IEEE Forms Security Initiative

Written by Marco Attard
29 August 2014

Twelve organisations, including Google, Twitter, HP and a number of universities, join the IEE to form the IEEE Centre for Secure Design (CSD), a new organization with the aim to finding common software design flaws.

“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,” Twitter security engineer Neil Daswani says. “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.”

As part of its launch the CSD brought together 12 member experts to identify the most significant security design flaws, and the techniques to avoid them. The result is the following list of 10 recommendations:

- Earn or give, but never assume, trust
- Use an authentication mechanism that cannot be bypassed or tampered with
- Authorise 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

“Bugs and flaws are two very different types of security defects,” Cigital CTO Gary McGraw says. “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 per cent 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.”

Go IEEE Centre for Secure Design Reveals Top Ten Most Significant Security Design Flaws