Value-Range Analysis Of C Programs: Towards Proving The Absence Of Buffer Overflow Vulnerabilities
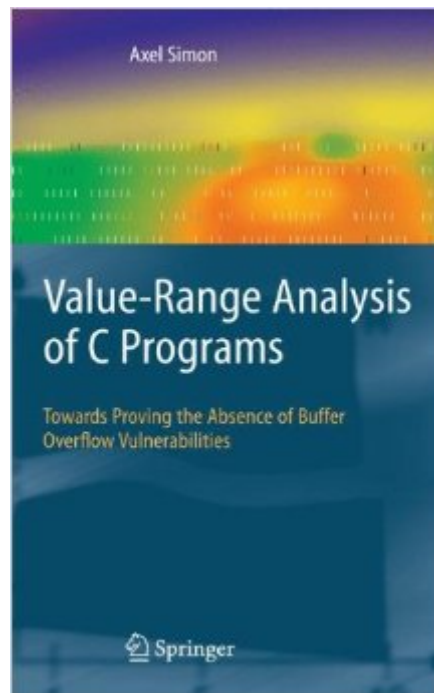
Axel Simon

Value-Range Analysis of C Programs

Towards Proving the Absence of Buffer Overflow Vulnerabilities

Springer

Synopsis

Abu?erover?owoccurswheninputiswrittenintoamemorybu?erthatisnot large enough to hold the input. Bu?er over?ows may allow a malicious person to gain control over a computer system in that a crafted input can trick the defectiveprogramintoexecutingcodethatisencodedintheinputitself.They are recognised as one of the most widespread forms of security vulnerability, and many workarounds, including new processor features, have been proposed to contain the threat. This book describes a static analysis that aims to prove the absence of bu?er over?ows in C programs. The analysis is conservative in the sense that it locates every possible over?ow. Furthermore, it is fully automatic in that it requires no user annotations in the input program.

Thekeyideaoftheanalysisistoinferasymbolicstateforeachp- gram point that describes the possible variable valuations that can arise at that point. The program is correct if the inferred values for array indices and pointer o?sets lie within the bounds of the accessed bu?er. The symbolic state consists of a ?nite set of linear inequalities whose feasible points induce a convex polyhedron that represents an approximation to possible variable valuations. The book formally describes how program operations are mapped to operations on polyhedra and details how to limit the analysis to those p- tionsofstructuresandarraysthatarerelevantforveri?cation.Withrespectto operations on string bu?ers, we demonstrate how to analyse C strings whose length is determined by anul character within the string.

Book Information

Hardcover: 302 pages

Publisher: Springer; 2008 edition (June 19, 2008)

Language: English

ISBN-10: 1848000162

ISBN-13: 978-1848000162

Product Dimensions: 6.1 x 0.8 x 9.2 inches

Shipping Weight: 1.3 pounds (View shipping rates and policies)

Average Customer Review: Be the first to review this item

Best Sellers Rank: #4,347,941 in Books (See Top 100 in Books)   #65 inÂ Books > Computers & Technology > Programming > Algorithms > Memory Management   #559 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Computer Design   #678 inÂ Books > Computers & Technology > Programming > Languages & Tools > Compilers

Download to continue reading...

Value-Range Analysis of C Programs: Towards Proving the Absence of Buffer Overflow Vulnerabilities Middle Range Theories: Application to Nursing Research (Peterson, Middle Range Theories) The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities (2 Volume set) Rules of the Road: A Plaintiff Lawyer's Guide to Proving Liability Proving Ground: A History of Dodge, Chrysler, and Plymouth Racing The Atomic Times: My H-Bomb Year at the Pacific Proving Ground Smaller Faster Lighter Denser Cheaper: How Innovation Keeps Proving the Catastrophists Wrong Pablo Neruda: Absence and Presence Candida HÃƒÂ¶fer: Architecture Of Absence Absence of Malick: Why did movie director Terrence Malick disappear after his first two brilliant movies? (Singles Classic) Absence of Evidence: An Examination of the Michelle Young Murder Case A Sunlit Absence: Silence, Awareness, and Contemplation Higher-Order Perl: Transforming Programs with Programs Insider's Guide to Graduate Programs in Clinical and Counseling Psychology: 2016/2017 Edition (Insider's Guide to Graduate Programs in Clinical & Counseling Psychology) Programs A-Plenty: Customize Your Programs With Scripts for Every Occasion (Expressive Art (Choral)) Christmas Programs for Children: Poems, Plays, and Programs for a Joyful Celebration! Analytics: Data Science, Data Analysis and Predictive Analytics for Business (Algorithms, Business Intelligence, Statistical Analysis, Decision Analysis, Business Analytics, Data Mining, Big Data) Towards a New Architecture (Dover Architecture) Towards a Philosophy of Photography A Case for Character: Towards a Lutheran Virtue Ethics