Information Flow: A Unified Basis for Vulnerability Mitigation, Malware Defense and Attack Scenario Reconstruction

R. Sekar
Stony Brook University
Stony Brook, NY, USA.
sekar@cs.stonybrook.edu

ABSTRACT

Access control and information flow are the two building blocks in the design of secure software. Of the two, access control seems ubiquitous, being widely used in operating systems, databases, firewalls, servers, web applications, and so on. The successes of information flow seem less obvious, and its benefits and potential underappreciated. Yet, when it comes to defending against malicious code, access control based defenses have proved susceptible to evasion, or they end up being so restrictive as to interfere with legitimate use. In this talk, I will argue that defenses based on information flow can be more discerning, as they utilize not only the operations performed but also their context, e.g., whether malicious actors could be exerting control over these operation or their key arguments. I will then describe successful applications of information flow to defend against every stage of a cyber attack campaign, including: (a) exploit mitigation for a wide range of software vulnerabilities, (b) malware containment across diverse OSes, including Linux, BSD, and Windows XP through Windows 10, and (c) attack campaign reconstruction, where we achieve a five to six orders of magnitude data reduction by applying our techniques.

CCS Concepts/ACM Classifiers

• Security and Privacy: Systems security

Author Keywords

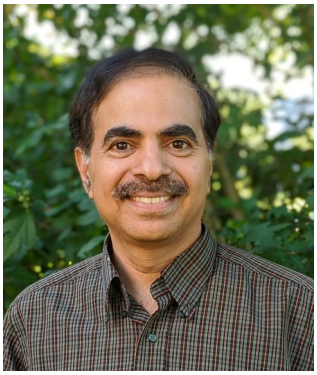
Exploit mitigation, malware defense, attack campaign reconstruction, information flow, access control.

FEAST '20, November 13, 2020, Virtual Event, USA.

ACM ISBN 978-1-4503-8089-8/20/11.
https://doi.org/10.1145/3411502.3418421

BIOGRAPHY

R. Sekar (http://www.cs.stonybrook.edu/~sekar/) is a SUNY Empire Innovation Professor and the Associate Chair of the Computer Science Department at Stony Brook University, where he directs the Secure Systems Lab. He received his Bachelor's degree in Electrical Engineering from IIT, Madras (India), and his Ph.D. in Computer Science from Stony Brook. Sekar's research interests span software and systems security. He is best known for his work on automated vulnerability mitigation, including randomization and taint-based techniques; information-flow based malware containment; intrusion detection and attack campaign investigation; and binary analysis and instrumentation. Sekar's research in these areas has been funded by several grants from AFOSR, DARPA, NSF and ONR, as well as the industry. He has supervised over 125 students, including four postdoctoral and international visiting researchers, 20+ Ph.D.s, and 80+ Master's. Sekar has received SUNY Chancellor's award for Excellence in Research, SUNY Research Foundation's Research and Scholarship award, Best paper awards at USENIX Security and Annual Computer Security Applications Conferences and honorable mention for best paper at SACMAT.



REFERENCES

[1] Sandeep Bhatkar, Daniel DuVarney and R. Sekar, Address Obfuscation: An Efficient Approach to Combat a Broad Range of Memory Error Exploits, USENIX Security, 2003.

[2] Sandeep Bhatkar and R. Sekar, Data Space Randomization, DIMVA 2008.

[3] Md Nahid Hossain, Sadegh Milajerdi, Junao Wang, Birhanu Eshete, Rigel Gjomemo, R. Sekar, Scott D. Stoller and V.N. Venkatakrishnan, SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data, USENIX Sec 2017.

[4] Md Nahid Hossain, Sanaz Sheikhi and R. Sekar, Combating Dependence Explosion in Forensic Analysis Using Alternative Tag Propagation Semantics, IEEE S&P 2020.

[5] Zhenkai Liang, Weiqing Sun, V.N. Venkatakrishnan and R. Sekar, Alcatraz: An Isolated Environment for Experimenting with Untrusted Software, ACM TISSEC 2009.

[6] Sadegh Milajerdi, Rigel Gjomemo, Birhanu Eshete, R. Sekar and V.N. Venkatakrishnan, HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows, IEEE S&P 2019.

[7] Riccardo Pelizzi and R. Sekar, Protection, Usability and Improvements in Reflected XSS Filters, ASIACCS 2012.

[8] R. Sekar, V.N. Venkatakrishnan, Samik Basu, Sandeep Bhatkar and Daniel DuVarney, Model-Carrying Code: A Practical Approach for Safe Execution of Untrusted Applications, SOSP 2003.

[9] R. Sekar, An Efficient Black-box Technique for Defeating Web Application Attacks, NDSS 2009.

[10] Weiqing Sun, R. Sekar, Gaurav Poothia and Tejas Karandikar, Practical Proactive Integrity Preservation: A Basis for Malware Defense, IEEE S&P 2008.

[11] Wai-Kit Sze and R. Sekar, A Portable User-Level Approach for System-wide Integrity Protection, ACSAC 2013.

[12] Wai-Kit Sze and R. Sekar, Provenance-based Integrity Protection for Windows, ACSAC 2015.

[13] Mingwei Zhang and R. Sekar, Control Flow Integrity for COTS Binaries, USENIX Security 2013.