DHS Science and Technology Directorate

Defense Experimental Research Testbed

Cybersecurity practitioners require risk-free research infrastructure

Providing appropriate security in cyberspace requires developing tools to test firewalls and anti-virus software and other measures designed to protect our nation's critical infrastructure. Creating and testing such tools on operational networks or live on the Internet presents tremendous risks, such as increasing the vulnerability of systems requiring protection or indicating to adversaries the intention to build safeguards against their infiltration.

To test whether a solution really works, it is critical that it is safely tested at scale. Far too often approaches are developed in small, contrived environments where they are never tested realistically, and then they under-deliver or fail when deployed. Consequently, the results of many experiments run on small models are unreliable indicators of the value of the tools or processes tested there.

Testing without risk

The Defense Experimental Research (DETER) testbed project enables cybersecurity researchers to run experiments on a secure "virtual Internet." The testbed provides contained environments that allow researchers to safely test advanced defense mechanisms against "live" threats without endangering other research or the larger Internet. The project was originally jointly funded by the Department of Homeland Security (DHS), Science and Technology Directorate and the National Science Foundation.

The DETER testbed provides a large-scale experimentation capability, as well as a safe means for qualitatively evaluating cybersecurity solutions against actual malware and other threats in a realistic environment. The testbed facilitates scientific experimentation and validation against established baselines of attack behavior and supports innovative approaches that involve "breaking" the network infrastructure (temporarily) while allowing the testbed to be reset and broken again and again. The testing framework allows researchers to experiment with a variety of parameters representing the network environment, including deployed defense technology, attack behaviors and network topologies, all without placing the actual Internet or real operational systems at risk.

The success of the DETER testbed lies largely in its collaboration with the cybersecurity research community. Annual workshops are conducted to disseminate and discuss project results, outcomes and reports documenting benchmarks, testbeds, data collection and analysis and evaluations of security mechanisms that have been deployed. It is important for the research community to share their results with each other and to discuss improvements to the DETER research infrastructure.

Significant impacts and accomplishments

The DETER testbed is used to test and evaluate cybersecurity technologies by more than 200 organization from more than 20 states and 17 countries, including major DHS-funded researchers and government, industry, academia and educational users. Additionally, the DETER testbed has been used by 30 institutions for more than 40 classes, ultimately reaching more than 2,000 students.

DETER provides the necessary infrastructure—networks, tools, methodologies and supporting processes—to support national testing of emerging and advanced security technologies. Current efforts will support larger and more complex experiments with increased usability.

To learn more about Experimental Research Testbed, contact sandt cyber liaison@hq.dhs.gov.