

CYBER INFORMATION ASSURANCE AND DECISION SUPPORT

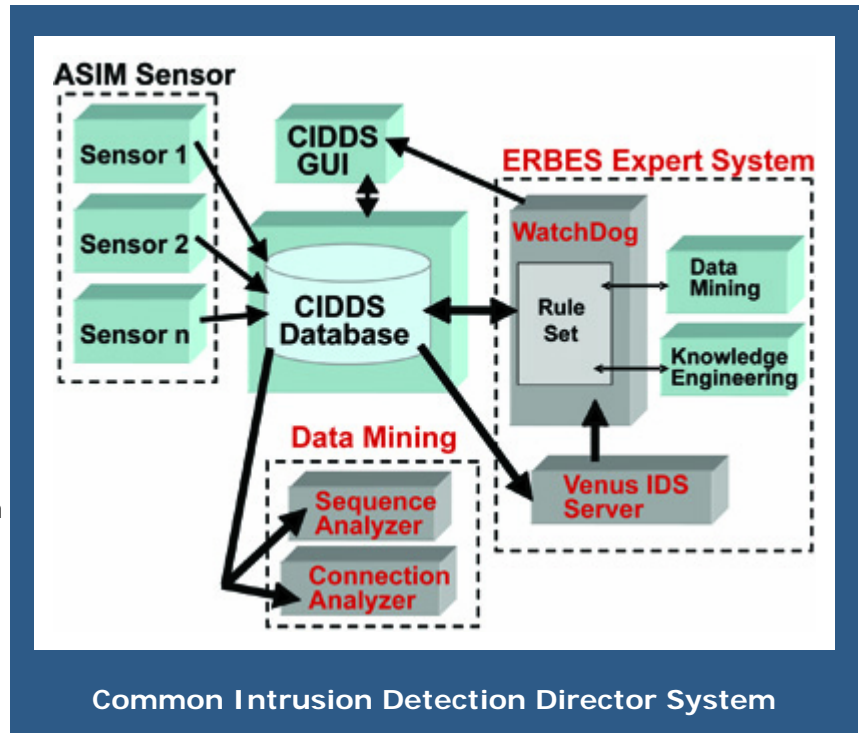
The Cyber Information Assurance and Decision Support (CIADS) team within the Information Sciences Division (ISD) has an extensive background in using and developing artificial intelligence (AI) technology for a broad range of security and decision-support applications.

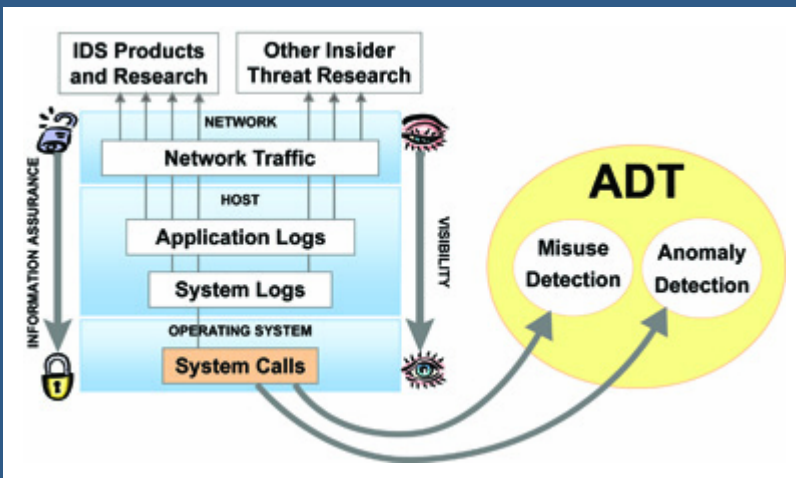
Core CIADS expertise:

- **Artificial Intelligence Technology:** Data mining, expert systems, pattern matching, and pattern recognition
- **Operating System Customization and Instrumentation:** Operating system kernel modification and monitoring, verification and validation, and custom appliance evaluation
- **Software and Systems Engineering:** Knowledge acquisition, data fusion, and software architectures
- **Automated Reasoning:** Machine learning, prediction, decision support, and content analysis
- **Agent-based Systems:** Multi-agent distributed systems, organizational adaptation, and agent-based modeling

Selected projects reflecting these areas of expertise are discussed below.

