

Innovation

This Air Force SBIR/STTR Innovation Story is an example of Air Force supported SBIR/STTR technology that met topic requirements and has outstanding potential for Air Force and DoD.

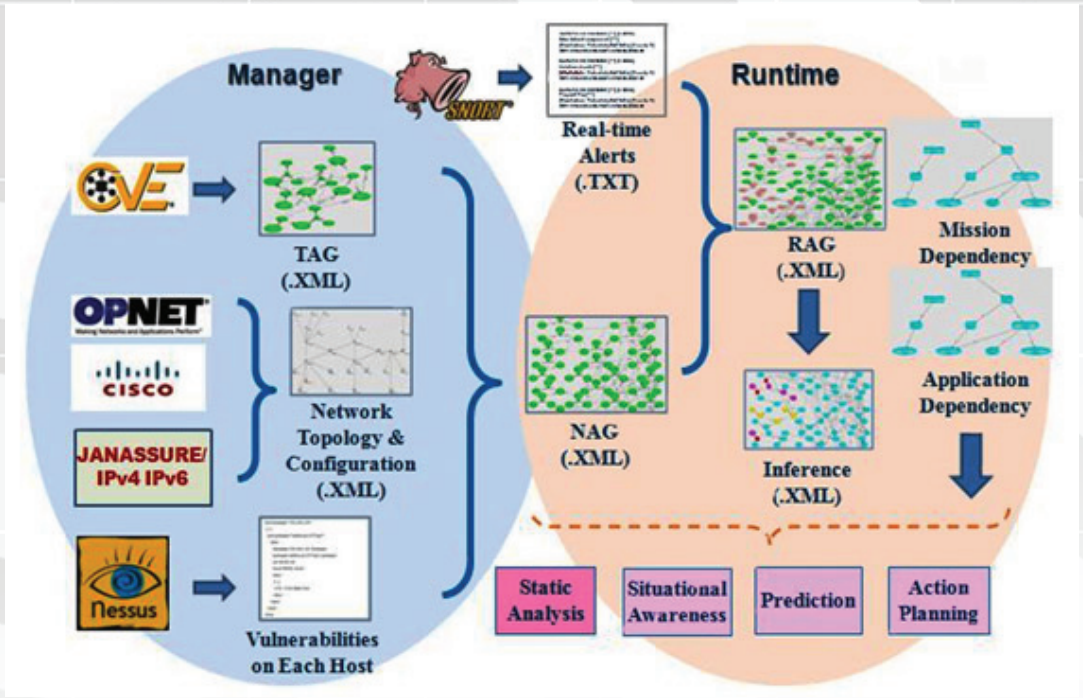
SBIR Topic Number:
AF071-080

SBIR Title:
Network Attack Damage Assessment

Contract Number:
FA8750-08-C-0137

SBIR Company Name:
Intelligent Automation, Inc., Rockville, MD

Technical Project Office:
AFRL Information Directorate, Rome, NY



NIRVANA Architecture

Integrated Graphical Models for Efficient and Practical Network Attack Damage Assessment

- Air Force requires technologies to determine network, mission, and operational impacts resulting from successful adversary cyber attacks, including real-time, automated damage assessment
- Intelligent Automation, Inc. (IAI) developed the Network Intrusion, Risk and Vulnerability Analysis (NIRVANA) software tool to provide a comprehensive cyber security analysis capability
- NIRVANA identifies network vulnerabilities, consequences of actions, and probable targets allowing operators to counter with near-real-time actions, effectively denying the attacker's goals
- The NIRVANA tool is applicable to virtually all enterprise networks—military and commercial alike—establishing IAI as a major player in the emerging cyber security market

20110517

A

DISTRIBUTION A:
Approved for public
release; distribution
unlimited.

Air Force Requirement

The Air Force requires technologies to determine network, operational, and mission impacts resulting from successful adversary cyber attacks. Real-time, automated damage assessment capabilities are required to assist cyber security analysts in finding the root cause of a cyber attack, to accurately find damaged network and system components, to contain the spread of malicious code, to quarantine damage, and to produce courses-of-action that provide continuity-of-operations for critical network and information enterprise functions. The scale of current enterprise networks, the multiple kinds and patches of operating systems and applications, and the overall complexity of enterprise networks, produces an overwhelming complex environment that helps obscure the cyber attacker's presence and actions. One of the key challenges in cyber security is not only to identify what was penetrated by the attacker, but also what he can do with it, and which systems and capabilities are compromised. Another important aspect is to assess the impact that the remedies proposed will have on the capabilities required to support the missions. State-sponsored and multi-prong attacks, as shown on the right, may create diversions that consume and distract personnel manpower, while the cyber attacker's actual objective is carefully obscured.

SBIR Technology

Intelligent Automation, Inc. (IAI) developed their Network Intrusion, Risk and Vulnerability Analysis (NIRVANA) software tool under this SBIR project to provide a comprehensive cyber security analysis capability. It uses data from multiple intrusion detection systems to produce a comprehensive situation awareness picture, including a static evaluation of network vulnerabilities, as shown here.



In this tool, network vulnerabilities are identified using the novel attack graphs, developed under a previous Army

SBIR program, associated with applications and mission requirements, allowing the tool to identify the consequences of actions. The technology developed can also estimate the probable targets intended by the attacker, allowing operators to counter with near-real-time actions, effectively denying the attacker's goals. The technique is designed to scale, allowing for coordination of multiple security domains, and several runtime operators. A video describing NIRVANA's key features and capabilities is available on IAI's website ([click link](#)).

Potential Air Force Application

Using this tool, the Air Force, DoD, and other large enterprises have the first comprehensive capability to visualize the implications of a cyber attack. Operators will be able to anticipate the actions of attackers, even when a slow-brewed or multi-prong attack, as shown here, is in progress.



The ability to anticipate and adjust in order to maintain mission readiness during the attack, although present in IAI's cyber security strategy, is a missing component of our current cyber deterrence arsenal. This NIRVANA technology is the first to provide coherent enterprise-wide network cyber attack damage assessment.

Company Impact

Cyber security analysis represents an emerging market, which is still very open for innovators. The development of IAI's NIRVANA tool, which is applicable to virtually all enterprise networks—both military and commercial alike-- has helped establish IAI as a major player in this market with innovative ideas and unique capabilities. The presentation of this technology, and others still under development, has already helped establish important transition partnerships in the cyber security area.



SBIR/STTR

Air Force SBIR Program
AFRL/XP
1864 4th Street
Wright-Patterson AFB OH 45433

AF SBIR/STTR Program
Manager: Augustine Vu
Website: www.afsbirstr.com
Comm: (800) 222-0336
Fax: (937) 255-2219
e-mail: afrl.xppn.dl.sbir.hq@wpafb.af.mil

