Areas URI Cyber Research Funding:

• Law enforcement tools and technologies including steganography detection, digital evidence search string support, cell phone security, cloud forensics

• Trust Sensor Interface

• Power Grid Security
URI Cyber State-of-the-Art Teaching Facilities; Collaborations with Law Enforcement, Emergency Responders On Network Forensics; and Protection of Critical Infrastructure:

• On-line Teaching Command Center
• Virtual Instructional Lab, a RAVE node
• RI State Crime Lab located on campus, which is a model for state crime labs
• URI is under contract to the RI State Computer Crimes Unit, for use of the URI computer forensics lab
• URI is working with the State Cybersecurity Group cooperatively seeking funding for training and cyber-preparedness in RI
• URI is collaborating with local businesses on research related to Trust in Sensor Networks
Panel : Cyber Challenges for Workforce Development

*Introductions and Facilitator:* Lisa DiPippo, Ph.D., Associate Professor, URI Department of Computer Science and Statistics

Johan Uvin, Ph.D., Deputy Assistant Secretary of Policy and Strategic Initiatives, Office of Vocational and Adult Education, U.S. Department of Education

Frank Zaborowski, Director, Competition Operations, CyberPatriot

Vic Fay-Wolfe, Ph.D., Professor, URI Department of Computer Science and Statistics

Panel Q & A Discussion
Johan Uvin, Ph.D.

Deputy Assistant Secretary of Policy and Strategic Initiatives
Office of Vocational and Adult Education
U.S. Department of Education

Cyber Challenges for Workforce Development
Cyber Crime is Worldwide

- Estimated 431 million adults/year victims of cybercrime
- $388 billion in estimated time and money lost
- Not just a criminal issue but a national security issue
Cyber Crime – A Global Threat

- Cyber-based Terrorism
- Espionage
- Computer Intrusions
- Major Cyber Fraud
- Exploitation of minors
- National Security
Goals
Tied to Federal Government Investments/National Security Interests

- Mark Weatherford, DHS Undersecretary of Cybersecurity:
  - Achieving **operational excellence**
  - Strengthening **partnerships** between the public and private sectors, particularly in the area of information sharing
  - Building a powerful, cutting-edge cybersecurity **workforce**.
Fighting Cyber Crime thru Partnerships

- Operation Ghost Click
  - A criminal cyber ring used malware to infect 4 million computers in more than 100 countries.
  - 500,000 infections in the U.S. alone, including computers belonging to individuals, businesses, and government agencies such as NASA.
  - Thieves made over $14 million in illicit fees.

- Partnerships are critical to solutions
  
  **Government**
  - FBI
  - NASA OIG
  - Estonian Police
  - Dutch National Police
  - Internet Systems Consortium
  - National Cyber-Forensics & Training Alliance

  **Private Sector**
  - Mandiant
  - Neustar
  - Spamhaus
  - Team Cymru
  - Trend Micro

  **Education**
  - University of Alabama at Birmingham
  - Georgia Tech University
Shortage of Qualified & Certified Personnel

- A 2010 Report by the CSIS Commission on Cybersecurity for the 44th Presidency *A Human Capital Crisis in Cybersecurity*

  - Noted the shortfall in trained personnel
  - Called for expanded education & rigorous certification
Labor Market for Critical Occupations

Information Security Analysts, Web Developers, and Computer Network Architects

2010 Median Pay
- $75,660 per year
- $36.37 per hour

Entry-Level Education
Bachelor’s degree

Work Experience in a Related Occupation
1 to 5 years

On-the-job Training
None

Number of Jobs, 2010
302,300

Job Outlook, 2010-20
22% (> average)

Employment Change, 2010-20
65,700

Key Industries for These Jobs
- Computer Systems Design and Related Services
- Management of Companies and Enterprises
- Wired Telecommunications Carriers
- Management, Scientific &Technical Consulting Services
- Data Processing, Hosting, and Related Services

Top Employment States/Metro Areas
CA, TX, VA, FL, NY, MD, MA, WA, DC

Washington-Arlington-Alexandria 19,070
New York-White Plains-Wayne 13,800
Los Angeles-Long Beach-Glendale 9,100
Seattle-Bellevue-Everett 7,910
Dallas-Plano-Irving 7,510
Boston-Cambridge-Quincy 7,010
Minneapolis-St. Paul-Bloomington 5,890
Atlanta-Sandy Springs-Marietta 5,850
San Jose-Sunnyvale-Santa Clara 5,710
Chicago-Joliet-Naperville 5,680
Creating a Pipeline of Skilled Workers

