Pratyusa K. Manadhata

manadhata@alumni.cmu.edu

RESEARCH INTERESTS

My broad research interest is in cybersecurity, with a current emphasis on (a) data science techniques for operational security, and (b) hardware-software co-design for system security. I have conducted research on and have built systems for data loss prevention, intrusion detection, malware detection, mobile security, and operational security.

EDUCATION

Carnegie Mellon University (CMU), Pittsburgh, PA 2003–2008
Ph.D., Computer Science

Indian Institute of Technology (IIT) Kanpur, India 1997–2001
B.Tech., Computer Science and Engineering

EXPERIENCE

Micro Focus (HPE Software), Sunnyvale, CA 2018–Present
Principal Researcher

- Stolen credential detection from enterprise event logs.
- Compromised user and device detection from event logs.

Hewlett Packard Labs, Princeton, NJ 2015–2017
Principal Researcher

- System and algorithms for enterprise user and entity behavior analysis.
- Time series analysis for behavior anomaly detection.
- Security analyst workflow and remediation.
- Hardware performance counter based ransomware detection.
- Encryption for non-volatile memory.
- Hardware assisted access control and system integrity enforcement.

Hewlett-Packard Laboratories, Princeton, NJ 2011–2014
Senior Researcher

- A decision theoretic approach for data exfiltration detection and remediation.
- Enterprise DNS log collection and analysis for threat detection.
- Malicious domain detection via graph inference.
- Fast submatch extraction for event log normalization.
- Mobile device location authentication.

Symantec Research Labs, Culver City, CA 2009–2010
Researcher

- Reputation based malware detection.
- Large scale malware behavior clustering.
- Text classification for data leakage prevention.

SELECTED AWARDS AND HONORS

1. Participant, Heidelberg Laureate Forum, 2013.
2. Best Paper Award, MobiSec, 2012.

PUBLICATIONS

Invited Book Chapters

1. Sara Mc Carthy, Arunesh Sinha, Milind Tambe, and Pratyusa K. Manadhata, *Decision Theory for Network Security: Active Sensing for Detection and Prevention of Data Exfiltration*, In *Applied Risk Analysis for Guiding Homeland Security Policy and Decisions*, John Wiley and Sons, 2017.
2. Pratyusa K. Manadhata, *Game Theoretic Approaches to Attack Surface Shifting*, In *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, Jajodia et al. (Editors), Advances in Information Security Volume 100, Springer, 2013.
3. Pratyusa K. Manadhata and Jeannette M. Wing, *A Formal Model for A System's Attack Surface*, In *Moving Target Defense: An Asymmetric Approach to Cyber Security*, Jajodia et al. (Editor), Advances in Information Security Volume 54, Springer, 2011.

Journal Articles

4. John Brassil, Pratyusa K. Manadhata, and Ravi Netravalli, *Traffic Signature-based Mobile Device Location Authentication*, IEEE Transactions on Mobile Computing, Volume 12, Issue 9, Sep 2014.
5. Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot, *The Operational Role of Security Information and Event Management Systems*, IEEE Security and Privacy, Volume 12, Issue 5, Sep/Oct 2014.
6. Alvaro Cardenas, Pratyusa K. Manadhata, and Sreeranga Rajan, *Big Data Analytics for Security Intelligence*, IEEE Security and Privacy, Volume 11, Issue 6, Nov/Dec 2013.
7. Pratyusa K. Manadhata and Jeannette M. Wing, *An Attack Surface Metric*, IEEE Transactions on Software Engineering, Volume 37, Issue 3, May 2011.

Peer Reviewed Conference Papers

8. Chandan Chowdhury, Dalton Hahn, Matthew French, Pratyusa Manadhata, Eugene Y. Vasserman, and Alexandru G. Bardas, *eyeDNS: Monitoring a University Campus Network*, IEEE ICC Communication and Information Systems Security Symposium, Kansas City, MO, May 2018.

9. Sara Mc Carthy, Arunesh Sinha, Milind Tambe and Pratyusa K. Manadhata, *Data Exfiltration Detection and Prevention: Virtually Distributed POMDPs for Practically Safer Networks*, 7th Conference on Decision and Game Theory for Security (GameSec), New York, NY, Nov 2016.

10. Amro Awad, Pratyusa K. Manadhata, Stuart Haber, Yan Solihin, and William Horne, *Silent Shredder: Zero-Cost Shredding for Secure Non-Volatile Main Memory Controllers*, 21st ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Atlanta, GA, Apr 2016.

