

CReWMaN and CSE@UTA Joint Seminar

Data Mining for Malicious Code Detection and Security Applications

SPEAKER: Dr. Bhavani Thuraisingham

Professor of Computer Science

Director of the Cyber Security Research Center

The University of Texas at Dallas

Date: Friday, Dec 1, 2006

Time: 10 am - 12 noon

Venue: WH 413 (CReWMaN Lab)

Abstract:

Data mining is the process of posing queries and extracting patterns, often previously unknown from large quantities of data using pattern matching or other reasoning techniques. Data mining has many applications in security including for national security as well as for cyber security. The threats to national security include attacking buildings, destroying critical infrastructures such as power grids and telecommunication systems. Data mining techniques are being investigated to find out who the suspicious people are and who is capable of carrying out terrorist activities. Cyber security is involved with protecting the computer and network systems against corruption due to Trojan horses, worms and viruses. Data mining also provide solutions in intrusion detection, auditing, credit card fraud detection and biometrics related applications. Other applications include data mining for malicious code detection such as worm detection and managing firewall policies. The challenge is to reduce false positives and false negatives. Additionally, we need to maintain the privacy of individuals. Much research has been carried out on privacy preserving data mining.

This presentation will provide an overview of data mining, the various types (real-time and non-real-time) of threats and then discuss the applications of

data mining for malicious code detection and cyber security. We will also discuss the consequences to privacy.

Biography:

Dr. Bhavani Thuraisingham joined The University of Texas at Dallas in 2004 as a Professor of Computer Science and Director of the Cyber Security Research Center in the Erik Jonsson School of Engineering and Computer Science. She is an elected Fellow of the IEEE for her work in data security. She received the IEEE Computer Society's prestigious 1997 Technical Achievement Award for outstanding and innovative contributions to secure data management.

Her work in information security and information management has resulted in over 70 journal articles, over 200 refereed papers in conferences and workshops, and three US patents. She is the author of seven books in data management, data mining and data security. She has given over 30 keynote presentations at various technical conferences and has also given invited talks at the White House Office of Science and Technology Policy and at the United Nations on Data Mining for counter-terrorism. She currently serves as the Editor in Chief of Computer Standards and Interfaces Journal.

Prior to joining UTD, Dr. Thuraisingham was at NSF and MITRE Corporation. At NSF she established the Data and Applications Security Program and co-founded the Cyber Trust theme and was involved in inter-agency activities in data mining for counter-terrorism. She joined MITRE in 1989, worked in the Information Security Center and was later a department head in Data and Information Management as well as Chief Scientist in Data Management. She has served as an expert consultant in information security and data management to the Department of Defense, the Department of Treasury and the Intelligence Community for over 10 years. Her industry experience includes six years of research and development at Control Data Corporation and Honeywell Inc.

Dr. Thuraisingham was educated in the United Kingdom both at the University of Bristol and at the University of Wales.