



Evaluation Methods for Internet Security Technology (EMIST)

DETER Community Workshop

June 15, 2006

Arlington, VA



UCDAVIS



EMIST TEAM

- PSU: G. Kesidis, P. Liu, P. McDaniel, D.J. Miller
- UCD: K. Levitt, F. Wu, J. Rowe, C.-N. Chua
- ICSI: V. Paxson, N. Weaver
- Purdue: S. Fahmy, N. Shroff
- SPARTA: S. Schwab, D. Sterne, R. Ostrenga, S. Murphy, R. Mundy, et al.
- SRI: P. Porras, L. Breisemeister
- DHS PM: D. Maughan
- NSF PMs: M. Maeda, J. Evans, D. Goodman
- Welcome and thanks to non-EMIST/DETER team member participants of this workshop.



EMIST experimental themes

- Experiment realism and reproducibility.
- Experiment methodologies (rigorous testing) and metrics.
- Software tools and formal frameworks for experiment specification:
 - Topology (RouteViews, Rocketfuel, PL topology generators, etc.)
 - Background traffic generation (trace driven)
 - Attack traffic generation (ditto)
 - End-systems
- Software tools for visualization of experimental results.
- Hardware platforms for some of the above: routers, IDS platforms, and ICSI's work with Stanford's netFPGA boards.
- Calibration of defenses under test.
- Experimental scale-down with fidelity.
- DETER/Emulab testbed-specific methodologies.



Some EMIST experimental plans

- Continued work on above research threads and summary reports.
- Hybrid BGP, worm, DDoS experiments.
- Focus on emerging live malware experiments on DETER:
 - DETER control plane quarantine
 - Realistic traffic, in particular with regard to DPI-based defenses
 - Deployment of defenses to test
- Expansion of netFPGA work.
- Tools to facilitate BGP experiment specification.