

TRANSITION TO EDUCATION:

Increasing the outcomes of your research

Cyber Security Division 2012 Principal Investigators' Meeting

October 9, 2012

Gary Bridges
Director, Client Services
SRI International
Gary.bridges@sri.com
650.703.4570

Transition to Education

- Over the past year, SRI investigated the degree to which CSD-funded PI's research results could be used as educational materials in the Nation's *Education Enterprise**

* Professors, instructional developers, curriculum specialists, and students in U. S. schools, colleges and Universities

CyberSTEP Value Proposition

NEED

- The Nation's educators are poorly equipped to provide badly-needed cyber security instruction*
- A significant part of this problem is lack of appropriate curriculum materials, especially emerging research results*

*National K-12 Study, National Cyber Security Alliance

CyberSTEP Value Proposition

APPROACH

- Explored the feasibility of establishing multiple pipelines through which CSD-funded research results can flow to the Nation's education enterprise

CyberSTEP Value Proposition

BENEFITS

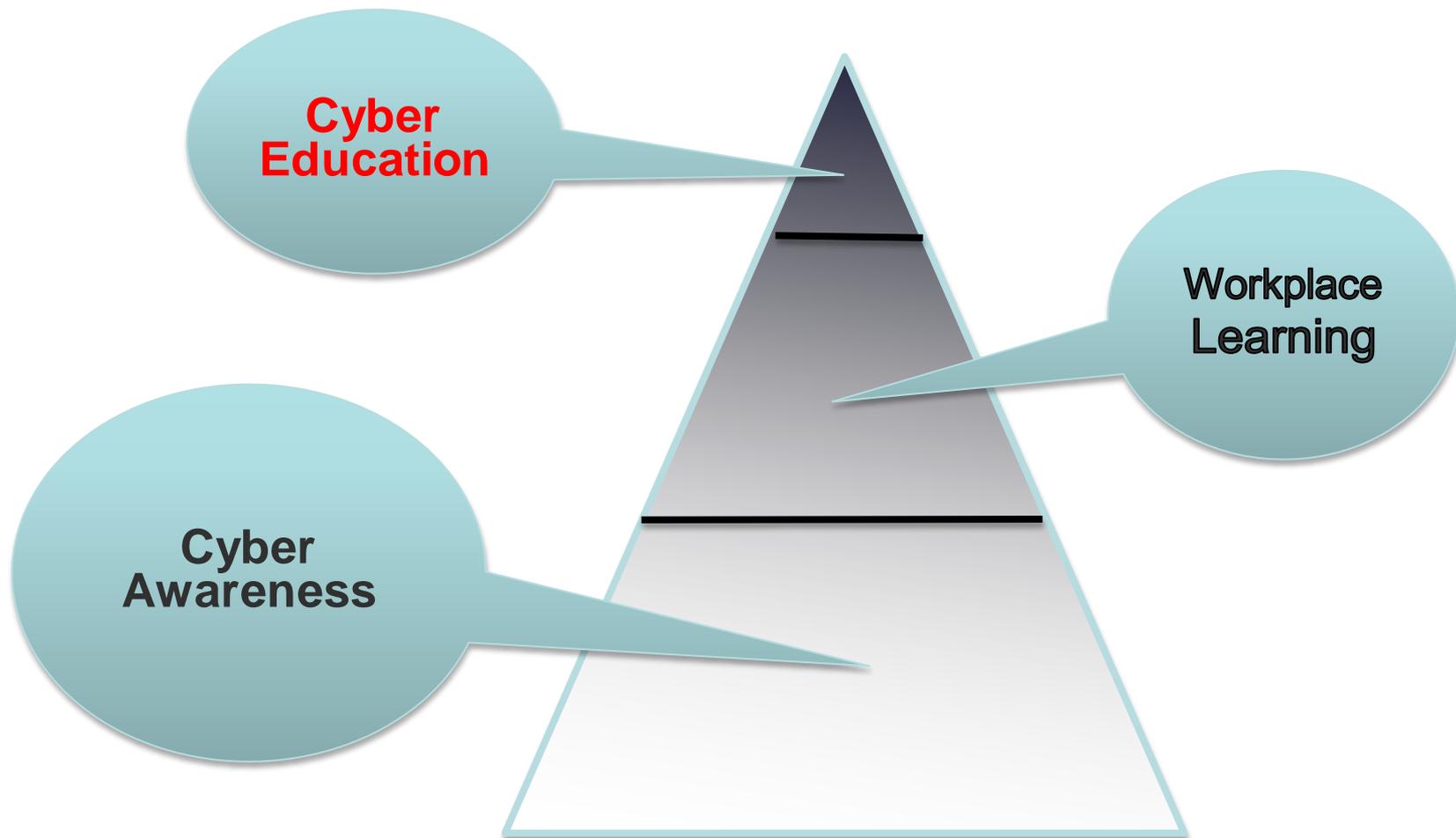
- Adds value to CSD-funded research by broadening user community
- Increases the currency and quality of cyber security education across the Nation
- Leverages existing R&D effort w/ minimal cost
- Maximizes transition / impact of CSD-funded research