- Partners in Business and Industry
- Federal Agencies
- Cyber Security Student
- Certified Industry Credential or Degree
- Career Pathways (CTE/STEM)
Meeting the Workforce Challenge

- The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence (CAE)
  - Producing a growing pipeline of professionals with IT expertise in various disciplines
  - 166 centers in 42 states
  - URI's Digital Forensics and Cyber Security Center (2012)
  - Creates cyber experts who help to protect national security and critical information infrastructure in both the private and public sectors
Start Early – Ensure STEM Foundation for All

Start Early (Pre-K thru Secondary) → Career & Technical Education Programs (Secondary thru 2- and 4- year Post-Secondary) → Labor Market Outcomes – Good Jobs

Security and Privacy

THE UNIVERSITY OF RHODE ISLAND
CYBERSECURITY SYMPOSIUM
Cyber Security Career Pathway

Baltimore Public Schools

Grade 9
Intro to Information Technology

Grade 10
HTML/JavaScript OR
Software & Computer Applications II OR
Database Applications

Grade 11
Visual Basic OR
Computer Science AP

Grade 12
Object Oriented Programming C++ OR
Computer Science AP
Maryland Programs of Study

- Computer Science and Cyber Security
  - Foundations of Computer Science
  - Computer Science Principles
  - Computer Science: Advanced Placement (AP)
  - CyberWatch: Microcomputer Operating Systems
  - CyberWatch: Ethics and the Information Age

- Pathway spans K-12 and postsecondary

- Dual credit – Industry certifications

- Strong partnerships: State, student organizations (competitions), Cyber-Watch, UMBC.
Resources for Furthering Cybersecurity

- Career opportunities and programs
- 31 emerging specialty areas
- Competencies and KSAs
- Internships & scholarships
- Teaching tools
- Hands-on experiences for students
- Examples of curriculum integration
- Competitions and cyber challenges
- Much more for parents, students, educators, employers and communities
Many of the challenges and competitions are stand-alone events or supplement curriculum.

Need to find ways for better integration into programs/curricula.
Virtual Cybersecurity Labs

- Government aims to establish a network of **virtual cybersecurity laboratories** that allow students and professionals alike to test out their latest cybersecurity technologies.
- The network of virtual cybersecurity labs will help provide easier, more coordinated access to the facilities to help test the technologies of tomorrow.
## Returns for Students Will Be There

### Computer and Information Technology

<table>
<thead>
<tr>
<th>OCCUPATION</th>
<th>ENTRY-LEVEL EDUCATION</th>
<th>2010 MEDIAN PAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and Information Research Scientists</td>
<td>Doctoral or professional degree</td>
<td>$100,660</td>
</tr>
<tr>
<td>Computer Programmers</td>
<td>Bachelor’s degree</td>
<td>$71,380</td>
</tr>
<tr>
<td>Computer Support Specialists</td>
<td>Some college, no degree</td>
<td>$46,260</td>
</tr>
<tr>
<td>Computer Systems Analysts</td>
<td>Bachelor’s degree</td>
<td>$77,740</td>
</tr>
<tr>
<td>Database Administrators</td>
<td>Bachelor’s degree</td>
<td>$73,490</td>
</tr>
<tr>
<td>Information Security Analysts, Web Developers, and Computer Network Architects</td>
<td>Bachelor’s degree</td>
<td>$75,660</td>
</tr>
<tr>
<td>Network and Computer Systems Administrators</td>
<td>Bachelor’s degree</td>
<td>$69,160</td>
</tr>
<tr>
<td>Software Developers</td>
<td>Bachelor’s degree</td>
<td>$90,530</td>
</tr>
</tbody>
</table>

Bureau of Labor Statistics – Occupational Profiles
Closing Thoughts

- Start early
- STEM foundation is key for all
- Ethics are critical
- Cross-sector partnerships ensure relevance
- Bringing real-world cyber security challenges into the classroom can be improved
- Existing funding can be leveraged
Frank Zaborowski
Director
Competition Operations, CyberPatriot
Air Force Association’s CyberPatriot
The National High School Cyber Defense Competition

Program Update
May 2013
Cyber is everywhere in America

- Finance
- Manufacturing
- Logistics
- Transportation
- Retail
- Public Safety
- National defense
• National cyber security can’t exist without strong, indigenous cyber workforce
• We aren’t graduating enough STEM scientists, technical grads, engineers, math majors, cyber experts
• We must motivate high-school youth to pursue STEM paths

When compared to other nations, the math and science achievement of U.S. pupils and the rate of STEM degree attainment appear inconsistent with a nation considered the world leader in scientific innovation. In a recent international assessment of 15-year-old students, the U.S. ranked 28th in math literacy and 24th in science literacy. Moreover, the U.S. ranks 20th among all nations in the proportion of 24-year-olds who earn degrees in natural science or engineering.

