1.

Record Nr.	UNISA996465893403316
Titolo	Recent Advances in Intrusion Detection [[electronic resource]] : 14th International Symposium, RAID 2011, Menlo Park, CA, USA, September 20-21, 2011, Proceedings / / edited by Robin Sommer, Davide Balzarotti, Gregor Maier
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
ISBN	3-642-23644-8
Edizione	[1st ed. 2011.]
Descrizione fisica	1 online resource (X, 399 p.)
Collana	Security and Cryptology ; ; 6961
Disciplina	005.8
Soggetti	Computer communication systems Data encryption (Computer science) Management information systems Computer science Computers and civilization Algorithms Data structures (Computer science) Computer Communication Networks Cryptology Management of Computing and Information Systems Computers and Society Algorithm Analysis and Problem Complexity Data Structures and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Title Page -- Preface -- Organization -- Table of Contents -- Application Security -- Minemu: The World's Fastest Taint Tracker -- Introduction -- A New Emulator Design for Fast Taint Tracking -- Memory Layout -- Data Sandboxing -- Code Sandboxing -- System Calls -- Signal Handling -- Usage -- Register Tagging in Minemu -- SSE Registers Used by Minemu -- Taint Tracking -- Is It Safe to Use SSE Registers? -- Evaluation -- Test Environment -- Effectiveness --

Minemu Performance -- How Does Minemu Compare to Related Work? -- Limitations and Future Work -- Related Work -- Conclusions -- References -- Dymo: Tracking Dynamic Code Identity -- Introduction -- System Overview -- System Requirements -- System Design -- System Implementation -- System Initialization -- Identity Label Generation -- Establishing Identity -- Applications for Dymo -- Application-Based Access Control -- Dymo Network Extension -- Evaluation -- Label Precision -- Effect of Process Tampering -- Performance Impact -- Security Analysis -- Related Work -- Conclusions -- References -- Automated Identification of Cryptographic Primitives in Binary Programs -- Introduction -- Related Work -- Static Approaches -- Dynamic Approaches -- Finding Cryptographic Primitives -- System Overview -- Fine-Grained Dynamic Binary Instrumentation -- Heuristics for Detecting Cryptographic Primitives -- Experimental Evaluation -- Evaluation Environment -- Results -- Off-the-Shelf Application -- Distortion with Executable Packers -- Real-World Malware Sample: GpCode -- Limitations -- Conclusion -- References -- Malware -- Shellzer: A Tool for the Dynamic Analysis of Malicious Shellcode -- Introduction -- Issues to Be Addressed -- Additional Resources Have to Be Available -- A Specific Execution Context Is Required -- Dealing with Malicious Behavior -- Performance Issues -- Evasion Techniques.

Overview of the System -- Architecture -- Analysis Process -- API Calls Detection and Tracing -- API Handling -- Performance Improvements -- Evasion Possibilities -- Evaluation -- Tool Evaluation -- Shellcode's Database Analysis -- Related Work -- Conclusion and Future Work -- References -- KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware -- Introduction -- Background -- Our Approach -- Detector -- Injector -- Shadower -- Classifier -- Optimizing Detection Accuracy -- Evaluation -- Synthetic Evaluation -- Malware Detection -- False Positive Analysis -- Discussion -- Related Work -- Conclusions -- References -- Packed, Printable, and Polymorphic Return-Oriented Programming -- Introduction -- Related Work -- Overview -- One-Layer Printable Packer for ROP -- Two-Layer Printable Packer for ROP -- Two-Layer Encoding and Degree of Polymorphism -- Decoders in Packed Shellcode -- Implementation of dec^1 -- Implementation of dec^2 -- Gadgets Used in Our Implementation -- Experiments and Discussions -- Experiments -- Discussions and Limitations -- Implications -- Extensions of Our Two-Layer Packer -- AV-Immune ROP Packer -- Packing shell Using ROP without Returns -- Conclusion -- Packed ROP for Winamp Exploit on Window 7 -- Packed ROP That is Av-Ammune -- Packed ROP without Returns -- On the Expressiveness of Return-into-libc Attacks -- Introduction -- Traditional View of RILC Attacks (on x86) -- Turing-Complete RILC -- Arithmetic and Logic -- Memory Accesses -- Branching -- System Calls -- Implementation and Evaluation -- Universal Turing Machine Simulator -- Selection Sort -- Discussion -- Related Work -- Conclusion -- References -- Anomaly Detection -- Cross-Domain Collaborative Anomaly Detection: So Far Yet So Close -- Introduction -- Related Work -- System Evaluation -- Data Sets -- Normalized Content.

