

Cyber security team creates winning network security product

May 11 2011

A team from the Virginia Tech Information Technology Security Laboratory and Bradley Department of Electrical and Computer Engineering won third place in the 2011 National Security Innovation Competition sponsored by the National Homeland Defense Foundation, a nonprofit forum for responding to terrorism tactics and natural disasters.

The Virginia Tech product, the Moving Target IPv6 Defense (MT6D), is an innovative network [security](#) and privacy tool for the new Internet Protocol version 6 (IPv6), an Internet address system that will replace the 20-year-old Internet Protocol version 4 (IPv4). Virginia Tech runs one of the few production scale IPv6 networks in the country, supporting the campus network of more than 30,000 computing and communication systems.

"MT6D provides a means for hosts to communicate with each other over the public Internet while maintaining complete anonymity from targeting, tracking, and traffic correlation," said Stephen Groat of Alexandria, Va., a Ph.D. student in computer engineering.

"We have leveraged IPv6 and the advanced Virginia Tech infrastructure to develop a product that will protect the networks of tomorrow," said William Urbanski, security analyst with the Virginia Tech IT Security Office.

According to Urbanski, MT6D dynamically obscures network and

transport layer addresses of data packets to achieve anonymity, including authentication privacy. It also protects against certain classes of network attacks. "That means that MT6D makes it nearly impossible to observe, track, or interfere with the conversation taking place between two computers on an IPv6 network," he said.

"The goal of our research is to protect sensitive communications commonly used by government agencies from eavesdroppers or social engineers," said Randy Marchany, Virginia Tech chief information security officer and one of the inventors. Many communications require messages to be authenticated. "The problem with message authentication is that a third party can use the identity tied to the authenticated message to track a sender," said Marchany.

MT6D differs from other dynamic obscuration techniques by combining network security with anonymity, according to Matthew Dunlop of Depoe Bay, Ore., a Ph.D. student in computer engineering. "It can be implemented embedded on a device or as a network gateway requiring negligible configuration, and is therefore transparent to hosts. MT6D has many applications including mobile devices, the smart grid, and industrial control systems (SCADA)."

"We were pleased to compete in this prestigious event and are highly honored to be placed third among the well-regarded competitors we faced. The true winners in this competition are those who are better-protected by the innovations that evolve from all of the participants' research," said Joe Tront, the W.S. "Pete" White Chair for Innovation in Engineering Education and professor of electrical and computer engineering.

The competition brought together experts from industry, academia, and government to present and review projects that address national security challenges. Universities from across the U.S. and Canada first competed

in the written submission phase from which 10 finalists were chosen. Finalists were invited to present their work to a judging team of renowned experts at this year's host institution, the U.S. Air Force Academy.

"Contest entries were judged on both technical merit and commercial potential," said John Geikler, senior licensing associate with Virginia Tech Intellectual Properties Inc., which is licensing the technology. Inventors Groat, Dunlop, Urbanski, Marchany, and Tront have filed a preliminary patent and are in the process securing the full patent.

The National Homeland Defense Foundation announced that the first place winner was the University of Ottawa for a blast strengthening of wood structures. Second place was the University of Notre Dame for eye recognition that includes dilation.

Provided by Virginia Polytechnic Institute and State University

Citation: Cyber security team creates winning network security product (2011, May 11) retrieved 20 April 2024 from <https://phys.org/news/2011-05-cyber-team-network-product.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.