2008 Congressional Research Study
“Science, Technology, Engineering, and Mathematics (STEM) Education: Background, Federal Policy, and Legislative Action”
• Cybersecurity jobs on average offer a premium of about $12,000 over average for all computer jobs.

• Average salary for cybersecurity jobs in 2012 was $100,733 versus $89,205 for all computer jobs.

• Demand for cybersecurity professionals over past five years grew 3.5 times faster than demand for other IT jobs and about 12 times faster than for all other jobs.

   Source: Computerworld, March 7, 2013

• Over next year, need for 330,000 more IT security professionals worldwide.

Julie Peeler, Director of ISC2 Foundation
What doesn’t work… What does…

• Academic instruction is important, but students aren’t particularly inspired by more class time, more lectures

• Multi-media instruction is a good tool, but they see plenty of that

• What excites, motivates: A well-organized, well-structured, competition
CyberPatriot Is...

1. The national high school cyber defense competition.
2. Carefully structured to excite, educate, and motivate participants.
3. Designed to instill in all participants the importance to our nation of cyber, cyber security, and good computer security practices.
4. Designed to motivate all participants to consider STEM academic disciplines to meet our nation’s needs.
5. Designed to motivate many participants to become the next generation of cyber defenders and our nation’s “digital workforce.”

“We will begin a national campaign to promote cyber security awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century.”

President Obama, May 2009
CyberPatriot Is Not...

1. “Hacker training” We don’t teach “hacking” tools or techniques, and “hacking” in competition is strictly forbidden.

2. A recruiting tool for the Air Force, the Department of Defense, or the Federal government This is about building a strong national foundation for cyber skills throughout our high schools.

3. Boring academic instruction CyberPatriot is designed with extremely high fun and excitement quotients.
History

CP-I: Feb 2009
Concept Demonstration (Orlando, Florida)
Eight teams (7 AFJROTC/1 CAP), all from Florida

CP-II: Apr 2009 – Feb 2010
Pilot Deployment
200+ teams (AFJROTC/CAP) – 42 States & Japan

CP-III: Apr 2010 – April 2011
First National Deployment
All-Service Division: JROTC of all Services, CAP
Open Division: Any high school
661 teams, 48 states

CP-IV: Apr 2011 – April 2012
Second National Deployment
All-Service Division: JROTC of all Services, CAP
Open Division: Any high school
1,014 teams, 50 states, Canada

CP-V: Apr 2012 – March 2013
Most Recent Season
All-Service Division: JROTC of all Services, CAP, U.S. Naval Sea Cadet Corps
Open Division: Any high school
1,225 teams, 50 states, Canada

CP-VI: Apr 2013 – March 2014
Upcoming Season
Open Division: Any high school
All-Service Division: JROTC of all Services, CAP, U.S. Naval Sea Cadet Corps
Goal: 3,000 teams
Team Structure

• **Coach** (Adult Leader): Supervises, chaperones team. Usually a teacher.

• **Mentor** (Technical Advisor)(Optional): Particularly useful when coach not cyber-savvy. Helps teach cyber concepts. AFA helps find them.

• **Competitors**: 2-5 students, 9th-12th grade, minimum age 13.

National Finals Competition teams consist of six competitors (five primary and one alternate), one coach, and one chaperone.
Two Competition Divisions

Open Division
- Open to any high school
  - Public, private, parochial, magnet, home-school
- Highly valued CyberPatriot competition attributes:
  - Technical/STEM education
  - Career preparation/development
  - Teamwork
  - Goal-achievement

All Service Division
- Open to any JROTC unit
  - Army, Navy, Air Force, Marine Corps
  - Naval Sea Cadet Corps
- Open to Civil Air Patrol cadet squadrons and composite squadrons
- Highly valued CyberPatriot competition attributes:
  - Teamwork
  - Goal-achievement
  - Leadership
Skills Participants Learn

