TIED – Trial Integration Environment Based on DETER

QPR March 31, 2009

Introduction

We report on three areas of work this quarter. These are continuing development of the TIED federation model, capabilities, and software, deployment and evangelization of TIED's federation facilities beyond the initial TIED federants, and development and deployment of regional and national scale Layer 2 network capabilities and infrastructure for TIED. Each of these areas is described in a subsection below. We also briefly describe two outreach activities, and provide a list of project participants and collaborators.

Major Accomplishments

- Trial deployment and use of TIED federation architecture implementation at facilities outside of the TIED project – WAIL and Utah Emulab.
- Initial configuration and provisioning of a layer 2 VLAN path from ISI in Los Angeles to ISI East in Arlington, VA, crossing LA DWP fiber, Los Nettos, CENIC, Internet 2, and MAX.
- Operation and demonstration of a large federated experiment using TIED/DETER technology at CATCH 2009[1], modeling and visualizing a Worm->Botnet->DDOS cybersecurity attack scenario of approximately 5000 virtual host nodes.

Description of Work Performed During the Quarter

1. Continued Development of TIED Federation Model, Capabilities, and Software

A primary focus of TIED activities over this quarter has been extending the TIED federation software (***fedd***) released at the end of the previous software by improving its input language and the richness of its authorization model. These activities directly support running a TIED clearinghouse (milestone d), lay the groundwork for extended capabilities (milestone g) and are informed by our assessment of the needs of our users. These tasks were ongoing throughout the quarter.

1.1. CEDL Design Extensions

Related Milestones:

Year 1, Milestone d: Operate prototype TIED clearinghouse.
Year 1, Milestone e: Provide user access to DETER testbed using TIED building blocks.
Year 1, Milestone f: Demonstrate and support running federated experiments by owner(s) outside the development team by the end of year 1.
Year 2, Milestone a: Develop and deploy TIED plugin to access and control wide area network resources.

The Common Experiment Description Language (CEDL) is central to the TIED and the DETER Federation Architecture (DFA) on which TIED is based. That architecture was summarized in last quarter's report and is also described at http://fedd.isi.deterlab.net. CEDL is the "assembly language" in which an experiment is represented and it encodes the topology and constraints on an experiment/slice. CEDL sits at a key interface for GENI users to access the TIED clearinghouse and DETER testbed (year 1 milestones d & e), provides the basis for describing federated experiments to

1 Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH 2009). March 3-4, 2009, Washington, DC., USA.

the TIED experiment federator (year 1 milestone f) and provides the structured canonical experiment representation necessary to support "plugins" for different component types (year 2 milestone a).

To date the DFA has been using a simple extension of Emulab's topology language, itself an extension of the ns-2 simulaton language (itself an extension of the tcl embedded configuration langage).

Just as adopting ns-2 helped Emulab transition early users from a simulation-based world to an emulation-based one, the DFA's incorporation of the Emulab language has smoothed the transition for early DFA adopters. However, there are several shortcomings of the language.

Tcl is a Turing-complete programming language. While most experiment descriptions are non-conditional, non-iterative lists of topology declaration statements, some experiments make use of the full power of tcl. This is a feature when the language is intended to be written directly by a researcher, as ns-2 confugurations were, because writers can make use of iteration to produce compact parameterizable descriptions. However, CEDL's role as a low level language output by user tools and input to the federation system will benefit from a simpler, more carefully designed representation.

As an example, CEDL maps attributes to experiment elements inside a topology. Though the current ns-2-based language is capable of assigning attributes to experiment elements, it does so very directly. We intend to extend CEDL to allow attributes to be applied using indirect mecahnisms as well. For example, rather than requiring an experiment designer to assign a "leaf" attribute to all nodes with one interface, the new CEDL would include a rule for assigning that attribute.

We are currently designing the replacement for our initial CEDL implementation that will address those issues and significantly improve the functionality of the TIED federation design. The process is continuing and will be documented on the ***fedd*** site and other appropriate outlets including a GENI design document.

