

Cyber Defense Technology Net- working and Evaluation

BY MEMBERS OF THE DETER AND EMIST PROJECTS

deck text: Creating an experimental infrastructure for developing
next-generation information security technologies.

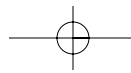
no art

1 As the Internet has become pervasive and our criti-
2 cal infrastructures have become inextricably tied to
3 information systems, the risk for economic, social,
4 and physical disruption due to the insecurities of
5 information systems has increased immeasurably.
6 Over the past 10 years there has been increased
7 investment in research on cyber security technolo-
8 gies by U.S. government agencies (including NSF,
9 DARPA, the armed forces) and industry. However, a
10 large-scale deployment of security technology suffi-
11 cient to protect the vital infrastructure is lacking.
12 One important reason for this deficiency is the lack
13 of an experimental infrastructure and rigorous scien-
14 tific methodologies for developing and testing next-
15 generation cyber security technology. To date, new
16 security technologies have been tested and validated
17 only in small- to medium-scale private research facil-
18 ities, which are not representative of large opera-
19 tional networks or of the portion of the Internet that
20 could be involved in an attack.

21 To make rapid advances in defending against
22 attacks, the state of the art in evaluation of network
23 security mechanisms must be improved. This will
24 require the development of large-scale security test-
25 beds [3] combined with new frameworks and stan-
26 dards for testing and benchmarking that make these
27 testbeds truly useful. Current deficiencies and
28 impediments to evaluating network security mecha-
29 nisms include lack of scientific rigor [6]; lack of rel-
30 evant and representative network data [5];
31 inadequate models of defense mechanisms; and
32 inadequate models of the network, and both the
33 background and attack traffic data [1]. The latter is
34 challenging because of the complexity of interac-
35 tions among traffic, topology, and protocols [1, 2].

36 To address these shortcomings, we have created
37 an experimental infrastructure network to support
38 the development and demonstration of next-genera-
39 tion information security technologies for cyber
40 defense. The Cyber Defense Technology Experimen-
41 tal Research network (DETER network) will pro-
42 vide the necessary infrastructure—networks, tools,
43 and supporting processes—to support national-scale
44 experimentation on emerging security research and
45 advanced development technologies. In parallel, the
46 Evaluation Methods for Internet Security Technology
47 (EMIST) project will develop scientifically rigorous
48 testing frameworks and methodologies for representa-





49 tive classes of network attacks and defense mecha-
50 nisms. As part of this research, approaches to deter-
51 mining domains of effective use for simulation,
52 emulation, hardware, and hybrids of the three are
53 being examined.

54 The goal of this joint effort¹ is to create, operate,
55 and support a researcher- and vendor-neutral exper-
56 imental infrastructure open to a wide community of
57 users. It is intended to be more than a passive
58 research instrument. It is envisioned to serve as a
59 center for interchange and collaboration among
60 security researchers, and as a shared laboratory in
61 which researchers, developers, and operators from
62 government, industry, and academia can experi-
63 ment with potential cyber security technologies
64 under realistic conditions, with the aim of accelerat-
65 ing research, development, and deployment of
66 effective defenses for U.S.-based computer net-
67 works.

68

69 **Information Security Challenges**

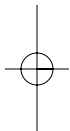
70 To develop a testbed framework for evaluating secu-
71 rity mechanisms, the project focuses on a select sub-
72 set of the overall problem space. Several different
73 types of attacks and defenses will be studied with
74 two goals: to elevate the understanding of the par-
75 ticular attack or defense by thoroughly evaluating it
76 via different testing scenarios; and to further the
77 understanding of the degree to which these evalua-
78 tions can be unified into a single framework that
79 spans the diversity of the problem space.

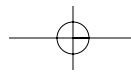
80 Three different classes of attacks are focus areas
81 for our research: denial-of-service, worms, and
82 attacks on the Internet's routing infrastructure, as
83 well as attacks that are coordinated combinations
84 of these three types. Together they span a broad
85 range of general types of attacks. In addition, the
86 project will closely monitor new Internet security
87 breaches in order to analyze how new attack sce-
88 narios can be incorporated into the developing test-
89 ing methodology. The focus of this effort will be on
90 attacks targeting network infrastructure, server end
91 systems, and critical end-user applications. Such
92 attacks are difficult to accurately simulate using
93 existing testing frameworks because of the major
94 challenges in accurately simulating Internet phe-
95 nomena in general [2, 4].

