Table of Contents

Attack Analysis and Prevention I
BuBBle: A Javascript Engine Level Countermeasure against Heap-Spraying Attacks p. 1
CsFire: Transparent Client-Side Mitigation of Malicious Cross-Domain Requests p. 18
Idea: Opcode-Sequence-Based Malware Detection p. 35

Attack Analysis and Prevention II
Experiences with PDG-Based IFC p. 44
Idea: Java vs. PHP: Security Implications of Language Choice for Web Applications p. 61
Idea: Towards Architecture-Centric Security Analysis of Software p. 70

Policy Verification and Enforcement I
Formally-Based Black-Box Monitoring of Security Protocols p. 79
Secure Code Generation for Web Applications p. 96
Idea: Reusability of Threat Models - Two Approaches with an Experimental Evaluation p. 114

Policy Verification and Enforcement II
Model-Driven Security Policy Deployment: Property Oriented Approach p. 123
Category-Based Authorisation Models: Operational Semantics and Expressive Power p. 140

Secure System and Software Development I
Formal Verification of Application-Specific Security Properties in a Model-Driven Approach p. 166
Idea: Enforcing Consumer-Specified Security Properties for Modular Software p. 182
Idea: Using System Level Testing for Revealing SQL Injection-Related Error Message Information Leaks p. 192

Secure System and Software Development II
Automatic Generation of Smart, Security-Aware GUI Models p. 201
Idea: A Feasibility Study in Model Based Prediction of Impact of Changes on System Quality p. 231

Author Index p. 241

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.