CyberSTEP Brief History

CyberSTEP 1

- SRI International interviewed 20 PI's to determine the educational uses of their research results
- Virtually all felt their research results could be useful as instructional curriculum content and learning activities
- Varying degrees of additional customizing needed for research results to be instructor-ready

Three Potential Transition Targets



CyberSTEP Brief History

CyberSTEP2

- SRI interviewed 4 additional PI's in depth to select a “worked example” of instructor-ready research results
- Dr. Dan Massey of Colorado State agreed to provide his research results AND instructional materials as the worked example for this project

Where Does My Research Fit?

- BGPmon Project: Monitors and Analyzes Internet Routing
- We'll use the 2013 ACM/IEEE Computer Science Curriculum Strawman to help locate a potential home
 - <http://ai.stanford.edu/users/sahami/CS2013/>

Where Does My Research Fit?

KNOWLEDGE AREAS

Algorithms and Complexity (AL)
Architecture and Organization (AR)
Computational Science (CN)
~~Discrete Structures (DS)~~
Graphics and Visualization (GV)
Human-Computer Interaction (HC)
Intelligent Systems (IS)
Information Assurance and Security (IAS)
~~Information Management (IM)~~

Networking and Communication (NC)
Operating Systems (OS)
Platform-Based Development (PBD)
Parallel and Distributed Computing (PD)
Programming Languages (PL) Software
Development Fundamentals (SDF)
Software Engineering (SE)
Systems Fundamentals (SF)
Social and Professional Practice (SP)

Where Does My Research Fit?

KNOWLEDGE UNITS (KU)

- Networking and Communication, for example

NETWORKING AND COMMUNICATION	<ol style="list-style-type: none">1. Introduction2. Networked Applications3. Reliable Data Delivery4. Routing and Forwarding5. Local Area Networks6. Resource Allocation7. Mobility
-----------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Instructional Materials

- Prepared instructional materials, including:
 - Overview of BGP routing
 - Simple student exercise to teach basic routing
 - Open-ended exercise to explore routing security
- Collected as easy to edit and extend Wiki pages

BGPmon Wiki Page

BGPmon

Monitoring and Securing Internet Routes

[Home](#)[Course Map](#)[Instructional Materials](#)[Assessments](#)[Final Project](#)[Contact](#)

Main

Home Page

Knowledge Area/ Knowledge Unit:

Networking and Communication/Routing and Forwarding

Overview

This course module introduces students to Internet routing concepts and the BGP routing protocol in particular. The Internet is logically organized as a collection of Autonomous Systems. Examples of Autonomous System can include large organizations such as ATT or Google and smaller organizations such as the University of Colorado. BGP is the routing protocol used announce reachability between Autonomous Systems. The course module will teach students basic BGP concepts and allow one monitor actual BGP route changes that occur in the Internet. BGP also has several well known security vulnerabilities and the final course project asks students to develop a tool that looks for invalid BGP routes.

