Phani Vadrevu

Computer Science Department
2000, Lakeshore Drive, New Orleans LA 70148
Office Phone: 504-280-4388 **E-mail**: phani@cs.uno.edu
Site: https://www.phanivadrevu.com

Assistant Professor of Computer Science **August 2018 – Now**
University of New Orleans (UNO), New Orleans LA
Faculty Member, Greater New Orleans Center for Information Assurance (GNOCIA)

- Teaching courses in Computer Science and Computer Security for undergraduate and graduate students
- Leading a team of 2 PhD, 3 Masters and 2 undergrad students in conducting research on various computer security topics. Our team is currently working on various research topics related to measuring and defending against various social engineering attacks such as phishing and technical support scams and studying browser fingerprinting mechanisms.
- Mentoring 3 external PhD students in conducting research related to new attack vectors on the web, technical support scams and malicious advertising.
- Regularly reviewing papers being submitted to top computer security journals such as IEEE TSDC, Elsevier COSE, ACM TOPS, IEEE TNSM.

Postdoctoral Research Associate, NIS Lab **August 2017 – July 2018**
University of Georgia (UGA), Athens GA

- Developed a system that can classify and detect various malicious advertisements that launch social engineering attacks on the web. The system can work at a large scale and automatically detect many currently undetectable malicious advertisements. This research work is currently under conference submission process.

PhD Student, Network Intelligence and Security Lab **August 2011 – July 2017**
University of Georgia (UGA), Athens GA

- Developed "ChromePic", a modified version of the Chromium web browser to allow for light-weight, platform-agnostic recording of user interactions with the browser for forensic analysis. We modified the source code of Chromium to allow for taking screenshots and DOM snapshots in an efficient manner. The work resulted in a publication at NDSS 2017 conference.
- Developed "MAXS", a novel probabilistic testing framework for scaling malware execution in dynamic analysis sandbox environments. We were able to reduce malware execution time by up to 50% using this system. The work resulted in a publication at ASIACCS 2016.
- Developed "AMICO", a network-based malware classification system that detects previously unknown malware executables in live networks using provenance information. The code was developed using C and Python using Weka for machine learning. The work resulted in a publication at ESORICS 2013. This system is currently deployed at 3 large universities and has also received funding from the DHS to transition to commercial markets. The project code is hosted at https://github.com/perdisci/amico/
- Developed a web-interface using D3.js for visualizing clusters produced by "FluxBuster", a system that detects live fast-flux networks.

Education

PhD, University of Georgia, Athens, USA **August 2010 – July 2017**

Major: Computer Science with focus on Web/Network Security and Machine Learning

BE, Birla Institute of Technology and Science, Pilani, India **August 2006 – May 2010**

Major: Mechanical Engineering

Grants

- **NSF**: "Collaborative Research: SaTC: CORE: Medium: Defending Against Social Engineering Attacks with In-Browser AI"; PI: $399,979; Total award: $1.2M
  https://www.nsf.gov/awardsearch/showAward?AWD_ID=2126655

Publications

1. Bhupendra Acharya, **Phani Vadrevu**
   "*PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling*"
   USENIX Security 2021, Online (Acceptance rate 18.7% = 246/1316)
   Artifact Evaluated
   Awards: Google Vulnerability Research Award ($5,000) for "abuse-related methodologies", Google Vulnerability Research Grant for "abuse-related methodologies" ($3133.7)
   https://www.phanivadrevu.com/files/papers/phishprint.pdf

2. Karthika Subramani, Xingzi Yuan, Omid Setayeshfar, **Phani Vadrevu**, Kyu Hyung Lee, Roberto Perdisci
   "When Push Comes to Ads: Measuring the Rise of (Malicious) Push Advertising"
   International Measurement Conference
   IMC 2020, Online (Acceptance rate 24.5% = 53/216)
   http://www.phanivadrevu.com/files/papers/pushads.pdf

3. **Phani Vadrevu**, Roberto Perdisci
   "What You See is NOT What You Get: Discovering and Tracking Social Engineering Ad Campaigns"
   International Measurement Conference
   IMC 2019, Amsterdam, Netherlands (Acceptance rate 19.3% = 38/197)
   http://www.phanivadrevu.com/files/papers/seacma.pdf