96

97 **Security Testing Methodologies**

98 Testing frameworks will be adapted for different
99 kinds of testbeds, including simulators such as NS
100 (see www.isi.edu/nsnam/ns), emulation facilities
101 such as Emulab [8], and both small and large hard-
102 ware testbeds. The frameworks will include attack
103 scenarios; attack simulators; generators for topology
104 and background traffic; data sets derived from live
105 traffic; and tools to monitor and summarize test
106 results. These frameworks will allow researchers to
107 experiment with a variety of parameters represent-
108 ing the network environment including attack
109 behaviors, deployed defense technology, and the
110 configuration of the defense mechanisms under test.
111 It will be critical to make headway on the very dif-





112 difficult problems, particularly:

113

- 114 • How to construct realistic topologies, including
- 115 bandwidth and inter-AS policies,
- 116 • How to generate realistic cross-traffic across these
- 117 topologies,
- 118 • How to quantify how accurate the models need
- 119 to be, and
- 120 • How to select the best metrics for evaluating vari-
- 121 ous defense mechanisms.

122

123 Conducting these tests will require incorporating
124 defense mechanisms into a testbed (as models or
125 operational code), and applying and evaluating the
126 frameworks and methodologies. Conducting these
127 tests will also help to ensure the testbed framework
128 allows other researchers to easily integrate and test
129 network defense mechanisms of their own. Further-
130 more, the documentation of the tests will serve as a
131 tutorial for users of the testbed framework as they
132 confirm their results or evaluate their own mecha-
133 nisms.

134

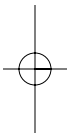
135 **Testbed Architecture and Requirements**

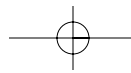
136 The preliminary requirements for the DETER Test-
137 bed are drawn from four sources: a DARPA-funded
138 study of security testbed requirements [3], input
139 from network security researchers, general consider-
140 ations on network research testbeds through a NSF
141 workshop [4], and experience with a variety of ear-
142 lier experimental and test networks. High-level
143 requirements are briefly described here.

144 The general objectives for the testbed design
145 require that it must be fully isolated from the Inter-
146 net and all experiments must be soundly confined
147 within the DETER network. Furthermore, it is
148 expected the network will be subjected to destruc-
149 tive traffic and that experiments may temporarily
150 damage the network. Therefore, there must also be
151 mechanisms for rapid reconstitution of the testing
152 environment.

153 The scale of the testbed is approximately 1,000
154 PCs, each with multiple network interface cards,
155 and a significant number of commercial routers and
156 programmable switches. Within this environment,
157 the network must provide sufficient topological
158 complexity to emulate a scaled down but function-
159 ally accurate representation of the hierarchical struc-
160 ture of the real Internet, and to approximate the
161 mixing of benign traffic and attack traffic that
162 occurs. Initially, the network will be formed using a
163 homogeneous network of existing technology. Care-
164 fully chosen hardware heterogeneity—commercial
165 router boxes—will be added as the effort progresses.
166 Finally, conducting experiments with large-scale
167 denial-of-service attacks and defense technologies to
168 protect the Internet infrastructure will require high-
169 bandwidth componentry.

170 In addition to the preceding infrastructure
171 requirements, there are various requirements for
172 software to facilitate experimentation. The utility of
173 DETER will depend on the power, convenience,
174 and flexibility of its software for setting up and





175 managing experiments including registration, defin-
176 ition, generation control, monitoring, check-point-
177 ing, and archiving. An important aspect of the
178 management software will be the requirement for
179 sophisticated network monitoring and traffic analy-
180 sis tools for both experimenters and DETER net-
181 work operators. Experimenters will also require
182 traffic generation software to generate attack traffic
183 and typical day-to-day (legitimate use) traffic.

184 **Preliminary Architecture.** DETER will be built
185 as three permanent hardware clusters, located at ISI
186 in Los Angeles, ISI-East in Virginia, and UC-Berke-
187 ley. To provide the earliest possible service to experi-
188 menters, initial development during the first six
189 months focuses on building software and configura-
190 tions for cyber security experimentation on Planet-
191 Lab and/or Emulab [8].

192 The architecture will also deploy aspects of the X-
193 bone (see www.isi.edu/xbone) to allow topologies
194 with revisitation, where, for example, a 10-node
195 ring can be used to emulate a 100-node ring by vis-
196 iting the same node multiple times. During the
197 early stages of the testbed, this will enable the simu-
198 lation of topologies that are larger than can be sup-
199 ported with one-to-one mapping of physical
200 resources. Meanwhile, a phased development effort,
201 moving from carefully-controlled emulation envi-
202 ronments to a mix of emulation and real network
203 hardware will occur.

