Svetlana Radosavac

✉ *contact@svetlanaradosavac.com*
http://www.svetlanaradosavac.com

Areas of expertise

Cyber Security, Fraud detection, Big Data, Machine Learning, Social Network Analysis (information and influence propagation, malware propagation), Wireless networks, game theory

Education

2002-2007 **PhD in Electrical and Computer Engineering**

University of Maryland College Park

Thesis: Intrusion Detection for Defense at the MAC and Routing Layers of Wireless Networks

2000-2002 **M.Sc. in Electrical and Computer Engineering**

University of Maryland College Park

Thesis:Detection and Classification of Network Intrusions using Hidden Markov Models

1999 **B.Sc. in Electrical and Computer Engineering**

University of Belgrade, Serbia

Experience

Nov. 2017 - current **Lead Analytic Scientist - CYber security**, *Fair Isaac Corporation (FICO)*, San Diego, CA.

- Part of the team that develops algorithms for detection of cybersecurity threats. Current responsibilities include development of big data tools for data analysis, machine learning algorithms for detection and prevention of threats and development of new features for threat prevention/detection. Tools used: PySpark SQL, Python, , scikit-learn, TensorFlow, Keras, Java.

Sept. 2017 - Nov. 2017 **Analytic Scientist**, *Fair Isaac Corporation (FICO)*, San Diego, CA.

- Part of the team that works on developing models for detecting cyber security threats in real time. My current responsibilities involve mathematical modeling of security threats (DDoS attacks, beaconing, exfiltration, DNS tunneling, trojans, etc.) and traffic analysis (daily network traffic from company network) using big data techniques. I have designed, tested and implemented numerous features for detecting threats in DNS, HTTP and Netflow. The developed adaptive learning model can detect brute force attacks within a couple of seconds and is able to detect a wide range of attacks by creating profiles for devices, DNS query names, IP addresses etc. Tools used: Java, Python, Spark, Storm, Hadoop
- Application of graph databases for network security. Modeled network traffic using graph databases (Netflow, HTTP and DNS). The tools was used for detecting anomalous network behavior, vulnerabilities and network misconfigurations Tools used: Neo4j.
- Application of graph databases for credit card fraud detection and network security. Modeled complex fraud networks with hundreds of millions of nodes and applied graph databases to detect points of compromise, credit card testing sites and fraudulent transactions. Tools used: Neo4j, Py2Neo and Groovy
- Big data analytics. Part of the team that developed automated Spark-based tools for analysis of network traffic. The tools are used for data quality analysis, traffic volume analysis and detection of anomalous and malicious instances of network traffic and can operate on hundreds of millions of records and process several days worth of network traffic.

Independent Consultant, *Big data and Machine Learning*, San Francisco, CA.

Worked on a number of projects involving collecting and processing data and applying machine learning algorithms for predicting future behavior using Twitter. One of the projects involves using Twitter Streaming API to collect data based on specific keywords and apply sentiment analysis to predict public opinion towards a public figure being tracked. In addition to that, the project involves retweet propagation analysis and application of Machine Learning algorithms for prediction of link propagation. Tools used: MongoDB, NetworkX, Gephi, Python.

Research Scientist, *DOCOMO Innovations*, Palo Alto, CA.

Big Data Driven Content Distribution using SDN Approach, *ICC 2011 best paper award*.

- Modeled a mobile network based on social connections of users
- Investigated how influentals affect information propagation in social networks
- Using data analysis predicted service adoption in cellular networks
- Designed a model for controlling the user exposure to different services to achieve a target utilization based on their previous behavior
- Used the results for slowing down propagation of malicious applications in mobile networks

Security management for open mobile platforms.

- Investigated security problems in open/semi-open mobile networks: creation of botnets by malicious applications, propagation of malicious applications in mobile networks and their impact on service availability
- Proposed admission policies for constructing a secure mobile network

Incentive Engineering for Network Security in Collaboration with UC Berkley School of Information, *[Project Manager]*.

- Behavioral economics:
  - Effects of framing on individual's decisions towards or against adopting network policies
  - Tradeoffs of investing in protection versus insurance and the effects on security;
  - The role of experts and intermediaries in the coordination of security investments;
  - Incentives of cyber criminals
- Using insurance to increase internet security
  - Proposed a new approach to the problem of Internet security by managing the residual risk by buying insurance against it and consequently re-arranging the incentive chain.
- Rebuilding the internet architecture: DDoS attacks and protection against them
  - Providing solutions for the architecture that ensures robustness against DDoS attacks by rearranging the economic incentives and removing the burden of dealing with unwanted traffic from the receiver.

Postdoctoral Research Assistant, *Institute for Systems Research*, College Park, MD.

- Worked on the following projects:
  - Secure Component Based routing (CBR) for MANETS
  - Impact of MAC layer misbehavior on the Network Layer

Graduate Research Assistant, *Institute for Systems Research*, College Park, MD.

