Director's Notes

CFITS

Center for Forensics, Information Technology, and Security

School of Computing

March 2021

DATA SCIENCE

Every Other Wednesday

4:45 to 6:00PM
Shelby Hall Rm 3104

SYSTEMS PROTECTION AND EXPLOITATION RESEARCH GROUP (SPERG)

Every Friday 10 – 11 a.m.
@Shelby Hall Rm 2327
www.soc.southalabama.edu/sperg/

PARTNER SCHOOL PROGRAM

Contact Keith Lynn at 251-460-7643. For scheduling HOLLA click on the link below.

Schedule HOLLA

Quote of the Month

"Treat your passwords like your toothbrush. Don't let anybody else use it, and get a new one every six months".

Clifford Stoll
(American Astronomer)

CFITS Lecture Series: Gary McGraw

Wednesday, March 17th at 2:30 pm

Virtual lecture: Zoom link:
https://southalabama.zoom.us/j/97833765945

Alumni Profile

Sabina Zafar

USA SoC Graduate of 2001

General Digital Electric

Enterprise Architecture Leader

Sabina Zafar graduated from USA's School of Computing in May 2001 with a degree in Information Systems. As a student, she participated in ACM and shares that the Senior Project was one of her favorite classes as it pushed her to think outside the box, work independently and collaborate with her professor. "I enjoyed having discussion with my professor, being challenged as well as challenging him. It opened up my mind to looking at the same problem multiple ways," she states.

Sabina's career path provided her with many opportunities for growth. After graduation, she worked for a year with Southwest Alabama Mental Health where she built and established an electronic patient check-in form system. She moved to Scottsdale, Arizona in 2003 where she started her own web design company which allowed her to work at home while raising her two young children. She moved to San Ramon, California in 2006 and began work at an Edtech company in 2007. Over the next ten years, Sabina worked with several companies and across several verticals including healthcare, financials, advertisement, publishing, gaming, manufacturing, oil & gas and power.

In 2017, General Electric Digital recruited her for their Corporate Leadership Program, which led to her role as Senior Director of Technology where she manages a global team of engineering professionals including enterprise architects, software developers and program managers. She recently joined the Electric Grid organization at GE Digital and provides technical leadership to key accounts. She currently serves as Enterprise Architecture Leader for the company.

Happy St. Patrick's Day!!!

CFITS

March 2021

CFITS Speaker Profile

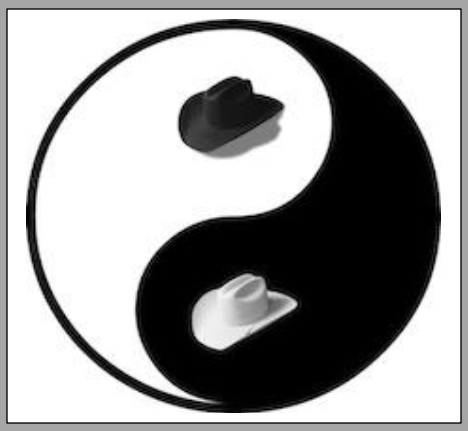
Gary McGraw

Co- Founder/ Author
Co-Founder of Berryville Institute of Machine Learning
https://garymcgraw.com
https://berryvilleiml.com/

Gary McGraw is co-founder of the Berryville Institute of Machine Learning. He is a globally recognized authority on software security and the author of eight best-selling books on this topic. His titles include Software Security, Exploiting Software, Building Secure Software, Java Security, Exploiting Online Games, and 6 other books; and he is editor of the Addison-Wesley Software Security series. Dr. McGraw has also written over 100 peer-reviewed scientific publications. Gary serves on the Advisory Boards of Code DX, Maxmyinterest, Runsafe Security, and Secure Code Warrior. He has also served as a Board member of Cigital and Codiscope (acquired by Synopsys) and as Advisor to Black Duck (acquired by Synopsys), Dasient (acquired by Twitter), Fortify Software (acquired by HP), and Invotas (acquired by FireEye). Gary produced the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine for thirteen years. His dual PhD is in Cognitive Science and Computer Science from Indiana University where he serves on the Dean's Advisory Council for the Luddy School of Informatics, Computing, and Engineering.

CFITS Lecture Title: Security Engineering for Machine Learning
(Read below for preview)

Machine Learning appears to have made impressive progress on many tasks including image classification, machine translation, autonomous vehicle control, playing complex games including chess, Go, and Atari video games, and more. This has led to much breathless popular press coverage of Artificial Intelligence, and has elevated deep learning to an almost magical status in the eyes of the public. ML, especially of the deep learning sort, is not magic, however. ML has become so popular that its application, though often poorly understood and partially motivated by hype, is exploding. In my view, this is not necessarily a good thing. I am concerned with the systematic risk invoked by adopting ML in a haphazard fashion. Our research at the Berryville Institute of Machine Learning (BIIML) is focused on understanding and categorizing security engineering risks introduced by ML at the design level. Though the idea of addressing security risk in ML is not a new one, most previous work has focused on either particular attacks against running ML systems (a kind of dynamic analysis) or on operational security issues surrounding ML. This talk focuses on two threads: building a taxonomy of known attacks on ML and the results of an architectural risk analysis (sometimes called a threat model) of ML systems in general. A list of the top five (of 78 known) ML security risks will be presented.



CFITS Lecture Zoom Link: https://southalabama.zoom.us/j/97833765945