



DETER and EMIST

Cyber Defense Technology Experimental Research (DETER) Testbed and Evaluation Methods for Internet Security Technology (EMIST)

Overview

DETER and EMIST are two companion efforts that are operating as one unified project and are funded by the National Science Foundation (NSF) and the Department of Homeland Security's Advanced Research Projects Agency (HSARPA). NSF contracted the University of Southern California Information Sciences Institute (USC ISI) for the DETER project. Their team includes the Security Research Division of SPARTA and University of California, Berkeley. NSF contracted Pennsylvania State University for the EMIST project. Their team includes SPARTA as well as the University of California, Davis, UC Berkeley International Computer Science Institute's Center for Internet Research, Purdue University, and SRI International.

The information technology sector has experienced inadequate wide scale deployment of security technologies, in spite of more than ten years of investment in network security research. Also, there is a lack of experimental infrastructure that could provide an environment for testing and validation in small to medium-scale private research laboratories. Finally, we are missing objective test data, traffic, and metrics.

The vision of DETER/EMIST is to provide the scientific knowledge required to enable the development of solutions to cyber security problems of national importance. The project mission is, through the creation of an experimental infrastructure network, including networks, tools, methodologies, and supporting processes, to support national-scale experimentation on research and advanced

development of security technologies.

Goals

The goals of DETER are to:

- Facilitate scientific experimentation.
- Establish baseline for validation of new approaches.
- Provide a safe platform for experimental approaches that involve breaking network infrastructure.
- Create researcher- and vendor-neutral environment.
- Provide access for wide community of users.

The goals of EMIST are to:

- Develop scientifically rigorous testing frameworks and methodologies for defenses against attacks on network infrastructure: scale-down with fidelity.
- Develop experiments to yield deeper understanding of how previous attacks have, and future attacks will, affect the Internet and its users.
- Develop prototypical experiments (benchmarks) and associated databases of:
 - topologies and topology generators
 - attack and background traffic traces and generators
 - defenses
 - special-purpose devices (meters, virtual nodes, etc.)
 - metrics for scale-down fidelity, performance, overhead, etc.
- Consult in the build-out of DETER and demonstrate its usefulness to vendors, researchers and customers of defense technology.
- Allow for open, convenient, rigorous and unbiased testing of cyber defenses on DETER in order to expedite their commercial deployment.

This work sponsored by NSF through University of California, Berkeley, Contract Number SA4158-10138PG, and The Pennsylvania State University, Contract Number 2642-NAI-NSF-5241, with McAfee Research, which is now the Security Research Division of SPARTA.



DETER and EMIST

Cyber Defense Technology Experimental Research (DETER) Testbed and Evaluation Methods for Internet Security Technology (EMIST)

- In particular, collaborate on a friendly EMIST front-end GUI to the DETER test bed.
- Quickly and publicly disseminate our results.

Our Role

We are a member of the executive committee to provide operations oversight and approval of proposed experiments. We are also a key contributor to DETER security architecture, policies, and procedures. We will ensure protection of DETER from Internet and vice versa and isolation between experiments. We are customizing the Emulab software.

We also lead the DDoS experiment working group and are defining the canonical DDoS experiment framework. We are coordinating development of testing tools with Purdue and UC Davis. These tools include those to generate synthetic traffic, replay traffic traces, and remap onto test topologies. The tools also include those to automate experiments, cycle

through different test scenarios, e.g., topologies, traffic mixes, positioning of defenses, collection

of data, etc. We are providing detailed example of a DDoS experiment based on FloodWatch. We are coordinating with other DDoS teams developing DDoS, Routing, and Worm experiment examples.

Current Status

The DETER Experimental Network is a cluster of over 300 experimental nodes, interconnected dynamically into arbitrary topologies using a VLAN switch.

Currently, there are two established clusters at USC ISI – West and the University of California, Berkeley.

The clusters are, and will continue to be, interconnected across Internet using encrypted tunnels.

Nodes from different clusters can be combined in one experiment when user chooses – When Internet introduces variability that will be desirable or at least tolerable.

The Whole Cluster

