AI for Security & Security of AI

A talk by Prof. Dipankar Dasgupta — IEEE & NAI Fellow

Please join us for a timely talk on the dual challenge of using AI to defend against cyber threats and defending AI itself from adversarial attacks. Prof. Dasgupta, a Fulbright Distinguished Scholar and world-renowned expert in computational intelligence for cybersecurity, will draw on three decades of research to survey the evolving attack landscape, the promise and pitfalls of LLMs in security, and a novel dual-filtering strategy for making AI systems more trustworthy. Whether you work in security, machine learning, or simply want to understand the stakes, you will want to attend this talk.

DATE	TIME	LOCATION
March 25, 2026	**10:30AM**	**Dunn Hall 129** **University of Memphis**

SPEAKER

Prof. Dipankar Dasgupta

William Hill Professor in Cybersecurity | Director, Center for Information Assurance (CfIA)

Department of Computer Science, University of Memphis

IEEE Fellow · NAI Fellow · ACM Distinguished Speaker · Fulbright Scholar 2024

ABSTRACT

Artificial Intelligence encompasses a broad family of techniques — neural networks, fuzzy logic, evolutionary computation, immunological computation, game theory, and more — that have been applied to cybersecurity for over 30 years. This talk surveys how AI-guided strategies are used today for real-time monitoring, malware detection, intrusion detection, and log analysis, as well as the evolving cyber-attack landscape they must confront.

A key focus will be the effectiveness and limitations of pre-trained Large Language Models (LLMs) in identifying and mitigating emerging threats. As LLMs grow more capable, so do the risks: researchers are finding ways to insert backdoors into models that can generate phishing emails, write polymorphic malware, and automate reconnaissance.

To address the security of AI itself, Prof. Dasgupta will present a **dual-filtering (DF)** defense strategy that mitigates both input-data and model-manipulation attacks. By inspecting the output decision boundary with a secondary classifier, the DF approach improves the trustworthiness of any ML-based decision-support system — without requiring adversarial sample generation — and remains robust to adaptive attacks through continual boundary updates. The talk will highlight how integrated AI techniques can bolster holistic cyber defense and why securing trustworthy AI is essential for safety-critical applications.

ABOUT THE SPEAKER

Dr. Dipankar Dasgupta has been a Professor of Computer Science at the University of Memphis since 1997 and is a leading expert in bio-inspired and machine-learning approaches to cyber defense. His pioneering work, including digital immunity, negative authentication, cloud insurance models, and adaptive authentication — has been recognized in outlets such as *Computer World Magazine*. With over 350 publications (including 4 patents), 23,000+ citations, and an h-index of 68, his research impact is widely acknowledged. Honors include the 2023 Presidential Award for Lifetime Achievement in Research, the 2014 ACM SIGEVO Impact Award, the 2012 Willard R. Sparks Eminent Faculty Award, and the NSF-Fulbright Distinguished Scholar award (2024). As founding Director of the Center for Information Assurance, he has led nationally designated Centers of Academic Excellence in both Education and Research since 2004 and has delivered over 300 invited talks worldwide.