- Worked on the following projects:
  - Resilient Cooperative Intrusion Detection Systems
  - Modeling and detecting access layer misbehavior in wireless networks
  - Impact of MAC layer misbehavior on the Network Layer
  - Application of Machine Learning Techniques for detecting intrusions
  - Fast Innate and Adaptive Immune Systems

Professional activities

Reviewer for most major security and networking journals and conferences:

Security: ACM Transactions on Information and System Security (TISSEC), IEEE Transactions on Dependable and Secure Computing, IEEE Security and Privacy Symposium, ACM Conference on Computer and Communications Security CCS,Recent Advances in Intrusion Detection (RAID), USENIX Security Symposium, Applied Cryptography and Network Security (ACNS), ACM Workshop on Security of Ad Hoc and Sensor Netowrks (SASN),GameNets.

Networking: IEEEACM Transactions on Networking, IEEE Wireless Communications, Elsevier Ad Hoc Networks, IEEE Transactions on Mobile Computing, ACM Conference on Mobile Computing and Networking (Mobicom), USENIX Sympsium on Networked Systems Design & Implementation (NSDI), IEEE Infocom, WISE, Mobicom, Mobihoc, IEEE ICC.

Selected publications

Journals.

1. S. Radosavac, U. Kozat and J. Kempf, "On the Use of Admission Control to prevent DDoS Attacks on Mobile Networks", submitted to Transactions on Mobile Computing
2. A. A. Cardenas, S. Radosavac and J. S. Baras, "Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments", IEEEACM Transactions on Networking (ToN), Pages 605-617, Vol. 17, Issue 2. April 2009.
3. S. Radosavac, G. V. Moustakides, J. S. Baras and I. Koutsopoulos, "An analytic framework for modeling and detecting access layer misbehavior in wireless networks", ACM Transactions on Information and System Security (ACM TISSEC), Vol. 11, No. 4, July 2008.
4. S. Radosavac and J. S. Baras, "Application of Sequential Detection Schemes for Obtaining Performance Bounds of Greedy Users in the IEEE 802.11 MAC", IEEE Communications Magazine: special issue on Security in Mobile Ad Hoc and Sensor Networks, pages 148-154, Vol. 46, No. 2, February 2008.
5. S. Radosavac, A. A. Cardenas, J. S. Baras and G. V. Moustakides, "Detecting IEEE 802.11 MAC Layer in Ad Hoc Networks: Robust strategies against individual and colluding attackers" Journal of Computer Security, special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 103-128, Jan 2007.

Conferences.

1. H. Sharara, C. Westphal, S. Radosavac and U. C. Kozat, "Utilizing Social Influence in Content Distribution Networks" in Proceedings of IEEE ICC-2011, Kyoto, Japan, 2011 (best paper award)
2. J. Grossklags, S. Radosavac, A. Cardenas, J. Chuang, "Nudge: Intermediaries' Role in Interdependent Network Security" Proceedings of 3rd International Conference on Trust and Trustworthy Computing (Trust'10), June 2010.
3. A. Cardenas, S. Radosavac, J. Grossklags, J. Chuang and C. Hoofnagle, "An Economic Map of Cybercrime", 37th Research Conference on Communication, Information and Internet Policy (TPRC) 2009, George Mason University Law School, Arlington, VA, September 25-27, 2009.
4. S. Radosavac, U. C. Kozat and J. Kempf, "On the Use of Admission Control for Better Quality of Security", ICC 2009, June 14-18 2009, Dresden, Germany
5. S. Radosavac, J. Kempf and U. C. Kozat , "Using Insurance for Increasing Internet Security", ACM SIGCOMM Workshop on the Economics of Networks, Systems and Computation (NetEcon '08), August 22, Seattle, WA
6. A. A. Cardenas, S. Radosavac and J. S. Baras, "An Analytical Evaluation of MAC Layer Misbehavior Detection Schemes", Proceedings of the 26th Annual IEEE Conference on Computer Communications, INFOCOM 2007.
7. S. Radosavac, J. S. Baras and G. V. Moustakides, "Impact of Optimal MAC Layer Attacks on the Network Layer", SASN '06: Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 135-146, October 2006.
8. S. Radosavac, J. S. Baras and I. Koutsopoulos,"A framework for MAC protocol misbehavior detection in wireless networks", WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pp. 33-42, Cologne, Germany, September 2, 2005.
9. A. A. Cardenas, S. Radosavac and J. S. Baras, "Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks", SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 17-22, Washington, DC, October 25, 2004.
10. J. S. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANETs", Workshop on 'Cross-Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management, Naval Research Laboratory, Washington, DC, June 2-3, 2004.
11. S. Radosavac and J. S. Baras, "Detection and classification of network intrusions using Hidden Markov Models", 37th Conference on Information Sciences and Systems (CISS), Baltimore, March 2003.

Patents

1. S. Radosavac, J. Kempf and U. Kozat, Method and apparatus for compensating for and reducing security attacks on network entities [pending]
2. U.Kozat, S. Radosavac and J. Kempf, Method and apparatus for security-risk based admission control [United States 8,316,428. Issued November 20, 2012]

Other

Work authorization: US citizen