

UCF Faculty Cluster Initiative and Dept. of Computer Science

Spring 2018 Seminar Series

An Adaptive Multi-Factor Authentication (A-MFA) Methodology February 1st 2018

Time 9:30am-10:30am – HEC 101A

Multi-factor Authentication (MFA) is the current trend to genuinely identify authorized users (in multiple ways) through an authentication process via passwords, security tokens, biometrics, cognitive behavior metrics, software/hardware sensors, etc. Existing MFA systems typically use static policies for selecting authentication factors and do not consider dynamic aspects of the operating environment. We are developing an authentication framework for adaptive selection of multiple modalities at different operating environment so to make authentication strategy unpredictable to the hackers. This methodology, called adaptive multi-factor authentication (A-MFA) incorporates a novel approach of calculating trustworthy values of different authentication factors while being used under different user environmental settings. Accordingly, a subset of authentication factors are determined (at triggering events) on the fly thereby leaving no exploitable a priori pattern or clue for adversaries. Empirical studies are conducted with varying environmental settings and the performance of the adaptive MFA is compared with other selection strategies. The empirical results reflects that such a methodology of adaptive authentication can provide legitimacy to user transactions with an added layer of access protection that is not rely on a fixed set of authentication modalities. Robustness of the system is assured by designing the framework in such a way that if any modality data get compromised, the system can still perform flawlessly using other non-compromised modalities. Scalability can also be achieved by adding new and/or improved modalities with existing set of modalities and integrating the operating/configuration parameters for the added modality. A Patent (#14/968676) on Adaptive Multi-Factor Authentication System is approved/allowed on November 2017.

The talk will also cover a summary of other recent research and outreach activities of the Center of Information Assurance at the University of Memphis.

Dr. Dipankar Dasgupta

Dipankar Dasgupta, IEEE Fellow Director, Center for Information Assurance
Professor of computer science at The University of Memphis



Dipankar Dasgupta is a Professor of Computer Science at the University of Memphis. Dr. Dasgupta is at the forefront of research in applying bio-inspired and machine learning approaches to cyber defense. Some of his groundbreaking works, like digital immunity, negative authentication, cloud insurance model, and Auth-Spectrum put his name in Computer World Magazine and other News media. Prof. Dasgupta is an Advisory Board member of Geospatial Data Center (GDC), Massachusetts Institute of Technology since 2010, and worked on joint research projects with MIT. His latest textbook on *Advances in User Authentication* is published by Springer-Verlag, August, 2017.

Dr. Dasgupta has more than 250 publications with 14000+ citations and having h-index of 55 as per Google scholar. He received five Best Paper Awards at international conferences (1996, 2006, 2009, 2012 and 2017) and two Best Runner-Up Paper Awards (2013 and 2014): one from ACM Information Security Curriculum Development in October 2013, and the other from ACM Cyber and Information Security Research (CISR-9) Conference in April 2014. He is the recipient of 2012 Willard R. Sparks Eminent Faculty Award, the highest distinction and most prestigious honor given to a faculty member by the University of Memphis. Prof. Dasgupta received the 2014 ACM SIGEVO Impact Award, and also designated as an ACM Distinguished Speaker. Since 2009 he has been organizing Symposium on Computational Intelligence in Cyber Security (CICS) at the IEEE Symposium Series on Computational Intelligence (SSCI) and annual Cyber Security Summit at Memphis

In addition to Prof. Dasgupta's research and creative activities, he also spearheads the University of Memphis's education, training and outreach activities on Information Assurance (IA). He is the founding Director of the Center for Information Assurance (CIA) which is a National Center for Academic Excellence in Information Assurance Education (CAE-IAE) and in Research (CAE-R). He is leading the University's CAST (Cluster to Advance Cyber-Security and Testing) initiative (funded by the FedEx Corporation) in promoting cross-disciplinary information security research. He has been involved in forming the National Cybersecurity Preparedness Consortium ([NCPC](#)) and continually receiving DHS/FEMA projects. Because of the center's wide range of activities, the University of Memphis is in the forefront of information security research, education, and outreach in the state as well as in the region.

Hosted by: **Dr. Gary Leavens**



4328 Scorpis Street

Orlando, FL 32816

WWW.CS.UCF.EDU