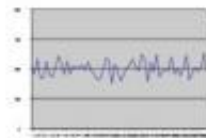# YIP research leads to new security algorithms

October 22 2010

Young Investigator Research Program computer scientists are making large strides in developing new tools and techniques to reverse-engineer data-hiding algorithms from watermark detectors, which once commercialized and deployed, will improve the security of the GlobalInformation Grid of the Air Force computer networks. Credit: Graphic by Craver, Binghamton University

The Air Force Office of Scientific Research's Young Investigator Research Program is enabling new scientists and engineers with exceptional ability to do creative basic research, enhance their career development and develop tools and techniques.

The current researchers are using the program with algorithms to improve the security of the Global information Grid of the Air Force computer networks.

"The YIP program is also significant because it allows program managers to have even more freedom in selecting researchers like AFOSR-supported scientists, Dr. Scott Craver of Binghamton University and Dr. Yan Chen of Northwestern University," said Dr. Robert Herklotz, AFOSR program manager.

Craver and Chen worked on two separate projects involving detection and evasion algorithms that when implemented will prove to be cutting-edge.

"The new technology will not only accurately block the known existing attacks, but will also defeat future possible attacks on networks, including wireless ones," said Dr. Yan Chen who accomplished his research goals by designing state-of-the-art algorithms, implementing them in prototype and evaluating them thoroughly. He will complete his YIP grant in November 2010.

Craver and his researchers who recently completed their YIP grant already, investigated reverse-engineering, detection and detection evasion algorithms.

"Our videoconferencing work requires that we tamper with existing software, a task that involves programming in multiple languages on multiple levels," said Craver. "On top of that we had to author entertaining computer animations for use as special effects and for our self-destructing e-mail project, we amended video signals."

Rather than waiting for attackers to define their method of defense, the researchers took a proactive approach. They searched and then found potential vulnerabilities in the emerging wireless network protocols and ultimately devised the cutting-edge algorithms.

"Our project generated the first network-based intrusion detection and

prevention system that is both highly accurate and fast, up to tens of gigabits per second," said Chen.

"There are many security problems in which one party attempts to detect unauthorized behavior by another party; in response an attacker tries to find strategies for evading a detector by adapting to its [algorithm](,)" he said. "Our primary area of focus is the detection of a secret watermark concealed in an image or video clip."

Craver and his co-researchers discovered their largest challenge is the lack of a strong mathematical foundation for detection and evasion algorithms.

However, under the three year long YIP [program](,), they have been working to put adversarial detection challenges on a strong mathematical foundation that will allow them to be confident about the security of future detection algorithms.

"Our vision is to significantly improve the current network defense technology, not only against the existing known attacks, but also for unknown attacks, while still being able to match the high-speed network environment," said Chen.

Provided by Air Force Office of Scientific Research