- Leadership and teamwork
- Creative and analytical problem solving
- Non-technical cyber principles (e.g. —social engineering, phishing, vishing, spear-phishing, etc.)
  - “Netiquette”
  - Cyber safety
  - Cyber hygiene
- Computing and networking principles
  - Operating systems
  - Network topologies
- Foundational cyber security principles
  - Cyber and system vulnerabilities
  - Network topology
  - Vulnerability remediation
  - Technical threats
What Participants See

CyberPatriot Competition System

Property of the
Air Force Association

Do not distribute without permission of the Air Force Association.
CyberPatriot Round 1 Image

Report Generated At: 10/17/12 18:58:19 Coordinated Universal Time

Approximate Running Time: 16:29:04

Current Team ID: 869F6E18F

70 out of 100 points received

Connection Status: GOOD

Internet Connectivity Check: OK
CyberPatriot Connection Status: OK
CyberPatriot Score Upload Status: OK

14 out of 20 known issues fixed:

An account lockout threshold has been set in the account policy

What Participants See
CP Growth

- Surge in registrations:
  - All Service Division: +26%
  - Open Division: +113%
- Strong growth in female and underrepresented populations
- Canadian presence at National Finals Competition
- CyberPatriot Centers of Excellence established
  - Enhanced focus, training, support
    - #001: Los Angeles Unified School District
    - #002: City of San Antonio, Texas
    - #003: Spokane Public Schools
    - #004: Rose State College, Oklahoma City
CP-V National Champions

All Service Division: Marine Military Academy Harlingen, Texas
Open Division: Chantilly Academy, Chantilly, Virginia
Funding Sources

Tiered Sponsorships

Presenting Sponsor

NORTHROP GRUMMAN

Foundation

Cyber Diamond

at&t

CISCO

Microsoft

Raytheon

USA TODAY EDUCATION

Cyber Gold

splunk

URS

Cyber Silver

EMBRY-RIDDLE Aeronautical University

K2 Share

LINCOLN LABORATORY

University of Maryland University College
The CyberPatriot
Middle School Program
1. We need to reach students earlier to effectively shape their education and career choices and draw them to math and science.

2. Youth need to be “immunized” against the growing on-line threats they face.

3. A strong middle school STEM presence will draw more high school students to high school programs.
Middle School Considerations

- Very different population
  - Different learning processes
- Statutory implications
- Enormous opportunity
  - 3x schools/students
  - Numbers will be a challenge
  - Ability to draw more females and minorities sooner
- Parental engagement different
• **Prime Pilot (LAUSD):** Late summer 2013
  - ~12 schools
• **Full Pilot:** October 2013
  - COEs (~50-100)
• **Full Deployment:** 2014-2015 school year
CyberPatriot is contributing to reversing the STEM shortfall
  – ~15,000 direct participants in 4 years
  – ~150,000 broad contacts in 4 years
CyberPatriot is placing young people on a path to educational, vocational, and professional success in an area of vital importance to our nation
CyberPatriot is reaching underrepresented populations and giving them opportunities they likely would never have had
Ours is a “target rich” environment
  – 40,000 high schools in America
This isn’t about AFA
This isn’t about the military
This isn’t about national defense

This is about a way of life
Victor Fay-Wolfe, Ph.D.
Professor
Department of Computer Science and Statistics
University of Rhode Island
The Open Cyber Challenge Platform*

Dr. Victor Fay-Wolfe, PhD
Director, URI Digital Forensics and Cyber Security Center

* Supported By The U.S. National Science Foundation grants:
  • Federal Cyber Service Scholarship For Service Program: Award 1241515
  • Research Experience For Undergraduates: Award 1004409
Problem

- Need for realistic, up-to-date, hands-on ways to teach cyber security.

- **Cyber challenges** – (team defends a real network data center from attacks) been proven effective in events and training.

- No low-cost option for establishing cyber challenge platform for high schools and colleges to use in their curriculum.
Current Cyber Challenges

- Some are restricted to government-only
  - Xnet
  - National Cyber Range
- Commercial packages are expensive
  - >$100K plus maintenance
- Some are created from scratch each time
  - National Collegiate Competition
  - DEFCON Capture The Flag
- Challenges are typically “free for all” – not designed to be configurable to test specific concepts
Solution

- Build cyber challenge \textit{platform}
- Free/low-cost software
- Reasonable hardware requirements
- Architected to be configurable by organizations
- Open source so new configurations can be released back to the community to keep challenges current
OCCP Architecture

- **Red Team** – attacks network to steal data and deny services
- **Gray Team** - is normal traffic and service requests that must be maintained
- **Blue Team** - defends network (patches vulnerabilities, etc)
- **White Team** – officiates and scores challenge
Uses In Cyber Security Teaching/Training

**Network Defense** – Blue Team is students, Red Team is scripted attacks. Negative points assigned to Blue for data stolen and services denied.

