Sandia National Laboratories

Information Design Assurance Red Team™

IDART™ is a multi-disciplinary assessment team working to improve the security of critical systems through systematic analysis using an adversary perspective. The team uses its own IDART red team assessment methods to help program and project managers make good decisions with reliable and actionable results, using a repeatable process.

Sandia National Laboratories retains a wide range of security expertise in a variety of operational contexts; this subject matter expertise is integrated into IDART assessments to assist in the characterization and analysis of target systems. The IDART methodology, which includes a spectrum of viewpoints and adversary models, is applicable to components, devices, networks, infrastructures, and world-wide enterprises.

In addition to assessment methodologies, IDART is working to develop new approaches for information assurance metrics, and tools for analyzing the security robustness of information systems contributing to our national security. IDART performs focused assessments in partnership with system stakeholders and include such tasks as:

- Identify nightmare consequences,
- Characterize target systems,
- Identify potential vulnerabilities whose exploitation will result in nightmare consequences, and
- Provide prioritized mitigation strategies so owners can make informed choices

IDART's red teaming methodology has been applied to a broad range of complex computer networks, systems, and applications; it also supports advanced analyses of CBRNE threats. IDART especially seeks to analyze systems and security technologies in design and development so that vulnerabilities can be addressed prior to deployment. Its goal is to implement repeatable assessments with measurable results that can be used to make improvements and evaluate progress.

IDART™
Information Design Assurance Red Team

Adversary models include a spectrum of outsider and insider threats characterized by both measurable capabilities, such as knowledge, access, and resources as well as intangibles such as risk tolerance and motivation. These models are used to screen attack possibilities and assist in threat-based prioritization of protection strategies. The principal advantage of these models is an adversary perspective that yields a view of information systems different from that of defenders and yields critical insights into the security of critical systems.

IDART occasionally provides red team assessment training to qualified groups on a case-by-case basis.

Part of the Information Systems Analysis Center at Sandia, IDART works closely with other groups performing Information Assurance activities including those providing cryptographic analysis, secure hardware and networks, and process control system security.

For more information contact:
Raymond Parks
Sandia National Laboratories
P.O. Box 5800 MS 0671
Albuquerque, NM 87185-0671
phone: (505) 844-4024
e-mail: rcparks@sandia.gov
http://www.idart.sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND# 2008-1348P

National Nuclear Security Administration

Sandia National Laboratories