1.2. Authorization System Design

Related milestones:

Year 1, Milestone a: Identify specific outreach communities for the year-1 program. Identify and document initial requirements they impose on TIED federation architecture and interfaces.
Year 1, Milestone g: Demonstrate extended clearinghouse / component functionalities key to outreach communities (e.g., extended security model access).
Year 1, Milestone i: Collaborate with Security team on security design for Spiral 1.

The initial implementation of TIED's federation system employs a simple attribute-based authorization logic based on a generalization of Emulab projects and users. This model is described in detail at http://fedd.isi.deterlab.net and in "Access Control for Federation of Emulab-based Network Testbeds" published in CSET 2008.

While this simple system has proved useful in prototyping our implementation of federation and transitioning DETER users into a federated environment, it has significant shortcomings in terms of scalability and expressiveness. Our assessment of user community needs (year 1 milestone a) identified the key characteristics of a more flexible and auditable system. Furthermore, our expanded user communities use a variety of systems to establish initial trust, and supporting that diversity is a major goal. To meet these needs, we are developing an alternative system known as Attribute-Based Access Control system (ABAC), derived from previous theoretical and practical work at NAI labs and Stanford University.

ABAC is rooted in an extended first order predicate calculus specialized to simply express common deduction rules used in making access control decisions. It reasons in terms of principals with asserted attributes and supports notions of delegation, validation and consensus in efficient and auditable ways. Furthermore, the reasoning rules are independent of how the attributes and principals establish their trustworthiness. This provides an important separation of concerns

between establishing trust and implementing authorization policy.

Work this quarter includes reviewing an existing implementation of an ABAC-like system from NAI to determine whether it is a suitable base for implementation in TIED, extension of the ***fedd*** authorization interfaces to support ABAC functionality, and design of a complete system integrating ABAC with primary trust establishment mechanisms such as Kerberos or Shibboleth.

Implementation of this extended functionality constitutes a major element of TIED's year 1 milestone g. We are also working in close collaboration with Steve Schwab at SPARTA to discuss and transfer lessons learned from our requirements analysis, design, and implementation to his Security Architecture project as appropriate (year 1 milestone i).

2. Federation (*fedd*) Deployment and Evangelization

Related milestones:

Year 1, Milestone d: Operate prototype TIED clearinghouse.
Year 1, Milestone e: Provide user access to DETER testbed using TIED building blocks.
Year 1, Milestone f: Demonstrate and support running federated experiments by owner(s) outside the development team by the end of year 1.

In order to more effectively demonstrate and propagate TIED's federation model and the **fedd** implementation of this model, we are working to incorporate several non-DETER testbeds into the TIED federation. Our current collaborators are the WAIL testbed at the University of Wisconsin and the Emulab testbed at the University of Utah. In addition, we are in contact with a group at Purdue who have submitted a proposal to GENI Solicitation 2. We have demonstrated initial capability to federate experiments across both DETER/Emulab and DETER/WAIL, in each case creating a single experiment larger than what could be supported by either testbed alone. We have also provided installation assistance and documentation clarification to staff at Utah and Wisconsin, and incorporated feedback from this effort into our next generation documentation. We continue to provide such support.

These outreach efforts are key to providing access to DETER using TIED building blocks (milestone e) and a precursor to providing federated experiments to people outside TIED (milestone f).

3. Deployment of TIED Layer 2 Network Infrastructure

Related milestones:

Year 1, Milestone j: Provide direct external ethernet-level (VLAN) access interface to TIED resources.
Year 2, Milestone a: Develop and deploy TIED plugin to access and control wide area network resources.

A key aspect of the TIED federation model is its ability to federate with and utilize a wide range of infrastructure resources, network types, and other facilities through the use of the canonical experiment description language CEDL and a variety of *federation plugins* to support different resource types. Our GENI solicitation 1 proposal placed particular focus on federation with networks controlled by DRAGON path allocation software. We view this

Working with the DRAGON project leader at ISI East, and our partners at regional ISPs Los Nettos and CENIC, we are deploying a DRAGON-controlled network between two existing and one planned TIED site to prototype this capability. The deployment is being designed to simplify eventual connections to other sites reachable through Internet2 and National Lambda Rail (NLR). This work directly feeds into year 1 milestone j – providing a boundary interface for switched ethernet VLAN connections – as well as addressing the broader GPO goals of national-scale end-to-end layer 2 capability and federation across multiple resource managers and owners.

