, Ministry of Science, Technology and Productive Innovation of Argentina; Carl Landwehr, George Washington University; Brook Schoenfield, Intel/McAfee; Danny Dhillon, RSA; Tadayoshi Kohno, University of Washington; Izar Tarandach, EMC; Jim DelGrosso, Cigital; Margo Seltzer, Harvard University; and Diomidis Spinellis, Athens University of Economics and Business.

"The Center for Secure Design will play a key role in refocusing software security on some of the most challenging open design problems in security," said Neil Daswani of the security engineering team at Twitter. "By putting focus on security design and not just focusing on implementation bugs in code, the CSD does even the most advanced companies in the space a huge service."

"Bugs and flaws are two very different types of security defects," said Gary McGraw, chief technology officer at Cigital and author of the seminal book *Software Security*. "We believe there has been quite a bit more focus on common bugs than there has been on secure design and the avoidance of flaws, which is worrying since design flaws account for 50% of software security issues. The IEEE Center for Secure Design allows us a chance to refocus, to gather real data, and to share our results with the world at large."

The following list of recommendations was born from the workshop to help developers avoid the top security design flaws (each technique is described in detail in the report):

- Earn or give, but never assume, trust
- Use an authentication mechanism that cannot be bypassed or tampered with
- Authorize after you authenticate
- Strictly separate data and control instructions, and never process control instructions received from untrusted sources

- Define an approach that ensures all data are explicitly validated
- Use cryptography correctly
- Identify sensitive data and how they should be handled
- Always consider the users
- Understand how integrating external components changes your attack surface
- Be flexible when considering future changes to objects and actors

To learn more about these recommendations, download the report, Avoiding the Top 10 Software Security Design Flaws, cybersecurity.ieee.org.

About IEEE Center for Secure Design
IEEE Center for Secure Design delivers platform-independent software security expertise from industry, academia and government. Managed by the IEEE Computer Society and founded in 2014, founding members include: Athens University of Economics and Business, Cigital, EMC, George Washington University, Google, Harvard University, HP, Intel/McAfee, RSA, Sadosky Foundation, Ministry of Science, Technology and Productive Innovation of Argentina, Twitter, and the University of Washington.

About IEEE Computer Society
IEEE Computer Society is the world's leading computing membership organization and the trusted information and career-development source for a global workforce of technology leaders including: professors, researchers, software engineers, IT professionals, employers, and students. The unmatched source for technology information, inspiration, and collaboration, the IEEE Computer Society is the source that computing professionals trust to provide high-quality, state-of-the-art information on an on-demand basis. The Computer Society provides a wide range of forums for top minds to come together, including technical conferences, publications, and a comprehensive digital library, unique training webinars, professional training, and the TechLeader Training Partner Program to help organizations increase their staff's technical knowledge and expertise, as well as the personalized information tool myComputer. To find out more about the community for technology leaders, visit http://www.computer.org.

###

North America, Latin America, and Asia Press Contact
Natalie Guillemette
SHIFT Communications
617-779-1820
Cigital@shiftcomm.com

Europe, Middle East, and Africa Press Contact
Kirsten Scott
éclat Marketing
+44.1276.486000
Cigital@eclat.co.uk