

The DETER Testbed and Networked Embedded Control for Cyber Physical Systems

Anthony D. Joseph
Professor, EECS Department
University of California, Berkeley

Terry V. Benzel
Deputy Director Computer Networks Division
Information Sciences Institute, University of Southern California

The cyber DEfense Technology Experimental Research (DETER) testbed [ACM04, DETER06], supported by NSF and DHS, is a general-purpose experimental testbed for cybersecurity research and education in use since 2003 by academic, industrial, and government experimenters. As the largest open, free experimental facility dedicated to cyber security research, the testbed provides a unique, powerful tool for experiments with resource needs preventing them from being performed anywhere else. DETER is also a teaching platform for cybersecurity classes. DETER safely supports cybersecurity experiments, including experiments on “risky” code that cannot be performed in the Internet because of traffic volumes or the risk of escape. Examples for which DETER has already been useful include DDoS attack dynamics and defenses, virus and worm propagation and defenses, and attacks on network routing infrastructure. The DETER testbed, based upon Utah’s Emulab software, allows remote experimenters to allocate large numbers of nodes, link them with nearly-arbitrary topologies, load arbitrary code for routing, traffic generation, defense mechanisms, and measurement tools, and execute their experiments.

The design, development, and testing of next-generation networked embedded controllers is an expensive and complex multi-year process that introduces many pressing challenges for systems designers, developers, and vendors, and for the physical plant owners/operators. As infrastructure that is replaced or upgraded on three to twelve year cycles, these systems represent significant capital and time investments, and, present significant opportunities for cyber vulnerability analysis and exploitation by malicious parties. The complexity of networked embedded controller-based systems is growing as these systems are increasingly being interconnected with enterprise networks, often for Total Quality Management purposes, and directly or indirectly with public networks, such as the Internet, for remote management purposes. Interconnection with enterprise networks introduces two threats: exposure to compromised desktop machines, and malicious insiders. Desktop machines are vulnerable to compromise by e-mail- or removable media-borne worms and viruses; once compromised, they can be used to attack networked embedded controller systems. Similarly, the insider threat is also a growing problem. Paper design and analysis, along with small-scale emulation, are insufficient tools for addressing these threats, as they may not capture all of the interaction effects found in a large, real system.

There are existing small-scale testbeds for evaluating networked embedded controllers; however we posit that incorporating extensive, realistic, large-scale emulation and testing of these systems into the design and development process would be an important and beneficial improvement. A key goal of this testing would be to anticipate types and scales of cyber attacks against systems under development, and to enable the accurate emulation of enterprise networks and embedded network controller systems. Another goal would be to identify best practices for the testing process. We believe that the DETER testbed could be an excellent starting point for building a public testbed where all interested parties could design, model, and test their systems. In addition, the testbed would be an ideal place to store libraries of testing strategies and data. By using Field Programmable Gate Array technology, it should be possible to emulate the behaviors of actual networked embedded controllers, sensors, actuators, and the corresponding control/data traffic. The size of testbeds is often limited by many factors, such as cooling, power, space, and weight requirements. These limitations can be partially addressed by building multiple smaller testbeds, however the scope and scale of experiments is limited. To emulate particularly large systems (e.g., a large regional power grid) with tens of thousands of sensors and actuators, we propose the dynamic federation of multiple networked embedded controller testbeds into a single very large

testbed (or for parallel development, multiple large testbeds). Such an approach offers administrative and flexibility, addresses the limitations associated with building very large testbeds, and it provides an on-demand ability to scale to large experiments. We are developing support for federation of multiple testbeds into a single logical testing environment.

A testbed can also be used for other important applications – periodic operator training and system red-teaming. Both applications are challenging, but necessary requirements given continually changing systems and threat models. By using a testbed, owners/operators can explore different console screen application designs and layouts, and they can gauge operator reactions to various scenarios (representing both normal, abnormal, and attack situations). The DETER testbed has already been used for training and classroom exercises, and could easily be adapted for operator training and system red-teaming tasks.

We believe that a five to ten year research plan in this area should focus on two key areas:

- **Building multiple testbeds where developers and owners/operators can explore and test new devices, protocols, architectures, and applications.** We need to develop testbeds that incorporate actual networked embedded controllers, FPGA- and software-based controller emulators, and actual and emulated software plant control systems. The testbeds should also be capable of being federated into one or more large testbeds for large-scale experiments and tests.
- **Improving the training of the operators and security defenders responsible for these systems.** We need to collect best-practices for evaluating operators' behaviors and reactions, and deploy traffic/scenario generation utilities. In addition, we need to emulate real-world networked embedded controller installations and work with corporate and government agencies to develop comprehensive red-team training software and systems.

[DETER06] Terry Benzel, Bob Braden, Dongho Kim, Clifford Neuman, Anthony D. Joseph, and Keith Sklower, Ron Ostrenga, and Stephen Schwab, *Experience with DETER: A Testbed for Security Research*. Second IEEE Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), Barcelona, March 2006.

[ACM04] DETER/EMIST team, *Cyber Defense Technology Networking and Evaluation*, Communications of the ACM, March 2004.

Dr. Joseph received his B.S., S.M., and Ph.D. degrees in computer science from MIT. He joined the UC Berkeley faculty in 1998, where he is developing adaptive techniques for: distributed detection of worms and viruses, dynamic prevention of end system infection, and automated containment of infected systems. He also co-leads the DETER testbed project in its efforts to build a secure, scalable testbed for conducting next-generation cybersecurity research into worms, viruses, distributed denial of service attacks, and attacks against routing infrastructure. He can be reached at adj@cs.berkeley.edu or at (510) 643-7212.

Terry V. Benzel is Deputy Director for the Computer Networks Division at the Information Sciences Institute (ISI) of the University of Southern California (USC). She participates in business development, technology transfer and special projects with industrial and academic partners. She is the technical project lead for the Cyber Defense Technology Experimental Research (DETER) testbed. Ms. Benzel has a joint appointment at the Marshall School of Business where she is a researcher at the Institute for Critical Information Infrastructure Protection. Prior to joining USC ISI, Ms. Benzel was a Division Vice President at Network Associates, Inc. She can be reached at tbenzel@isi.edu or at (310) 448-9438.