11. Liu Yang, Vinod Ganapathy, Pratyusa K. Manadhata, and Ye Wu, *A Novel Algorithm for Pattern Matching with Back References*, 34th IEEE International Performance Computing and Communications Conference (IPCCC), Nanjing, China, Dec 2015.

12. Pratyusa K. Manadhata, Sandeep Yadav, Prasad Rao, and William Horne, *Detecting Malicious Domains via Graph Inference*, 19th European Symposium on Research in Computer Security (ESORICS), Wroclaw, Poland, Sep 2014.

13. Bill Horne, Stuart Haber, Pratyusa K. Manadhata, Miranda Mowbray, and Prasad Rao, *Efficient Submatch Extraction for Practical Regular Expression*, 7th International Conference on Language and Automata Theory and Applications (LATA), Bilbao, Spain, Apr 2013.

14. Liu Yang, Pratyusa K. Manadhata, William Horne, Prasad Rao, and Vinod Ganapathy, *Fast Submatch Extraction using OBDDs*, 8th ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), Austin, TX, Oct 2012.

15. John Brassil, Ravi Netravali, Stuart Haber, Pratyusa K. Manadhata, and Prasad Rao, *Authenticating a Mobile Device's Location Using Voice Signatures*, 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, Oct 2012.

16. John Brassil and Pratyusa K. Manadhata, *Securing a Femtocell-based Location Service*, International Conference on Selected Topics in Mobile and Wireless Networking (iCOST), Avignon, France, Jul 2012.

17. John Brassil and Pratyusa K. Manadhata, *Verifying the Location of a Mobile Device User*, 4th International Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec), Frankfurt, Germany, Jun 2012.

18. John Brassil and Pratyusa K. Manadhata, *Proving the Location of a Mobile Device User*, Virginia Tech Wireless Symposium, Blacksburg, VA, May 2012.

19. Michael Hart, Pratyusa K. Manadhata, and Rob Johnson, *Text Classification for Data Loss Prevention*, Privacy Enhancing Technologies Symposium (PETS), Waterloo, Canada, Jul 2011.

20. Pratyusa K. Manadhata, Yuecel Karabulut, and Jeannette M. Wing, *Measuring the Attack Surfaces of Enterprise Software*, International Symposium on Engineering Secure Software and Systems (ESSoS), Leuven, Belgium, Feb 2009.

21. Pratyusa K. Manadhata, Yuecel Karabulut, and Jeannette M. Wing, *Measuring the Attack Surfaces of SAP Software Systems*, IEEE International Symposium on Software Reliability Engineering (ISSRE), Seattle, WA, Nov 2008.

Peer Reviewed Workshop Papers

22. Pratyusa K. Manadhata, Sandeep Yadav, Prasad Rao, and William Horne, *Detecting Malicious Domains via Graph Inference*, ACM Computer and Communications Security (CCS) Workshop on Artificial Intelligence and Security (AISec), Phoenix, AZ, Nov 2014.

23. Pratyusa K. Manadhata, *Big Data for Security: Challenges, Opportunities, and Examples*, ACM CCS Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Raleigh, NC, Oct 2012.

24. Pratyusa K. Manadhata, Jeannette M. Wing, Mark A. Flynn, and Miles A. McQueen, *Measuring the Attack Surfaces of Two FTP Daemons*, ACM CCS Workshop on Quality of Protection, Alexandria, VA, Oct 2006.

25. Pratyusa K. Manadhata and Jeannette M. Wing, *An Attack Surface Metric*, USENIX Security Workshop on Security Metrics, Vancouver, BC, August 2006.

PATENTS

Granted

1. *Techniques for classifying non-process threats*, US9652616.

2. *Submatch Extraction*, US9558299.

3. *Authenticating a User's Location in a Femtocell-Based Network*, US9408025.

4. *Submatch Extraction*, US9336194.

5. *System and Method for Vulnerability Risk Analysis*, US9317692.

6. *Security Alert Prioritization*, US9124621.

7. *Mobile Device Location Authentication*, US9094817.

8. *Malware Detection Using File Names*, US9038186.

9. *Inferring A State Of Behavior Through Marginal Probability Estimation*, US9032527.

10. *Malware Detection Using File Names*, US8621233.

11. *Systems and Methods for Classifying Unknown Files/Spam based on a User Actions, a File's Prevalence Within a User Community, and a Predetermined Prevalence Threshold*, US8572007.

