

SAST

Closest thing to reality without being there

- ▶ One tool suite, many security applications
- ▶ User autonomy
- ▶ Scalable
- ▶ Interoperable among computational environments
- ▶ Software/hardware independence
- ▶ Rapid experience building



SAST

(Security Assessment Simulation Toolkit)

Anyone who depends on computers, networks, or digital devices faces increased risk through vulnerabilities that can substantially impact if not disrupt their mission. These can include hardware, software and network attacks by adversaries or catastrophic failures.

VULNERABILITY RISK FACTORS INCLUDE:

- ▶ *increased sophistication of stealthy attacks*
- ▶ *rapidly changing threats*
- ▶ *insufficient numbers of highly qualified, security personnel*
- ▶ *lack of adequate capabilities to measure security performance*
- ▶ *substantial pressures to reduce security costs while improving performance*
- ▶ *uncertainty of vulnerabilities.*

OPPORTUNITY

The Security Assessment Simulation Toolkit (SAST) offers a suite of simulation tools directly applicable to cyber security training, exercises, testing, evaluation, information assurance and information operations.

Figure 1 depicts many of the applications possible, along with the core SAST components that make it a reality.



Figure 1. Foundational Capability

As a training tool, security personnel can use SAST directly via a network range to rapidly build experience in cyber security augmenting traditional training programs. SAST allows you to train as you operate, or in the case of DoD, train as you fight. It is valuable to refresh security skills at the user's convenience and rapidly update skills when new exploits emerge.

MUTT and CAT, each components of SAST, provide network traffic flows with far greater realism than exists through any other means for exercising cyber security defenses. Furthermore, they enable the effective use of network ranges for many critical security applications. SAST scales from exercising small units up to large, multiple organizations at the national level.

For testing and evaluation, SAST makes possible the ability to measure the individual or collective performance of cyber security tools or personnel. Such capability affords great value when evaluating the effectiveness of one's own defensive posture; when adopting new methods or evaluating new tools to determine their collective effectiveness.

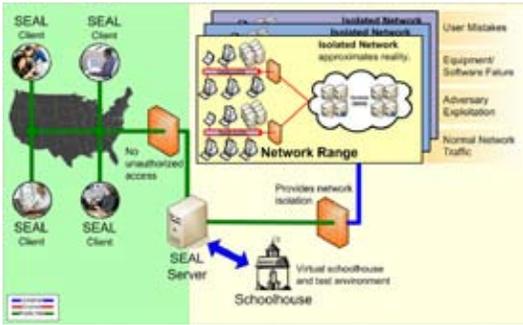


Figure 2. SAST Concept

Fundamental principals of SAST include:

- ▶ full user autonomy for tool use
- ▶ performance measurement
- ▶ scalability from a few computers to a massive network
- ▶ virtual equipment (eg: computers)
- ▶ virtual people
- ▶ interoperability across many computational platforms and networks

The fundamental SAST concept [Figure 2] for all applications involves the use of the SAST core capabilities (MUTT, CAT, SEAL) [Figure 1] in conjunction with a network range [Figure 2]. The network range approximates reality through the use of real computers, networks, switches, firewalls, synthetic people, and exploits. Essentially the SAST software virtualizes the user community by synthesizing peoples' behavior to generate the associated traffic and subsequently allows for a level of interaction not possible with other technologies. SEAL, via its clients, makes access to the SAST range possible anywhere in the world. A brief description of the major SAST components follows:

Multi-user Traffic Tool (MUTT): offers the capability to model the actual behavior of the population of network users and organizations individually or collectively to any level of fidelity desired by the user. It can simulate scenario-based schedules and timeframes. From the model, MUTT automatically generates



complete session network traffic from any one or more computers in the network range up through total network saturation.

Coordinated Attack Tool (CAT): offers the capability to directly insert malicious



exploits into the network and computational environment as well as user and equipment failures or errors. CAT automates most of this process while allowing operator intervention.

Secure Environment For Accelerated Learning (SEAL):



offers the capability to remotely access the SAST simulation environment from any where Internet or network services exist, along with the ability to customize views in the network range depending on the roles a user plays. Furthermore, a user can obtain a multi-dimensional view of a cyber attack via SEAL.

AVAILABILITY

SAST or any of its components are available license-free in the form of a 4-CD set to government agencies. Live demonstrations of SAST are available at Pacific Northwest National Laboratory

(PNNL). New features are currently in development and will become available through semi-annual software releases.



SPONSORS

The Department of Defense (DoD), Technical Support Working Group (TSWG); Defense-wide Information Assurance Program (DIAP); Office of Naval Research (ONR); National Center for Advanced Secure Systems Research (NCASSR); Defense Information Systems Agency (DISA); and the Department of Energy (DOE) sponsored the research that makes the SAST capability possible.

Any government organization can directly leverage these substantial investments or choose to move this technology forward should they have unique requirements to defend the integrity of their computer and network systems. The SAST program shares the outcomes of its research and resulting products with all of the SAST partners.

To receive the benefits of becoming a SAST partner and learn more about how your organization can become a part of this team, please contact the individual listed below who will be happy to assist you.

ABOUT PNNL

Pacific Northwest National Laboratory is a Department of Energy Office of Science national laboratory where interdisciplinary teams advance science and technology and deliver solutions to America's most intractable problems in energy, national security, and the environment. PNNL employs 4,000 staff, has a \$855 million annual budget, and has been managed by Ohio-based Battelle since the Lab's inception in 1965.

For more information contact:

Wayne Meitzler
 Cyber Security R&D Program Manager
 Pacific Northwest National Laboratory
 P.O. Box 999, MSIN K8-41
 Richland, Washington 99354
 Phone: (509) 375-3718
 Secure Phone: (509) 372-6815
 Fax: (509) 375-6644
 wayne.meitzler@pnl.gov
 SIPR: wayne.meitzler@pnnl.doe.sgov.gov
www.pnl.gov



Pacific Northwest
 NATIONAL LABORATORY