Figure 1 below shows our plan for initial connectivity topology between two existing TIED / DETER site, at USC/ISI and at UC Berkeley, together with a third planned site at ISI East, in Arlington, Virginia. The planned ISI East site will include a small (10-20 machine) infrastructure cluster

together with a user facility supporting multiple plasma screens and advanced capabilities for network and security experiment visualization.

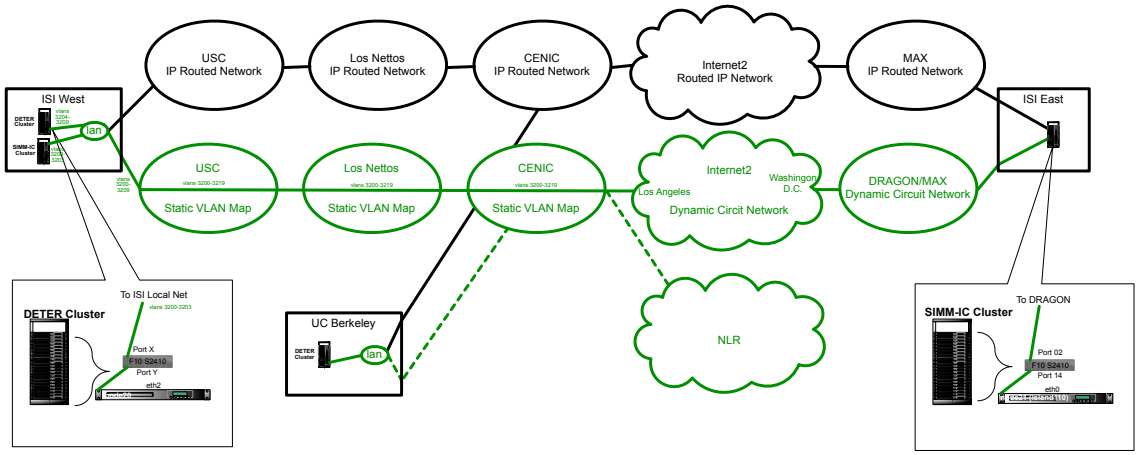

Figure 1: TIED Layer 2/3 Network Connection Plan, 3/2009

Once available, this infrastructure will provide on-demand provisioned network access to TIED federants reachable through Internet2 and particularly NLR. While the initial federants are all operated by the TIED project team, our intention is to quickly support additional, non-TIED federants as the capability is proven. This will directly address the deliverables related to providing end-to-end slice creation across dynamic virtual local area networks (VLANs), incorporation of non-TIED resources, and access to the TIED facility from multiple communities and points of presence.

Providing this infrastructure requires coordination and cooperation between several Internet Service Providers and Regional networks. As Figure 1 shows, a range of different entities need to work together to provide this connection. The administrative and engineering effort has been substantial. We have reached the final stages of this deployment and expect to demonstrate the capability in the next quarter.

We note that due to both GENI and DETER program objectives this activity is being given higher priority than anticipated in our original TIED proposal, and we anticipate that significant elements of the capability will be operational earlier than originally proposed.

Project Participants

Individuals directly supported by TIED award:
John Wroclawski, PI
Ted Faber, Research Computer Scientist

Individuals contributing to the project with outside support:
Terry Benzel, Deputy Division Director and Research Scientist
Annette Deschon, Systems Programmer
Tom Lehman, Research Computer Scientist
Jelena Mirkovic – Research Computer Scientist

Publications

(These publications were listed as "to appear" in our 12/31/08 QPR. They are repeated here because each actually appeared and was presented in the timeframe of this report.)