12. *Method and Apparatus for Automatically Optimizing a Startup Sequence to Improve System Boot Time*, US8370613.

13. *Measuring Confidence of File Clustering and Clustering Based File Classification*, US8214365.

Pending

14. *DNS Based Infection Scores*, US20170323102.

15. *Packet Logging*, US20170163670.
16. *Advanced Persistent Threat Identification*, US20170070518.
17. *Domain name and Internet Protocol address approved and disapproved membership inference*, US2016-0226819.
18. *Resource Classification Using Resource Requests*, US20160142432.
19. *Resource Reference Classification*, US20160014041.
20. *Assigning An Advertisement*, US20130282497.
21. *Payment Transaction*, PCT/US2013/076451.
22. *Propagating Belief Information about Malicious and Benign Nodes*, PCT/US2015/047380.
23. *Extracted Data Classification to Determine if a DNS Packet is Malicious*, PCT/US2015/047497.
24. *Identification of a DNS Packet as Malicious Based on a Value*, PCT/US2015/047524.
25. *Efficiently Storing Initialization Vectors*, PCT/US2015/050632.
26. *Hardware Support for Efficient Bulk Zeroing in NVM-based Systems*, PCT/US2015/053308.
27. *Silent Shredder: Zero-Cost Zeroing NVMM Controller*, PCT/US2015/053320.
28. *Generation of Site Specific Whitelists using Heavy Hitters*, PCT/US2015/51119.
29. *Abnormal Behavior Detection of Enterprise Entities Using Time-series Data*, 15/386101.
30. *Combining On-Chip Memory and I/O Encryption*, 15/420736.
31. *Intelligent Organization of SIEM Alerts for Investigations*, 15/420417.
32. *Automated Remediation of SIEM Alerts*, 15/420521.
33. *Aggregation and Correlation of Anomalies and Other Weak Indicators*, 15/437230.
34. *Characterizing Anomaly Detection Procedures Using Threat Intelligence*, 15/433136.
35. *Continuous Validation of Analytics using Threat Intelligence*, 15/463562.
36. *User/Entity Profile Risk Scoring*, 15/596041.
37. *Graph-based User/Entity Methods for Security Threat Detection*, 15/596042.
38. *Lateral Movement Detection*, 15/689043.
39. *A Pluggable and Scalable Infrastructure Framework for User and Entity Behavior Analysis*, 15/692655.
40. *Scalable Infrastructure for Lateral Movement Detection*, 15/689045.
41. *Machine Learning Modeling Approaches for Lateral Movement Detection*, 15/689047.

42. *Indicating Malware Generated Domain Names using Digits*, 15/884983.
43. *Indicating Malware Generated Domain Names using n-Grams*, 15/884978.
44. *Indicating Malware Generated Domain Names using Edit Distance*, 15/884988.
45. *Secure Analytics on Encrypted Network Traffic*, 15/885560.
46. *Unauthorized Authentication Event Detection*, 15/959461.
47. *Determining Potentially Malware Generated Domain Names*.

INVITED TALKS

1. *Detection of Authentication Events involving Stolen Enterprise Credentials*, RSA Conference, San Francisco, CA, Apr 2018.
2. *Operational Security Games (Panelist)*, Conference on Decision and Game Theory for Security (GameSec), New York, NY, Nov 2016.
3. *Enterprise Data Exfiltration Detection and Prevention*, IEEE CNS Network Forensics Workshop, Philadelphia, PA, Oct 2016.
4. *Enterprise Data Exfiltration*, USC/ARO Workshop on Cyber Physical Systems, University of Southern California, LA, CA, Feb 2016.
5. *Machine Learning for Enterprise Security (Keynote)*, ACM CCS Workshop on Artificial Intelligence and Security (AISec), Denver, CO, Oct 2015 .
6. *HP Labs Reveals Progress on The Machine (Panelist)*, HP Discover, Las Vegas, NV, Jun 2015.
7. *Security for The Machine*, HP Discover, Las Vegas, NV, Jun 2015.
8. *A Data Science Approach to Enterprise Security*, Department of Computer Science Seminar, New Jersey Institute of Technology, Newark, NJ, Jan 2015.
9. *Big Data Analytics for Security (Panelist)*, IEEE NIST Big Data Public Working Group Workshop, Bethesda, MD, Oct 2014.
10. *Attack Surface Measurement and Reduction*, ARO Workshop on Cyber Security Dynamics, University of North Carolina, Chapel Hill, NC, Sep 2014.
11. *Security Event Management: Challenges and Opportunities*, Applied Communication Sciences, Basking Ridge, NJ, Jun 2014.
12. *Security Event Management: Challenges and Opportunities*, Department of Computer Science and Engineering Colloquium, Penn State University, State College, PA, May 2014.
13. *Big Data Analytics for Security*, IEEE Computer Society's Distinguished Lecturer Webinar, Apr 2014.
14. *Security Event Management: Challenges and Opportunities*, DIMACS Workshop on Secure Cloud Computing, Rutgers University, Piscataway, NJ, Mar 2014.

