LangSec 2016

LangSec's goal is to provide the strongest defense for connected software and hardware, expressed as a practical design methodology for handling hostile inputs. LangSec offers a coherent computer science explanation for the current “epidemic of insecurity” and imposes an easy-to-understand structure on the seemingly ad hoc collection of software mistakes or design flaws. This explanation is predicated on the connection between fundamental computability principles and the continued recurrence of software flaws despite numerous and diverse secure programming initiatives.

LangSec posits that the only path to trustworthy software that safely handles untrusted inputs is treating all valid or expected inputs as a formal language and treating the respective input-handling routines as a recognizer for that language.

However, far from being an “Ivory Tower” theory, the LangSec approach to systems design is primarily concerned with achieving practical assurance: development that is rooted in fundamentally sound theory, but is expressed in efficient and practical tools for building software. One major objective of the workshop is to develop and share this viewpoint with attendees and the broader systems security community, to help establish a foundation for research based on LangSec principles.

The overall goal of the workshop is to bring more clarity and focus to two complementary areas: (1) practical software assurance and (2) vulnerability analysis (identification, characterization, and exploit development). The LangSec community views these activities as related and highly structured engineering disciplines and seeks to provide a forum to explore and develop this relationship.