



Transition

SBIR Topic Number:
AF03-94

Title:
Netwar

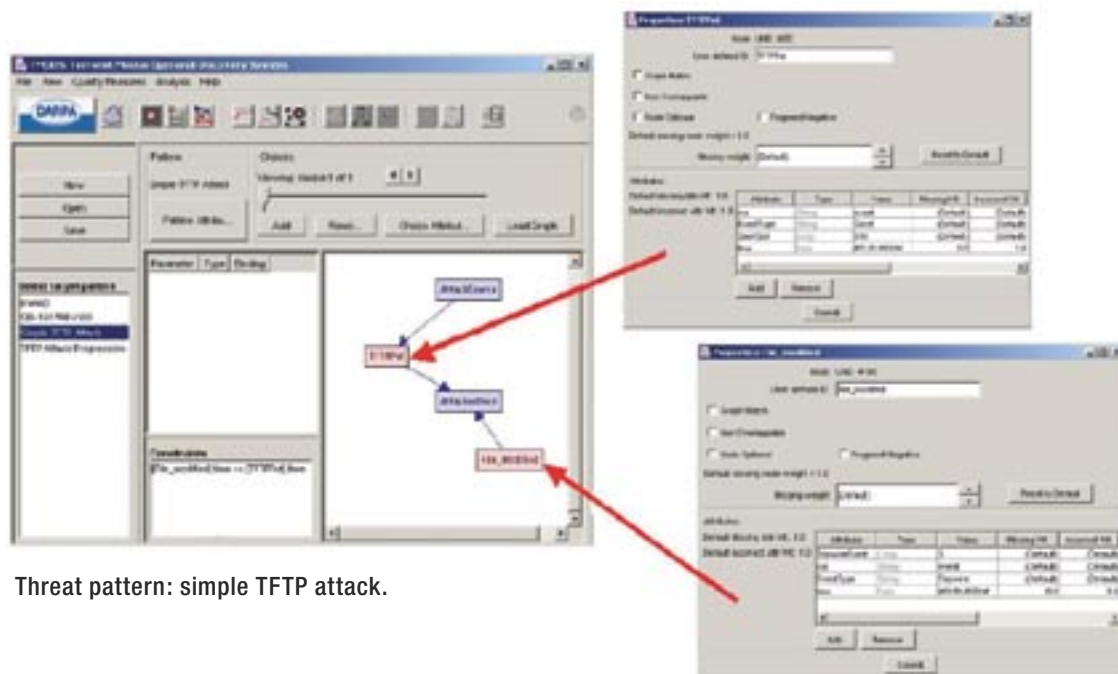
Contract Number:
F30602-03-C-0129 and
F30602-99-C-0020

Company Name:
21st Century
Technologies Inc.,
Austin, TX

Technical Project Office:
AFRL Information
Directorate

Transition Office:
Air Force Information
Warfare Center (AFIWC),
US Army INSCOM and
the Department of
Homeland Security

An example of Air Force supported SBIR technology that has been transitioned into an Air Force or other DoD system or subsystem or used by Air Force test ranges and facilities or maintenance depots.



Threat pattern: simple TFTP attack.

Intrusion Detection and Threat Prediction System to Counter Computer Attacks

- The number of attacks against Air Force computer systems is estimated to be doubling every year.
- Computer attacks demonstrate clear patterns. These patterns can be graphically represented. The Air Force required graph matching and network analysis tools to detect attacks.
- SBIR supported development of technology called Netwar, a powerful intrusion detection and threat prediction system. Currently being validated, Netwar is to be transitioned to elements of the Air Force Information Warfare Center (AFIWC).

A

DISTRIBUTION A:
Approved for public
release; distribution
unlimited.

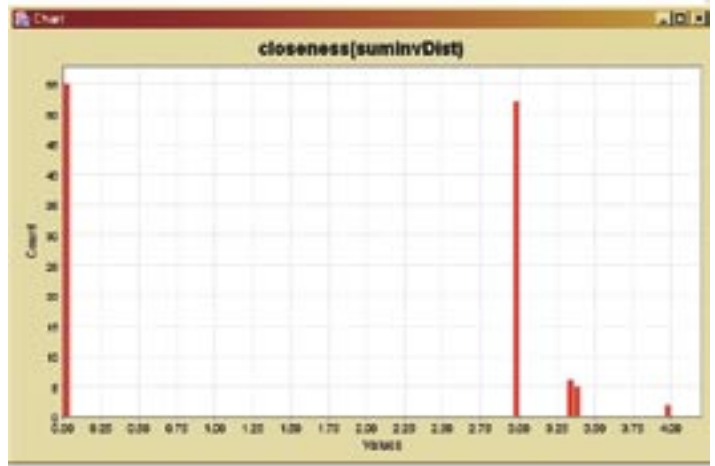
Air Force Requirements

It is essential to protect the United States' strategic advantage in information dominance. In 2002, the Air Force Computer Emergency Response Team (AFCERT) estimated that over 4.4 billion suspicious connections occurred against Air Force computer systems. Of those, more than 60% of the activity initiated from a foreign location. It is estimated that the number of such attacks is approximately doubling every year. These attacks, when successful, directly impact the security and flow of network communications and information that is vital to the execution of day to day military operations. The seriousness of the situation has prompted the US Air Force Institute of Technology to hold Cyber Defense Exercises. As part of their education in modern, network-centric warfare, officers' drill by defending networks and servers against attacks from a "red team" of hackers.

Computer network topology is natively represented as a graph. Intrusions and attacks – whether they are insider or outsider generated, individual or coordinated attacks – have clear 'pattern graph' representations that can be exploited entirely on structural properties. The Air Force requires powerful graph matching and social network analysis tools that can detect anomalous pattern graphs and associated social networks to help prevent attacks on network communications.

SBIR Technology

Using Air Force SBIR Phase I and II contracts, 21st Century Technologies, Inc. worked with the Air Force to develop a unique product called Netwar to detect anomalous network activity. Netwar technology uses graph representations, graph matching and social network analysis algorithms enabling the development of extremely powerful intrusion detection and threat prediction systems.



Social Network Analysis results increases likelihood of actual attack.

Air Force Transition Payoff

Under the Phase II SBIR, 21st Century Technologies is working with AFRL's Rome Laboratory to demonstrate how Netwar technology can improve the accuracy and precision over current IDS systems presently used at the Air Force Information Warfare Center (AFIWC). Using a testbed of network data, Rome Lab is simulating network operations occurring at AFIWC. Based on initial estimates Rome Lab anticipates an improvement in threat detection accuracy of 50% and an improvement of precision of 75%. Once this technology has been validated, Netwar technology will be transitioned for insertion within AFIWC elements at the Air Intelligence Agency.

Company Impact

In addition to the planned deployment at the Air Intelligence Agency for advanced intrusion detection, Netwar technology has or is also being considered for insertion in other federal agency network systems. Total revenue related to the Netwar effort is expected to exceed three million dollars.



U.S. AIR FORCE

SBIR

AF SBIR Program Manager
AFRL/XPTT
1864 4th Street,
Room 1, Building 15
Wright-Patterson AFB, OH 45433

AF SBIR Program Manager: Steve Guilfoos
e-mail: stephen.guilfoos@wpafb.af.mil
Website: www.sbirstrmall.com

DSN Fax: 785-2329
T: (800) 222-0336
F: (937) 255-2329

**Air Force
Research Laboratory | AFRL**
Science and Technology for Tomorrow's Aerospace Force