Intrusion Detection Systems (IDSs) and Credit Card Fraud Detection Systems With increasingly critical data being stored on computer systems, it is important to protect the computers and data from outside intrusions. Many information survival systems, such as intrusion detection systems (IDSs) and credit card fraud detection systems must be capable of detecting new and unknown patterns or anomalies. At the same time, they must be able to efficiently adapt existing models when knowledge about new patterns becomes available. Many current IDSs focus on programs on the host computer system. However, many recent network-based attacks do not involve users or system programs on the victim hosts, and thus render anomaly detection models based on user and program activities less effective.

Defense Against Newly Developed Intrusions This technology provides effective defense against newly developed intrusions while maintaining the ability to detect known intrusions. It generates an anomaly detection model for classifying activities of a computer system by using a training data set which corresponds to activity on the computer system. For a selected feature and a selected value, a quantity is determined which corresponds to the relative sparsity of such value. Once the threshold is determined, these instances are classified as an anomaly, and then added to the training set to create a new training set consisting of normal and anomalous data.

Applications:
• Intrusion detection system
  o Virus scanning
  o Spyware scanning
• Credit card fraud detection

Advantages:
• Combines multiple models for classifying anomalies for effective and accurate detection
• Reduce misidentification cost


Licensing Status: Available for Licensing and Sponsored Research Support
Inventors

Salvatore Stolfo