204

205 **Conclusion**

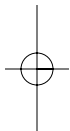
206 The development of testing methodologies comple-
207 mented by an experimental infrastructure will sup-
208 port the realistic and consistent evaluation of
209 mechanisms purported to mitigate large-scale
210 attacks. This is an extremely challenging undertak-
211 ing—no existing testbed or framework can be
212 claimed to be effective. The research described here
213 requires significant advances in the modeling of net-
214 work attacks and the interactions between attacks
215 and their environments, including deployed defense
216 technology, background traffic, topology, protocols,
217 and applications. It will also require advances in the
218 understanding of metrics for evaluating defense
219 mechanisms.

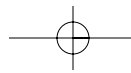
220 Our results will provide new scientific knowledge
221 to enable the development of solutions to cyber
222 security problems of national importance. This will
223 be accomplished through experimentation and vali-
224 dation of cyber defense technologies using scientific
225 methods. The lack of open, objective, and repeat-
226 able validation of cyber defense technologies has
227 been a significant factor hindering wide-scale adop-
228 tion of next-generation solutions. Results obtained
229 using the DETER testbed will contribute to the
230 development of innovative new technologies that
231 increase commercial availability and viability of new
232 production networks and services, providing true
233 cyber protection.

234

235 **References**

236 1. Floyd, S. and Kohler, E. Internet research needs
237 better models. *Hotnets-I* (Oct. 2002).





- 238
239 2. Floyd, S. and Paxson, V. Difficulties in simulat-
240 ing the Internet. *IEEE/ACM Transactions on Net-*
241 *working* 9, 4 (Aug. 2001), 392–403.
242
243 3. Hardaker, W. et al. *Justification and Require-*
244 *ments for a National DDoS Defense Technology*
245 *Evaluation Facility*. Network Associates Laborato-
246 ries Report 02-052, July 26, 2002.
247
248 4. Kurose, J., Ed. *Report of NSF Workshop on Net-*
249 *work Research Testbeds* (Nov. 2002);
250 gaia.cs.umass.edu/testbed_workshop.
251
252 5. McHugh, J. Testing intrusion detection systems:
253 A critique of the 1998 and 1999 DARPA intrusion
254 detection system valuations as performed by Lin-
255 coln Laboratory. *ACM Transactions on Information*
256 *and System Security* 3, 4 (Nov. 2000), 262–294.
257
258 6. Pawlikowski, K., Jeong, H., and Lee, J. On cred-
259 ibility of simulation studies of telecommunication
260 networks. *IEEE Communications Magazine* (Jan.
261 2001).
262
263 7. Peterson, L., Anderson, T., Culler, D., and
264 Roscoe, T. A blueprint for introducing disruptive
265 technology into the Internet. In *Proceedings of the*
266 *1st ACM Workshop on Hot Topics in Networks (Hot-*
267 *Nets-I)* (Oct. 2002), 4–140.
268
269 8. White, B. et al. An integrated experimental
270 environment for distributed systems and networks.
271 In *Proceedings of the Fifth Symposium on Operating*
272 *Systems Design and Implementation (OSDI02)*,
273 (Dec. 2002).
274
275
276 Members of the DETER and EMIST network
277 project include R. Bajcsy, T. Benzel, M. Bishop, B.
278 Braden, C. Brodley, S. Fahmy, S. Floyd, W.
279 Hardaker, A. Joseph, G. Kesidis, K. Levitt, B. Lin-
280 dell, P. Liu, D. Miller, R. Mundy, C. Neuman, R.
281 Ostrenga, V. Paxson, P. Porras, C. Rosenberg, J.
282 Tygar, S. Sastry, D. Sterne, and S.F. Wu.

283
284 FOOTNOTES:

285
286 ¹There are nine teams involved in the joint effort:
287 U.C. Berkeley, U.C. Davis, USC ISI, Penn State,
288 NAI Laboratories, ICSI, Purdue, SPARTA Inc.,
289 and SRI International. The project also includes an
290 industrial advisory board consisting of equipment
291 vendors, carriers, and ISPs including AOL, Cisco,
292 Alcatel, Hewlett-Packard, IBM, Intel, Juniper, and
293 Los Nettos.
294

295
296 Permission to make digital or hard copies of all or part of this work for personal or
297 classroom use is granted without fee provided that copies are not made or distributed
298 for profit or commercial advantage and that copies bear this notice and the full cita-
299 tion on the first page. To copy otherwise, to republish, to post on servers or to redis-
300 tribute to lists, requires prior specific permission and/or a fee.