**Penetration Testing** – Red Team is students, Blue Team is scripted. Positive points assigned for data stolen and services denied.

**Secure Programming** – Blue Team is student programmers, Red Team is scripted attacks (e.g. SQL injection). Negative points assigned for data stolen and services denied.

**Digital Forensics** – Red Team is scripted attack, Blue Team of students must find what data was stolen and who did it.
Virtual Target Network (VTN)

- VMWare vSphere package of virtual machines on a virtual network
- Runs on one low-end/moderate physical computer/server
- Virtual internal network, external (Internet) network, private white team network
- Current network defense scenario uses “metasploitable”, which is a virtual web server with vulnerabilities as part of the metasploit project.
Blue Team

- Scripts in Penetration Testing
- In Network Defense:
  - Blue Team gets short “network administrator” document showing network architecture, passwords, etc.
  - Blue Team is given pre-training on the specific tools and components used (e.g. pfSense firewall)
  - Blue Team is provided a “network administrator” virtual desktop with all required tools (and possibly an Internet connection to get other tools and documentation). E.g.
    - WireShark
    - Interface to Snort Intrusion Detection
    - Putty and remote login tools
  - Blue Team has an email account on the network administrator desktop to which hints can be emailed
Blue Team Tools

Blue Team member using web interface from the Blue network administrator desktop to fix a weak firewall rule

Blue Team member using web interface from the Blue network administrator desktop to examine the mail server system log
Red Team – Attacks Network/Data Center

- Scripted for network defense, secure programming and forensics
- Human for penetration testing
- For current network defense scenario:
  - Exploits come from Metasploit (open source) library
  - Configuration file specifies attacks and timing
  - Ruby (scripting language) scripts execute exploit attempts
  - Red scripts report success to White scripts for scoring
Red Team In Demo

Attacks Run
- Brute force login
  - ssh
  - rlogin
- Web application exploit
  - tikiwiki php exec
- Exposed internal services

Post Exploit
- Privilege escalation
- Backdoor accounts
- Stolen passwords
- Website defacement
- Erase logs
Gray Team – Normal Service Requests

- Ruby scripts generate traffic
- What protocols, timing/density of requests, and specific VTN services are specified in configuration file
- Use of standard protocol libraries (e.g. http library) to generate traffic under Ruby scripting
- Gray scripts report to White Team successful receipt of services for scoring purposes
White Team – Scores and Officiates

- Uses Nagios (open source network monitoring) to get status of services
- Uses Nagios messages to receive updates from the other teams
- In Network Defense scenario:
  - Red team reports successful exploits (negative points)
  - Gray team report successful services (positive points) and denied/incorrect service (negative points)
  - Provides “hint” communication for White Team humans to help Blue Team humans
- Displays running score
- Provides monitoring of all parts of the system by White Team human administrators
Uses In Cyber Security Teaching/Training

**Network Defense** – Blue Team is students, Red Team is scripted attacks. Negative points assigned to Blue for data stolen and services denied.

**Penetration Testing** – Red Team is students, Blue Team is scripted. Positive points assigned for data stolen and services denied.

**Secure Programming** – Blue Team is student programmers, Red Team is scripted attacks (e.g. SQL injection). Negative points assigned for data stolen and services denied.

**Digital Forensics** – Red Team is scripted attack, Blue Team of students must find what data was stolen and who did it.
Status

- University of Rhode Island is building the OCCP under funding from the National Science Foundation

- Low cost/free hardware and VMware environment

- URI will release OCCP free and open source on web portal

- First network defense scenario developed and alpha tested
The Open Cyber Challenge Platform*

Dr. Victor Fay-Wolfe
Director, URI Digital Forensics and Cyber Security Center

Web: http://dfcsc.uri.edu
OCCP Project: http://dfcsc.uri.edu/research/occp_demo
Panel: Cyber Challenges for Workforce Development

Introductions and Facilitator: Lisa DiPippo, Ph.D., Associate Professor, URI Department of Computer Science and Statistics

Johan Uvin, Ph.D., Deputy Assistant Secretary of Policy and Strategic Initiatives, Office of Vocational and Adult Education, U.S. Department of Education

Frank Zaborowski, Director, Competition Operations, CyberPatriot

Vic Fay-Wolfe, Ph.D., Professor, URI Department of Computer Science and Statistics

Panel Q & A Discussion