7555-01-P

NATIONAL SCIENCE FOUNDATION

Assumption Buster Workshop: Defense-in-Depth is a Smart Investment for Cyber Security

AGENCY: The National Coordination Office (NCO) for the Networking and Information Technology Research and Development (NITRD) Program.

ACTION: Call for participation

FOR FURTHER INFORMATION, CONTACT:

assumptionbusters@nitrd.gov

DATES: WORKSHOP: March 22, 2011; **DEADLINE:** February 10, 2011. Apply via e-mail to assumptionbusters@nitrd.gov Travel expenses will be paid for selected participants who live more than 50 miles from Washington DC, up to the limits established by Federal Government travel regulations and restrictions.

SUMMARY: The NCO, on behalf of the Special Cyber Operations Research and Engineering (SCORE) Committee, an interagency working group that coordinates cyber security research activities in support of national security systems, is seeking expert participants in a day-long workshop on the pros and cons of the defense-in-depth strategy for cyber security. The workshop will be held March 22, 2011 in the Washington DC area. Applications will be accepted until

5:00PM EST February 10, 2011. Accepted participants will be notified by February 28, 2011.

SUPPLEMENTARY INFORMATION:

Overview: This notice is issued by the National Coordination Office for the Networking and Information Technology Research and Development (NITRD) Program on behalf of the SCORE Committee.

Background:

There is a strong and often repeated call for research to provide novel cyber security solutions. The rhetoric of this call is to elicit new solutions that are radically different from existing solutions. Continuing research that achieves only incremental improvements is a losing proposition. We are lagging behind and need technological leaps to get, and keep, ahead of adversaries who are themselves rapidly improving attack technology. To answer this call, we must examine the key assumptions that underlie current security architectures. Challenging those assumptions both opens up the possibilities for novel solutions that are rooted in a fundamentally different understanding of the problem and provides an even stronger basis for moving forward on those assumptions that are well-founded. The SCORE Committee is conducting a series of four workshops to begin the assumption buster process. The

assumptions that underlie this series are that cyber space is an adversarial domain, that the adversary is tenacious, clever, and capable, and that re-examining cyber security solutions in the context of these assumptions will result in key insights that will lead to the novel solutions we desperately need. To ensure that our discussion has the requisite adversarial flavor, we are inviting researchers who develop solutions of the type under discussion, and researchers who exploit these solutions. The goal is to engage in robust debate of topics generally believed to be true to determine to what extent that claim is warranted. The adversarial nature of these debates is meant to ensure the threat environment is reflected in the discussion in order to elicit innovative research concepts that will have a greater chance of having a sustained positive impact on our cyber security posture.

The first topic to be explored in this series is "Defense-in-depth is a Smart Investment." The workshop on this topic will be held in the Washington DC area on March 22, 2011.

Assertion: "Defense-in-Depth is a smart investment because it provides an environment in which we can safely and

securely conduct computing functions and achieve mission success."

This assertion reflects a commonly held viewpoint that Defense-in-Depth is a smart investment for achieving perfect safety/security in computing. To analyze this statement we must look at it from two perspectives. First, we need to determine how the cyber security community developed confidence in Defense-in-Depth despite mounting evidence of its limitations, and second, we must look at the mechanisms in place to evaluate the cost/benefit of implementing Defense-in-Depth that layers mechanisms of uncertain effectiveness.

Initially developed by the military for perimeter protection, Defense-in-Depth was adopted by the National Security Agency (NSA) for main-frame computer system protection. The Defense-in-Depth strategy was designed to provide multiple layers of security mechanisms focusing on people, technology, and operations (including physical security) in order to achieve robust information assurance (IA).[1] Today's highly networked computing environments, however, have significantly changed the cyber security calculus, and Defense-in-Depth has struggled to keep pace

[1] *Defense-in-depth: A practical strategy for achieving Information Assurance in today's highly networked environments.*

with change. Over time, it became evident that Defense-in-depth failed to provide information assurance against all but the most elementary threats, in the process putting at risk mission essential functions. The 2009 White House Cyberspace Policy Review called for "changes in technology" to protect cyberspace, and the 2010 DHS DOD MOA sought to "aid in preventing, detecting, mitigating and recovering from the effects of an attack", suggesting a new dimension for Defense-in-depth along the lifecycle of an attack.

Defense-in-Depth can provide robust information assurance properties if implemented along multiple dimensions; however, we must consider whether layers of sometimes ineffective defense tools may result in *delaying* potential compromise without providing any guarantee that compromise will be completely *prevented*. In today's highly networked world, Defense-in-Depth may best be viewed as a practical way to defer harm rather than a means to security. It is worth considering whether the Defense-in-Depth strategy tends to contribute more to network *survivability* than it does to mission assurance.

Intrusions into DoD and other information systems over the past decade provide ample evidence that Defense-in-Depth provides no significant barrier to sophisticated,

motivated, and determined adversaries given those adversaries can structure their attacks to pass through all the layers of defensive measures. In the meantime, kinetic Defense-in-Depth of weapons platforms (such as aircraft) evolved into a life-cycle strategy of stealth (prevent), radars (detect), jammers and chaff (mitigate), fire extinguishers (survive) and parachutes (recover), a strategy that could provide value in the cyber domain.

How to Apply

If you would like to participate in this workshop, please submit 1) a resume or curriculum vita of no more than two pages which highlights your expertise in this area and 2) a one-page paper stating you opinion of the assertion and outlining your key thoughts on the topic. The workshop will accommodate no more than 60 participants, so these brief documents need to make a compelling case for your participation. Applications should be submitted to assumptionbusters@nitrd.gov no later than 5:00 PM EST on February 10, 2011.

Selection and Notification:

The SCORE committee will select an expert group that reflects a broad range of opinions on the assertion.

Accepted participants will be notified by e-mail no later than February 28, 2011. We cannot guarantee that we will contact individuals who are not selected, though we will attempt to do so unless the volume of responses is overwhelming.

Submitted by the National Science Foundation for the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) on February 2, 2011.

Suzanne H. Plimpton,
Reports Clearance Officer,
National Science Foundation.

[FR Doc. 2011-2580 Filed 02/04/2011 at 8:45 am; Publication Date: 02/07/2011]