



# Cybersecurity Speaker Series

## Detection of Cyber Attacks Utilizing Behavioral Semantics

August 13, 2015 @ 2:00 PM

FedEx Institute of Technology Methodist Presentation Theatre

**Prof. Victor A. Skormin, SUNY-BU**

### ABSTRACT:

Cyber attacks presents a formidable threat to critical components of the national infrastructure. Modern industrial, military and government systems are run by dedicated computer networks. The end user accesses such a system not directly but through a special computer interface by defining required operational regimes, or data to be retrieved, or information to be recorded, or data to be transmitted, etc. Then it is up to the computer to provide the necessary set point values to process controllers, to sample sensors, to perform search, retrieval of the requested data, to operate printers or computer graphics, to locate available communication channels, code and transmit data, etc. Examples go far beyond power plants and rocket launchers. Banking industry, insurance, libraries, data depositories, hospitals utilize their own **dedicated** computer facilities operating in this fashion. "Dedicated" is the key word - it emphasizes that these computer facilities run only a few preapproved applications and are closed to general public. (In contrast, a university campus computer is open to general public and runs virtually any application.) Attacking dedicated computers offers a highly efficient way to render useless the processes they service and compromise stored information.

We will discuss a cyber security technology that is based on behavioral normalcy profiling and operates on the level of functionalities thus providing unambiguous representation of the goals of the particular applications. The approach reliably detects malware and non-malicious applications that are not approved for a particular computer system. A fully operational system prototype enhanced by advanced visualization will be demonstrated. Several important applications of the approach will be discussed.

### BIOSKETCH:

**Dr. Victor A. Skormin** is a Professor of Electrical and Computer Engineering at Binghamton University (State University of New York - SUNY), Binghamton NY. He has a MS (1968) degree from the Kazakh Polytechnic Institute, Alma-Ata, U.S.S.R, and a Ph.D. (1974) degree from the Institute of Steel and Alloys, Moscow, U.S.S.R. While at Binghamton, he established a control engineering curriculum, a laboratory for laser communication research, pioneered computer network security research at Binghamton, and established and directed the Center for Advanced Information Technologies. He received the SUNY Chancellor's Awards for Excellence in Teaching and for Excellence in Research, the IEEE Award "For Leadership in Establishing University Industry Links...", and the rank of Distinguished Service Professor.

Dr. Skormin's research in the areas of technical diagnostics, laser communications, and computer network security has been supported by the National Science Foundation, NASA and the Air Force. He served as a consultant to Eastman Kodak, General Electric, Corning Glass Works, Martin Marietta, Universal Instruments and the Air Force Research Laboratory. Twice in his career Dr. Skormin has been appointed by the National Research Council as an Air Force Senior Research Associate. Since 2001 he is an organizer of the on-going bi-annual International conference "Mathematical Methods, Models and Architectures for Computer Networks Security" in St. Petersburg, Russia (sponsored by the US Air Force and Navy). He is a Honorary Professor of the Kazakh National Technical University, Almaty, Kazakhstan, and an International Member of the Russian Academy of Navigation and Motion Control Sciences.

Dr. Skormin is an author/editor of several books and a large number of research papers; he supervised 23 PhD dissertation, and served as an Editor for Space Systems of the IEEE AES Transactions. He is a Life Senior Member of IEEE.