ARTIFICIAL INTELLIGENCE TECHNOLOGY FOR CYBER SECURITY. CIADS' expertise in artificial intelligence technology includes the development of the high-performance LEAPS (Lazy Evaluation Algorithm for Production Systems) expert system algorithm, which has been shown to outperform the well-known Rete algorithm in terms of speed and storage efficiency. Using the LEAPS algorithm, CIADS has developed the Enhanced Rule-Based Expert System (ERBES), which is in use by the Air Force Information Operations Center (AFIOC) as the core analytical engine of its Common Intrusion Detection Director System (CIDDS). CIDDS protects Air Force computer networks worldwide by providing decision support through data reduction, data correlation and data summarization of Automated Security Incident Measurement (ASIM) sensor data. Results are presented to human analysts who are tasked with monitoring the Air Force networks for intrusive activity. ERBES employs automated reasoning for rapid detection of correlations in large amounts of data. Extensions to ERBES have expanded its data acquisition and data fusion capabilities to include input from widely used government and commercial sensor products and freeware, including Snort, JIDS, NetRanger, ASIM, Dragon and system logs. In addition, the system uses data mining to detect attack patterns and can provide automated analysis of attacks to include severity levels, damage assessment, and recommended courses of action. CIADS has further leveraged this experience with intrusion detection and network traffic analysis to evaluate network packet inspection tools and appliances for compliance with sponsor requirements.





Security Monitoring for Insider Threat Detection

OPERATING SYSTEM INSTRUMENTATION AND MONITORING.

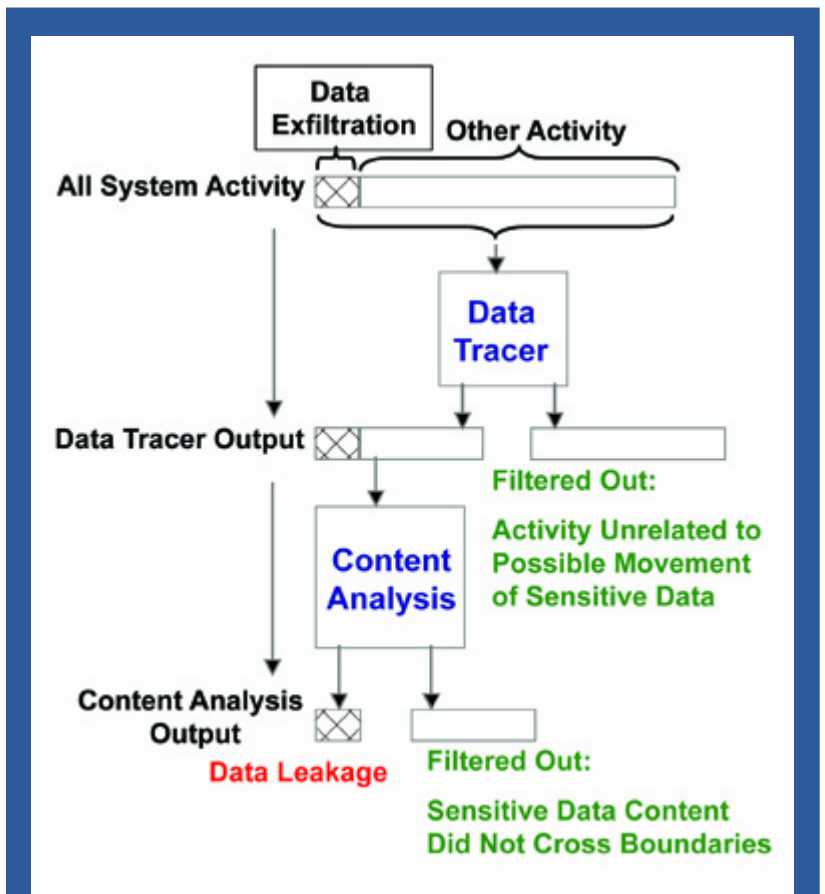
CIADS has significant experience with low-level operating system instrumentation and monitoring. Recent work for the U.S. Government's Advanced Research and Development Activity focused on classified data leakage related to the insider threat using an ARL:UT-developed software tool called Data Tracer. This tool allows an organization to determine if, when, and how digitally stored classified data has leaked. Data Tracer operates by monitoring at the operating system level to track all possible flows of classified data on a computer system. In its current implementation, Data Tracer can report when data has been released in violation