Content Anomaly Detector and Models -- Alert Exchange -- Scaling to Multiple Sites -- Model Comparison -- Correlation Results -- Conclusions -- References -- Revisiting Traffic Anomaly Detection Using Software Defined Networking -- Introduction -- Background and Related Work -- Background: Software Defined Networking -- Related Work -- Anomaly Detection in Software Defined Networks -- Threshold Random Walk with Credit Based Rate Limiting -- Rate-Limiting --

Maximum Entropy Detector -- NETAD -- Dataset Description -- Benign Network Traffic -- Attack Traffic -- Evaluation -- Experimental Setup -- Ease of Implementation -- Accuracy Evaluation -- Efficiency Evaluation -- CPU Usage -- Conclusions and Future Work -- References -- Modeling User Search Behavior for Masquerade Detection -- Introduction -- Related Work -- Objective and Approach -- Data Gathering and ``Capture the Flag'' Exercise -- Host Sensor -- RUU Dataset -- User Study Experiment -- RUU Experiment -- Modeling -- Experimental Methodology -- Detection Accuracy Evaluation -- Performance Evaluation -- Future Research -- Concluding Remarks -- References -- Network Security -- Securing Application-Level Topology Estimation Networks: Facing the Frog-Boiling Attack -- Introduction -- System Model -- Virtual Coordinate Systems -- Vivaldi Overview -- Attack Model and Strategies -- Single Attack Strategies -- Complex Attack Strategies -- Mitigation Framework -- Background -- Feature Set -- Experimental Results -- Simulation Results -- PlanetLab Results -- Related Work -- Conclusion -- References -- Detecting Traffic Snooping in Tor Using Decoys -- Introduction -- Background -- Tor Anonymity Network -- Threat Model -- System Architecture -- Approach -- Implementation -- Deployment Results -- Discussion and Future work -- Detection Confidence -- Decoy Traffic Credibility.

Detection of HTTP Session Hijacking -- Traffic Eavesdropping and Anonymity Degradation -- Eavesdropping Detection as a Network Service -- Related Work -- Conclusion -- References -- Cross-Analysis of Botnet Victims: New Insights and Implications -- Introduction -- Data Collection and Term Definition -- Cross-Analysis of Botnet Victims -- Point of Departure -- Geographical Distribution of Infected Networks -- IP Address Population -- Remote Accessibility -- Dynamism of IP Address -- Neighborhood Correlation of Botnet Victims -- Watch Your Neighbors -- Cross-Bonet Prediction -- Limitations and Discussions -- Related Work -- Conclusion and Future Work -- References -- Web Security and Social Networks -- Banksafe Information Stealer Detection Inside the Web Browser -- Introduction -- Related Work -- Overview of Banking Trojans -- Detection of Browser Manipulations -- Inline Hooks -- IAT Hooks -- EAT Hooks -- Other Methods -- False Positive Evasion -- Experimental Evaluation -- Classification of Zeus and SpyEye -- AV Signature Detection -- Comparison to Behavior Blockers -- Other Information Stealers -- Legitimate Browser Hooking -- Discussion -- Summary -- Future Work -- References -- IceShield: Detection and Mitigation of Malicious Websites with a Frozen DOM -- Introduction -- Design Overview -- Motivation and Basic Idea -- Dynamic Detection and Protection Framework -- System Implementation -- Heuristics to Identify Suspicious Sites -- Dynamic Instrumentation and Detection -- Scoring Metric -- User Protection -- Implementation as Browser Extension -- Fingerprinting -- Evaluation -- Evaluation Environment -- Classification Results -- Detecting Unknown Exploits -- Performance Results -- Limitations -- Related Work -- Conclusion -- References -- Spam Filtering in Twitter Using Sender-Receiver Relationship -- Introduction -- Background.

Twitter Features -- How Twitter Deals with Spam -- Overview -- Graph -- Features -- Experiments and Evaluation -- Data Collection -- Spam Classification -- Spam Account Detection with Including a User Relation Feature -- Discussion -- Combination of Account Features and Relation Features -- Live Detection -- Limitations -- Conclusion -- References -- Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers -- Introduction -- Related Work -- Data Collection -- Analyzing Evasion Tactics -- Description of Evasion

Sommario/riassunto

This book constitutes the proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection, RAID 2011, held in Menlo Park, CA, USA in September 2011. The 20 papers presented were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on application security; malware; anomaly detection; Web security and social networks; and sandboxing and embedded environments.