

TRACK: InfraGard Track / Cyber-crime, terrorism, and information warfare
SESSION #: ITCT#9
DATE: Tuesday April 20, 2010
TIME: 2:55-4:10pm
SESSION TITLE: "Building a Resilient Homeland Network and Protecting Critical Cyber Infrastructure with Deep Packet Inspection"
SPEAKER(S): Joel Ebrahimi – Solutions Engineer
ORGANIZATION: Bivio Networks

ABSTRACT: "Building a Resilient Homeland Network and Protecting Critical Cyber Infrastructure with Deep Packet Inspection"

An ever more interactive Web environment has spawned a new era of communication and information sharing capabilities. Unfortunately, this environment is also host to a new generation of sophisticated cybersecurity threats and a conduit for criminal activity. Simple e-mail communication, for instance, can now be used to facilitate a host of illicit activities, ranging from insider trading to terrorist acts.

Now more than ever, government agencies have a need to fully understand and manage who is on the network, what users are doing and the resources to which they have access.

With the creation of the Comprehensive National Cybersecurity Initiative (CNCI) — a multi-year, multi-billion dollar project mandating a proactive approach to securing government computer systems against foreign and domestic threats — agencies are cracking down on cyber terrorism.

It is not enough simply to respond to cyber threats. Agencies tasked with preventing them or making the U.S. more resilient against them must get ahead of the curve by creating a policy-centric network that effectively identifies and neutralizes potentially malicious threats before they have the chance to inflict harm. The challenge has been — and continues to be — how best to reconcile effective network security policy with the goal of deploying a secure common communications platform that supports information sharing within and between agencies.

One powerful tool at the government's disposal — deep packet inspection (DPI) — gives federal agencies unprecedented "visibility" into deeper levels of network traffic. By enabling the examination of a data packet's entire payload, DPI allows network managers to identify and remedy security vulnerabilities without stifling network speed or performance. What is more, federal agencies can deploy DPI-enabled applications on one common programmable platform to contain costs, limit space requirements and cut energy consumption.

The audience will learn the fundamentals of DPI, as well as how the technology will be a primary component of agency efforts to meet and satisfy the CNCI mandate. The presentation will feature a case study on the use of DPI technology by the Defense Information Systems Agency (DISA).

SPEAKER BIO(S): Joel Ebrahimi is a solutions engineer at Bivio Networks, where he helps service providers, carriers and government organizations deploy DPI-enabled systems for improved network security, visibility, control and monetization. He holds a bachelor's in computer science from the University of California, Santa Barbara.