LangSec: The 7^{th} Workshop on Language-theoretic Security and Applications
May 27, 2021

Call for papers

Current computer software that processes electronic data such as documents, images, videos, and messages is vulnerable to maliciously crafted input data. *Language-theoretic security* (LangSec) is a design and programming philosophy that focuses on formally correct and verifiable input handling throughout all phases of the software development lifecycle. In doing so, it offers a practical method of *assurance* of software free from broad and currently dominant classes of bugs and vulnerabilities related to incorrect parsing and interpretation of messages between software components (packets, protocol messages, file formats, function parameters, etc.).

LangSec aims to (1) produce verifiable parsers, free of typical classes of ad-hoc parsing bugs, (2) produce verifiable, composable implementations of distributed systems that ensure equivalent parsing of messages by all components and eliminate exploitable differences in message interpretation by the elements of a distributed system, and (3) mitigate the common risks of ungoverned development by explicitly exposing the processing dependencies on the parsed input.

Bugs in input processing (wherever input is taken at a software module's communication boundary) clearly dominate other kinds of bugs. Hence the first order of business in securing software that does any communication is ensuring that no unanticipated state is entered and no unexpected computation occurs while consuming inputs. In practice, however, such code is often ad-hoc and lacks a clear, formal language-theoretic definition of valid payloads. What's worse, inputs are "checked" with recognizers that cannot possibly accept or reject them correctly, e.g., context-free formats with regular expressions. In such cases, subsequent code assumes properties that couldn't possibly have been checked, and thus cannot be trusted to abide by their specification. Non-existence of unexpected computation is then highly unlikely, and unanticipated state conditions proliferate.

Important Dates

Research paper submissions due: 15 January 2021, AOE
Work-in-progress reports and panels submissions due: February 1, 2021, AOE
Notification to authors:: 15 February 2021
Final files due: 5 March 2021

Call for Papers

The LangSec workshop solicits contributions of research papers and work-in-progress reports related to the growing area of language–theoretic security. LangSec offers a connection between fundamental Computer Science concepts (language theory, computability) and the continued existence of software flaws.

Submissions should be in PDF file format and made via EasyChair. Submissions must not be anonymized. The confidentiality of submissions will be protected as is customary, but submissions with non-disclosure agreements or forms attached will be returned without review. **Shepherding will be available for authors with less academic writing experience.**

Research Papers

The LangSec PC encourages submission of research papers from academia, industry, and government. There is no hard maximum page limit, but length should be justified by the content and quality of the text. The PC expects research papers to vary between 4 and 15 pages in length. Shorter papers are encouraged, but longer

papers that document high-quality or extensive experimentation are very much in scope. Submissions should address LangSec principles and anti-patterns, report on practical applications of these principles, discuss the development of curriculum, training material, or frameworks, etc. Research papers are encouraged to address some of the topics listed below, but the list is not exhaustive:

1. inference of formal language specifications of data from samples
2. generation of secure parsers from formal language specifications
3. theory that describes the complexity hierarchy of verifying parser implementations
4. comprehensive taxonomies of LangSec phenomena
5. LangSec case studies of successes and failures
6. measurement studies of LangSec systems or data sets
7. computer languages, file formats, and network protocols built on LangSec principles
8. systems architectures and designs based on LangSec principles
9. re-engineering efforts of existing languages, formats, and protocols to reduce computational power
10. novel system designs for isolation and separation of parsers and processing
11. structured techniques for building weird machines
12. systems and frameworks for post-hoc or design time recognizer definition
13. identification of LangSec anti-patterns; certification of absence
14. models for unexpected computation
15. embedding runtime language recognizers

The PC expects that topics should cover recent LangSec-related advances and or make the connection between research and practical assurance through computability theory. The PC is interested in contributions from type theory, programming languages, and formal methods. This year, the LangSec workshop especially encourages research papers that apply the language-theoretic perspective to policy mechanisms, such as treating policy formulation and enforcement as language definition and language recognition problems (cf. F.Schneider, "Enforceable Security Policies", 2000; K.W. Hamlen et al., "Computability Classes for Enforcement Mechanisms", 2005; M.R. Clarkson et al. "Hyperproperties", 2010).

The PC encourages submissions that discuss actual implementations, prototypes, and proofs-of-concept. The resulting talk must not be a product pitch or a product manual, but the PC expects that the demonstration should enlighten and educate the audience to the extent that the audience could subsequently apply the tool or system in their own research or work. Proof-of-concept submissions are encouraged to include in their paper submission links to videos or other media demonstrating the project.

Work-in-Progress Reports

The LangSec PC encourages submissions of work-in-progress reports (between 4 and 10 pages). They should describe ongoing LangSec-relevant projects that are producing promising results but do not yet amount to a full paper. The authors of accepted work-in-progress reports will be invited to give presentations at the workshop. In addition, the PC will invite a select set of high-quality work-in-progress reports to be included in the workshop proceedings.