of the organization's security policy. A future implementation could, in addition, prevent these detected leaks by blocking them before they are completed. A recent extension to Data Tracer's capabilities allows monitoring of potential data leakage among virtual machines on a virtual multi-level security platform.

CONTENT ANALYSIS / INSIDER THREAT DETECTION.

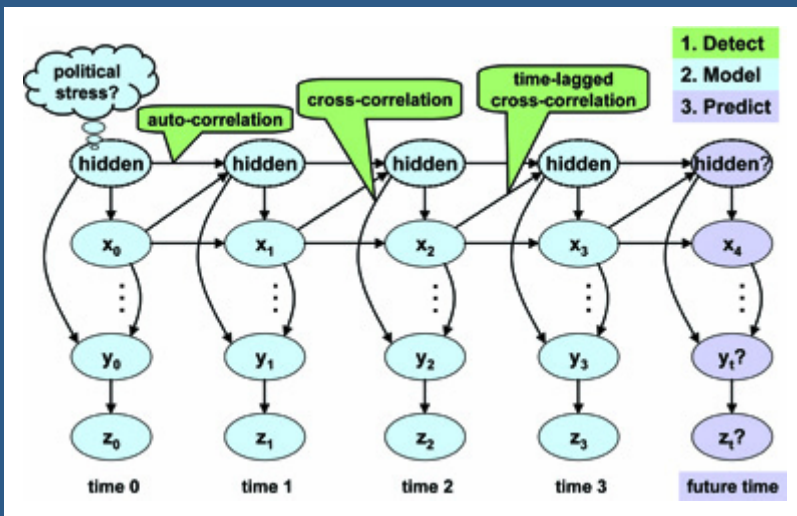
A major application area for CIADS research is content analysis for detecting leaks of classified information. Recent work performed for the intelligence community includes data mining and machine learning research for monitoring of content traversing the IT perimeter at controlled interfaces to detect indications of insider leakage of classified data.

Another application of the CIADS content analysis capabilities is the creation of a software system to analyze document text and provide automated suggestions for the security classification level (e.g., TS, S, C, or U) that should apply to that text based on known classification guidance. This software applies expert system technology, and knowledge acquisition and knowledge modeling capabilities are used to capture and interpret classification guidelines and the concepts revealed in the documents analyzed.



Content Analysis for Insider Threat Detection Using ARL:UT's Data Tracer

ATTACK PREDICTION. CIADS is investigating the use of temporal trends and attack pattern information to predict attacks such as physical terrorist attacks and many types of cyber attacks (hacking). In this research, CIADS has studied the use of Bayesian networks to combine temporal trends with correlational patterns. CIADS has performed experiments to identify specific types of temporal trends that can and cannot be modeled by existing Bayesian network research and developed a method to address these limitations.



Predicting Attacks with Dynamic Bayesian Networks

DISTRIBUTED AGENTS. CIADS' experience in development and design of distributed-agent-based systems dates to 1997. Key capabilities of these systems include dynamic organization adaptation, policy interpretation, and user support. Recent research has focused on agent modeling and automated generation of explanations for agent behavior.

For further information regarding the Cyber Information Assurance and Decision Support program, please contact: Director-SISL@arlut.utexas.edu