4. Bo Li, **Phani Vadrevu**, Kyu Hyung Lee, Roberto Perdisci
   "*JSgraph: Enabling Reconstruction of Web Attacks via Efficient Tracking of Live In-Browser JavaScript Executions*"
   Network and Distributed System Security Symposium
   NDSS 2018, San Diego, U.S. (Acceptance rate 21.5% = 71/331)
   http://www.phanivadrevu.com/files/papers/jsgraph.pdf

5. **Phani Vadrevu**, Jienan Liu, Bo Li, Babak Rahbarinia, Kyu Hyung Lee, Roberto Perdisci.
   "*Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots*"
   Network and Distributed System Security Symposium
   NDSS 2017, San Diego, U.S. (Acceptance rate 16.1% = 68/423)
   http://www.phanivadrevu.com/files/papers/chromepic.pdf

6. **Phani Vadrevu**, Roberto Perdisci.
   "*MAXS: Scaling Malware Execution with Sequential Multi-Hypothesis Testing*"
   11th ACM Asia Conference on Computer and Communications Security
   ASIACCS 2016, Xi'an, China (Acceptance Rate: 20.9% = 73/350)
   http://www.phanivadrevu.com/files/papers/maxs.pdf

7. **Phani Vadrevu**, Babak Rahbarinia, Roberto Perdisci, Kang Li, Manos Antonakakis.
   "*Measuring and Detecting Malware Downloads in Live Network Traffic*"
   18th European Symposium on Research in Computer Security
   ESORICS 2013, Egham, U.K. (Acceptance Rate: 17.8% = 43/242)
   http://www.phanivadrevu.com/papers/amico.pdf

Invited Talks and Demos

1. "*Discovering Ad-driven Social Engineering Campaigns at Scale*"
   January 29th, 2021.
   Georgia Tech Cybersecurity Lecture Series, Virtual Session
2. "*Discovering and Tracking Ad-driven Social Engineering Attack Campaigns*"
   December 17th, 2020.
   NSA CAE Tech Talk, Virtual Session
3. "*Discovering and Tracking Ad-driven Social Engineering Attack Campaigns*"
   October 16th, 2020.
   DXC Analytics Guild, Virtual Session
4. *"Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots"*
   January 27th, 2017.
   Georgia Tech Cybersecurity Lecture Series, Atlanta, GA
5. *"AMICO: Detecting malware downloads in live networks"*
   October 25th, 2016.
   DHS TTP Technology Demonstration – Financial Sector, New York, NY
6. *"AMICO: Detecting malware downloads in live networks"*
   August 19th, 2015.
   DHS TTP Technology Demonstration – Silicon Valley, Santa Clara, CA
7. *"Improvements to Glastopf, the web application honeypot"*
   February 12th, 2013.
   The Honeynet Project Workshop Demo, Dubai, UAE

Teaching Experience:

1. Introduction to Cryptography (CSCI 4130/5130)
   Fall 2018, Spring 2020, Spring 2021, Spring 2022
   Graduate and undergraduate course

2. Principles of Operating Systems (CSCI 4401/5401)
   Spring 2019, Fall 2019, Spring 2020, Spring 2021, Spring 2022
   Graduate and undergraduate course

3. Introduction to Cybersecurity (CSCI 4621/5621)
   Spring 2019, Fall 2020
   Graduate and undergraduate course

4. Research Topics in Web Security (CSCI 6990)
   Fall 2020
   Graduate and undergraduate course

5. Introduction to Cloud Computing (CSCI 4452/5452)
   Fall 2021
   Graduate and undergraduate course

6. Network Operations and Defenses (CSCI 4460/5460)
   Fall 2021
   Graduate and undergraduate course

Professional Service:

1. *Program Committee Member*
   ACSAC 2022
   CODASPY 2020-22
   MADWeb (co-located with NDSS) 2021-22

2. *Proposal Review Panelist*
   NSF SBIR/STTR, 2019

3. *Journal Reviewer*
   ACM Transactions on the Web (TWEB)
   IEEE Transactions on Dependable and Secure Computing (TDSC)
   ACM Topics on Privacy and Security (TOPS)
   Elsevier Computers & Security (COSE)
   International Journal of Information Security (IJIS)
   IEEE Transactions on Network and Service Management (TNSM)