A Federated Experiment Environment for Emulab-based Testbeds. T. Faber and J. Wroclawski. 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TRIDENTCOM 2009) . April 6-8, 2009, Washington D.C., USA.

This paper presents an overall description of the DETER Federation Architecture that underpins our work on TIED; outlines key elements of the architecture including resource allocation, authorization and access control, and experiment control environment, and presents a brief description of the development prototype.

Current Developments in DETER Cybersecurity Testbed Technology. T. Benzel, R. Braden, T. Faber, J. Mirkovic, S. Schwab, K. Sollins, and J. Wroclawski. Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH 2009). March 3-4, 2009, Washington, DC., USA.

This paper presents rationale and initial design for three key areas of current technical work on DETER: Federation, Risky Experiment Management, and Experiment Health Management. Although the paper describes work outside of the TIED award per se*, we list it here because it discusses several technologies related to TIED and because it captures work of significant value to GENI but funded by another agency of the US Government.*

Outreach Activities

CSET 2009 – TIED project members are primary organizers of the 2nd Usenix Workshop on Cyber Security Experimentation and Test (CSET 2009) to be held on August 10, 2009 in conjunction with the annual Usenix Security Symposium. This workshop brings together researchers and testbed developers interested in sharing experiences and defining an agenda for the development of scientific, realistic evaluation approaches to security threats and defenses. With NSF support, CSET 2009 offers a student travel program, and makes particular effort to recruit presenters and attendees from underserved communities. TIED project member Terry Benzel serves as General Chair of CSET 2009, while contributor Jelena Mirkovic serves as co-Program Chair. Further information is available at http://www.usenix.org/event/cset09.

WISE 2009 – TIED project member Terry Benzel will participate and present at the 2009 Women's Institute in Summer Enrichment (WISE 2009) hosted by the NSF-sponsored TRUST Center at UC Berkeley. WISE is a 1-week residential summer program on the University California, Berkeley campus that brings together graduate students, post-doctoral fellows, and professors from all disciplines that are interested in the technical, social, political, and economic ramifications of security technologies and security research. Leading experts from across the country teach power courses in several disciplines, including computer science, economics, law, and electrical engineering. The program structure includes rigorous classes in the mornings and opportunities to explore through hands-on experiments and team-based projects in the afternoons. Further information is available at http://www.truststc.org/wise.

Collaborations

1) University of Utah: Emulab group (Rob Ricci and staff) – development and testing of the TIED Federation Architecture software.
2) University of Wisconsin: WAIL (Paul Barford and staff) – development and testing of the TIED Federation Architecture software.
3) SPARTA: (Steve Schwab) – Development of attribute based security models for federation (to be implemented in the TIED code base)
4) SPARTA: (Steve Schwab, Brett Wilson) – Development of support for federated experiments within the SEER Experiment Control Environment.
5) USC/ISI East: (Tom Lehman) DRAGON project at ISI-East. See discussion under Activities and Findings, above.

Other Contributions

TIED demonstration at GEC4 – TIED project member Ted Faber demonstrated operating early

versions of TIED's *fedd* federation facility and *SEER* experiment management system at the 4th GENI Engineering Conference, held March 31-April 2, 2009. The demonstration showed the SEER experiment management system controlling a large federated experiment deployed across multiple Emulab-style testbeds as federants.

Federated large-scale experiment demonstration at CATCH 2009 – Members of the DETER project demonstrated to an audience of cybersecurity researchers and congressional and government staff a large federated experiment using TIED and DETER technology at CATCH 2009, March 3-4 in Washington, DC. The demonstration modeled a cybersecurity scenario involving first, the propagation of a worm throughout the worldwide Internet from an initial source to some 5000 infected machines; second, the use of this worm to create and deploy a botnet; and third, the use of this botnet, commanded from a central point, to launch a distributed denial of service attack on a single e-commerce web server.

Although framed in the context of DETER, our presentation of this material discussed the connection and contribution of these technologies to the TIED project and their potential within GENI, as well as the contribution of infrastructure and facilities to large-scale networking and cybersecurity research more generally.