Time Required to Complete This Exercise

Timeline: 4 weeks

Workload: 4 hrs/wk

Objectives

After successfully completing this course, you should:

- Understand how the Internet is logically divided into Autonomous Systems
- Understand how BGP is used to exchange reachability information between Autonomous Systems
- Understand the concept of longest prefix match when forwarding IP packets.
- Learn how to monitor BGP routing changes and look for changes associated with a particular prefix
- Understand the security vulnerabilities of BGP and develop a tool that looks for invalid BGP routes

Search

HomePage

My Project

The BGPmon Project

PERL BGPmon Modules

A BGP Hijacking Event

A Continent Drops Off The Net

Route Origin Verifier (ROVER)

Instructor

BGPmon Wiki Page

BGPmon

Monitoring and Securing Internet Routes



[Home](#) [Course Map](#) [Instructional Materials](#) [Assessments](#) [Final Project](#) [Contact](#)

Main Projects

The final project asks you to look for BGP routing hijacks in the actual Internet.

Identify A Few Critical Prefixes

Select a small number of critical prefixes to track. For example, you may want to monitor the routes to your institution or to some other site of interest such as your bank or your favorite website. Your critical prefix list may be as simple or complex as you desire.

For example, you might use the WHOIS database to find the prefixes that are owned by your organization. Alternatively, you might identify the IP address for your website and look for any prefix that is used to route to that prefix.

Write A BGP Monitoring Tool

Using the [BGPmon Project Live Data Feed](#), write a tool that receives real-time BGP updates and then filter this live data to show only updates that impact your critical prefixes.

Note the [Perl BGPmon Modules](#) allow you to easily obtain and parse BGP data.

Construct a Historical View of Your Prefixes

Using the [BGPmon Project Archives](#), write a tool that reviews one year of data and shows only updates that impact your critical prefixes.

Again note the [Perl BGPmon Modules](#) allow you to easily obtain and parse BGP data.

Develop a hypothesis for how you expect your prefixes to behave.

Search

[HomePage](#)

My Project

[The BGPmon Project](#)

[PERL BGPmon Modules](#)

[A BGP Hijacking Event](#)

[A Continent Drops Off The Net](#)

[Route Origin Verifier \(ROVER\)](#)

Instructor

Wiki Template

Sample Project

Project Sub title

CyberSTE

Cyber Security Transition to Education

Sponsored by the Department of Homeland Security

[Home](#)

[Course Map](#)

[Instructional Materials](#)

[Assessments](#)

[Final Project](#)

[Bibliography](#)

[Contact](#)

Main

Home Page

Knowledge Area/ Knowledge Unit:

Insert Your Knowledge Area and Knowledge Unit - Taken from the [2013 ACM/IEEE Computer Science Curriculum Strawman](#)

Overview

The goal of this project is to transition Department of Homeland Security research into instructional materials. Each project is expected to develop one or more instructional course modules. These course modules will vary with the project, but are expected to include Instructional Materials, Assessments, and a Final Project. The students taking this course may be undergraduates or graduates in an existing course or may be students pursuing independent learning.

This template provides an example of the resulting format for the course that you will develop and gives some instruction on each part for what you the course developer should complete. On every page you will find a description of what needs to be included on that page and directions for completing that section. As you put your own content up, you should remove the directions in this template.

Your final result will be a self-contained course module focused around a final project. It will comprise a couple key components, which lead directly into the final project, and their prerequisite components. In addition, your course will provide assessments leading into and out of each key component. This structure will allow your course to be taken as a whole module or broken into individual self-contained components that may be used separately. The 'Course Map' tab shows a visual representation of this structure.

Time Required to Complete This Exercise

Timeline: X weeks

Workload: Y hrs/wk

Search

Go

[HomePage](#)

My Project

[Inset Link to Your DHS Project](#)

[Project Specific Links Go Here](#)

[Instructor](#)

Transitioning Your Results

- Your research results probably have a home in the Nation's education enterprise
- We're available to explore this with you further:
 - Gary Bridges, 650.703.4570, gary.bridges@sri.com
 - David Balenson, 703.247.8551, david.balenson@sri.com
 - Dan Massey, 720-937-5755, massey@cs.colostate.edu