Cloud Data Analytics for Security: Applications, Challenges, and Opportunities

Danfeng (Daphne) Yao
Virginia Tech
Blacksburg, VA 24060
danfeng@vt.edu

ABSTRACT

In this keynote, I describe the emerging need of cloud data analytics for security and call for the security community to devote to closing the gap between research innovation and practical deployment.

Cloud data analytics refer to cloud platforms that provide pattern recognition and data discovery services to clients. This talk will discuss how cloud data analytics can be designed to achieve system security, that is, securing clients' systems against advanced exploits and attacks by providing transparent and seamless automatic data gathering, system behavior monitoring, and feedback. Such a cloud framework has the potential to provide practical security services and has multiple advantages, e.g., update-to-date security protection, scalability, individualized anomaly detection, and ease of deployment. It would allow clients to outsource complex system security monitoring and computation tasks to the cloud/security service providers, without having to tend to tedious low-level details (e.g., model training and tuning, update).

This new direction of security analytics in the cloud presents a wide range of exciting research and business opportunities, as well as unique technical and privacy challenges. I survey the existing data-driven system and network monitoring techniques and discuss what it will take to outsource them to the cloud. The talk will draw from my research experiences on a number of data-driven security projects, including program anomaly detection [2,4], data-leak detection as a service [1,3], and network traffic causal analysis [5].

CCS Concepts/ACM Classifiers

I.0 Computing Methodologies: GENERAL

Keywords

Deployment; security practice; cloud; anomaly detection; software security; system security; exploits and attacks; data analytics

SCC'17, April 2, 2017, Abu Dhabi, United Arab Emirates.
ACM ISBN 978-1-4503-4970-3/17/04.
DOI: http://dx.doi.org/10.1145/3055259.3055266

BIOGRAPHY

Daphne Yao is an associate professor of computer science at Virginia Tech. In the past decade, she has been working on designing and developing data-driven anomaly detection techniques for securing networked systems against stealthy exploits and attacks. Her expertise also includes mobile security and cloud security. Dr. Yao received her Ph.D. in Computer Science from Brown University.

Dr. Yao is an Elizabeth and James E. Turner Jr. '56 Faculty Fellow and L-3 Faculty Fellow. She received the NSF CAREER Award in 2010 for her work on human-behavior driven malware detection, and the ARO Young Investigator Award for her semantic reasoning for mission-oriented security work in 2014. She has several Best Paper Awards (e.g., *ICNP* '12, *CollaborateCom* '09, and *ICICS* '06) and Best Poster Awards (e.g., *ACM CODASPY* '15). She was given the Award for Technological Innovation from Brown University in 2006. She held multiple U.S. patents for her anomaly detection technologies.

Dr. Yao is an associate editor of *IEEE Transactions on Dependable and Secure Computing* (*TDSC*). She serves as PC members in numerous computer security conferences, including *ACM CCS*. She has over 75 peer-reviewed publications in major security and privacy conferences and journals. Daphne is an active member of the security research community. She is currently running for Secretary/Treasurer at ACM Special Interest Group on Security, Audit and Control (SIGSAC) in the 2017 election.

REFERENCES

1. F. Liu, X. Shu, D. Yao, and A. Butt. Privacy-Preserving Scanning of Big Content for Sensitive Data Exposure with MapReduce. In P*roceedings of the ACM Conference on Data and Application Security and Privacy* (*CODASPY*). 2015.
2. X. Shu, D. Yao, and N. Ramakrishnan. Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* (*CCS*). 2015.
3. X. Shu and D. Yao. Data Leak Detection As a Service. In *Proceedings of the International Conference on Security and Privacy in Communication Networks* (*SECURECOMM*). 2012.
4. K. Xu, K. Tian, D. Yao, and B. Ryder. A Sharper Sense of Self: Probabilistic Reasoning of Program Behaviors for Anomaly Detection with Context Sensitivity. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN*). 2016.
5. H. Zhang, D. Yao, N. Ramakrishnan, and Z. Zhang. Causality Reasoning about Network Events for Detecting Stealthy Malware Activities. *Computers & Security* (*C&S*). 58: 180-198. Elsevier. 2016.