UTSA®
The University of Texas at San Antonio™
COLLEGE OF BUSINESS

Center for Education and Research in Information and Infrastructure Security

Conducting high-impact research

Enhancing the security of the nation's information infrastructure

Educating the workforce needed now and in the future

Contact
Nicole Beebe, Director
(210) 458-8040
http://business.utsa.edu/ceris

Research Initiatives

Data Type Classification

Researchers at UTSA have significantly advanced the state of the art in naive statistical data type classification by using advanced machine learning techniques and training sets to perform statistical, content-based analysis to predict data type. Researchers have instantiated their baseline file type classification capability in open source software called Sceadan.

Forensic Search Hit Clustering/Ranking Algorithms

Digital forensic investigators desperately need a way to locate search hits relevant to investigative objectives more quickly. UTSA researchers comparatively evaluated four unsupervised machine learning algorithms for clustering digital forensic string search hits and adapted the winning algorithm to fit the environmental context and constraints unique to digital forensic investigations.

Insider Threat Detection

Trusted, yet malicious insiders remain a significant problem for organizations of all types. Advancement in information retrieval, digital forensics and knowledge mapping now enable us to index, analyze and map unstructured data quickly and effectively. We propose a system that maps sensitive content and topics across an organization in a knowledge map.

Bio-Inspired Threat Metrics

Researchers at UTSA propose to meld industry methods and academic research to develop a bio-inspired quantifiable digital threat metric process for use during real-time malware outbreak investigations. The researchers will view malware through the lens of food and water borne pathogenic outbreaks.

Data Analytics

Data analytics focuses on the application and research of "big data" as it pertains to cyber security and intelligence. The focus is on three main areas: (1) research advancements in data analytics that provide decision makers with improved intelligence, obtained more effectively and efficiently than currently possible; (2) improved ability to process, visualize and interact with big data from a vast virtual net of sensor, communication and Internet data through advancements in cloud-based computation and data visualization; and (3) service as a national resource for research data analysis outreach and community advancement. Functionally analytics can be divided into four areas: (1) algorithms; (2) decision making; (3) visualization; and (4) computation.

Security of Cyber Physical Systems

Researchers are focused on securing physical systems including the electrical grid and the oil industry. On-going research for the electrical grid includes vulnerability assessments of the organizations that produce electrical energy, the vulnerability of the distribution network and the vulnerability and privacy associated with smart meters. In the oil and gas industry, vulnerabilities include the process from the exploration to the refining and distribution of raw materials and refined products.

Data Compression

Informational analysis reveals Markov dependencies between coefficients in block-transformed data. These dependencies imply a hierarchical classification structure that can be used to cluster correlated information within a transform block. Because the correlations within a clustered block are Markovian, any Markov prediction scheme is appropriate for dynamically modeling cluster statistics. By supplying cluster statistics and coefficient values to an entropy encoder, the method obtains greater compression compared to traditional, ad hoc modeling and encoding methods. The hierarchical structure of the clusters also facilitates progressive encoding, wherein an entropy encoder processes cluster data down the hierarchy, from most significant to least significant. A prototype implementation losslessly compresses original JPEG media 11% to 55% further. Within the JPEG-2000 framework, the new progressive encoding method offers higher quality decoding at equivalent bit rates.