Analyzing memory accesses in obfuscated x86 executables
Hybrid engine for polymorphic shellcode detection
Experiences using minos as a tool for capturing and analyzing novel worms for unknown vulnerabilities
A pointillist approach for comparing honeypots
Automatic detection of attacks on cryptographic protocols: a case study
METAL: a tool for extracting attack manifestations
Flow-level traffic analysis of the blaster and sobig worm outbreaks in an Internet backbone
A learning-based approach to the detection of SQL attacks
Masquerade detection via customized grammars
A prevention model for algorithmic complexity attacks
Detecting malicious code by model checking
Improving the efficiency of misuse detection
Enhancing the accuracy of network-based intrusion detection with host-based context

TCPtransform: property-oriented TCP traffic transformation

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