15. *From "More is less to "More is more: A Sneak Peek at Big Data for Security Research from HP Labs*, HP Discover, Barcelona, Spain, Dec 2013.

16. *Big Data Analytics for Security*, Heidelberg Laureate Forum, Heidelberg, Germany, Sep 2013.

17. *Using Big Data for Good: Security Analytics in the Real World*, The Conference on Big Data Security, Boston, MA, Jul 2013.

18. *Big Data for Security at HP Labs*, AT&T Security Research Center, New York, NY, Feb 2013.

19. *Big Data for Security: Challenges, Opportunities, and Examples*, ACM CCS Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Raleigh, NC, Oct 2012.

20. *Big Data for Security: Challenges, Opportunities, and Experiments*, Experimental Security Panoramas (ESP) for Critical System Protection Workshop, Salt Lake City, UT, Aug 2012.

21. *Game Theoretic Approaches to Attack Surface Shifting*, ARO Workshop on Moving Target Defense, George Mason University, Fairfax, VA, Oct 2011.

22. *An Attack Surface Metric*, AT&T Research, Florham Park, NJ, Apr 2010.

23. *An Attack Surface Metric*, Fujitsu Labs of America, Sunnyvale, CA, Nov 2009.

24. *Measuring the Attack Surfaces of Enterprise Software*, SAP Academic Symposium, Aug 2008.

25. *Measuring Attack Surfaces of Business Applications*, SAP Research, Palo Alto, CA, Jun 2007.

26. *Attack Surface Measurement*, SAP Research, Karlsruhe, Germany, May 2007.

MENTORING

Ph.D. Thesis Committee

1. Amruta Gokhale, Rutgers University, 2015.

Research Interns

2. Ihsan Sarfraz, Purdue University, 2017.

3. Kyle Williams, University of California Irvine, 2017.

4. Hai Nguyen, Rutgers University, 2016.

5. Vasudevan Rengasamy, Pennsylvania State University, 2016.

6. Amro Awad, North Carolina State University, 2015.

7. Daeyoung Kim, Rutgers University, 2015.

8. Jannik Franz, Cooperative State University Stuttgart, 2015.

9. Alex Bardas, Kansas State University, 2014.

10. Amruta Gokhale, Rutgers University, 2013.

11. Xiang Cai, Stony Brook University, 2012.

12. Liu Yang, Rutgers University, 2011.

13. Sandeep Yadav, Texas A&M University, 2011.

14. Michael Hart, Stony Brook University, 2010.

Masters Thesis Co-Supervision

15. E. Chaos Golubitsky, Carnegie Mellon University, 2005.

SERVICES

Program Committee Member

1. International Conference on Science of Cyber Security (SciSec), 2018.

2. ACM CCS Workshop on Artificial Intelligence and Security (AISec), 2013, 2014, 2015, 2016, and 2017.

3. European Symposium on Research in Computer Security (ESORICS), 2013, 2016, and 2017.

4. IEEE CNS Network Forensics Workshop, 2016.

5. IEEE International Symposium on Resilient Cyber Systems, 2013, 2014, 2015, 2016, and 2017.

6. International Conference on Network and System Security (NSS), 2015.

7. IARIA International Conference on Wireless and Mobile Communications, 2014.

8. ACM International Conference of Security of Internet of Things (SecurIT), 2012.

9. IFIP International Conference on Trust Management, 2010, 2011, and 2012.

10. EUROMICRO Workshop on Security Metrics and Measurement in Software-Intensive Systems, 2011.

11. ESSoS Workshop on Security Predictions, 2011.

Working Groups

12. *Co-lead*, Data Analytics, Cloud Security Alliance Big Data Working Group, 2012–2014.

Reviewer

13. ACM Computing Surveys, ACM Transactions on Security and Privacy, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE/ACM Transactions on Networking, IEEE Security and Privacy, IEEE Transactions on Software Engineering, and Information and Software Technology.