Securing the eCampus 2.0
ISTS, Dartmouth College

Breakout Panel Sessions
12 November 2008

SISMAT: Secure Information Systems Mentoring and Training

mlocasto@gmu.edu
SISMAT Panelists

- Scout Sinclair, Dartmouth College
  - Motivation, overview

- Michael E. Locasto, George Mason University
  - Course content & structure

- Douglas C. Madory, DHMC
  - Satisfied customer

- Adam Goldstein, PKCS
  - Satisfied customer
SISMAT Overview
SISMAT Course Structure

- Each day structured such that:
  - Two morning “lectures” or a guest speaker
  - Two afternoon labs
- Guest Speakers
  - Doug, Scout, Scott Rea, C. Shepherd (NSA), J. Marchesini
- Agenda/Syllabus/Curriculum
  - Maintained dynamically on a wiki
  - Links to readings, points that came up in “lecture”, and extra help / Web sites for labs
The STUDENTS
  - Small group, bright, exceptional, motivated
  - John Marchesini
    - Multiple days, extra expert & pair of hands
    - Author of one of the texts
  - Discussion of ethics on the last day

Professional Development Weekend
Professional Development Weekend

- Invite & host faculty mentors
- Brainstorm ways to help weave in and deliver information security content in “regular” courses
- Set agendas for mentored research projects
- Lay groundwork for future recruiting
SISMAT Conception
Scout Sinclair, Dept. of Computer Science, Dartmouth College
My life as an undergrad

Classes! (and Great Learning of Important Things)
Workstudy: helpdesk + CS sysadmin
Junior year: security reading course
Senior year: no security thesis advisor
On to graduate school...

Dartmouth is a research university disguised as a small liberal arts college. Staff! And Experts! And research! **Question:** how can I bring these resources back to Wellesley? (Or, how can Dartmouth ISTS reach out to smaller area institutions?)
Secure Information Systems Mentoring and Training

**Undergrads.** (Training)
The “**real world.**” (Internships)
**Faculty.** (Mentor-the-mentors for student research projects)
What is Dartmouth-Hitchcock?

- DHMC consists of over 8000 staff on a 225 acre campus in Lebanon, NH and consists of:
  - Mary Hitchcock Memorial Hospital (400 beds)
  - The Dartmouth-Hitchcock Clinic (a network of more than 900 primary and specialty care physicians located throughout New Hampshire and Vermont)
  - Dartmouth Medical School
  - Veterans Affairs Regional Medical and Office Center in White River Junction, VT.
7,000 Networked PCs & 3,000 Laptops
450 Servers (150 Virtual)
100 Terabytes of Data Storage
11,000 Blitzmail Accounts
Data Network Connects 54 Sites in Three States
Clinical Information System (EMR)
- 7000+ accounts
D-HDRS Runs 3,000 Web Reports & 4,000 Ad Hoc Queries/Month
50,000 Statements Processed/Month
What does IS Security do?

- Setting IS Security Policy
- User Education and Awareness
- Coordination and Maintenance of Contingency Planning
- Security Auditing
- General IS Security consulting and analytical support.
SISMAT Student – Jonah Berquist

- Rising Junior at Evergreen State College
- Computer Science Major (equivalent)
- Key Contributions
  - Automating account auditing processes
  - Developing security education resources
  - Research paper entitled, “Authentication Methodologies in Academic Medical Centers”
    - Interfaced with national Association of Academic Medical Centers
    - Developed and executed survey
    - Results will form basis of publication
PKCS and SISMAT

Adam Goldstein
IT Security Engineer
Peter Kiewit Computing Services
Dartmouth College
PKCS CSI and SISMAT

- Cyber-security Initiative (CSI) started in Summer 2006
- CSI is an ongoing collaboration between PKCS, and faculty and students from Computer Science, Thayer School of Engineering, and ISTS
- Focused on coordinating research interests with projects aimed at improving the security of College IT systems
SISMAT Internship

- Two interns for two months over the summer
- Projects included:
  - Assisted in developing an automated SecureLinux installation program
  - Designed and implemented high speed network traffic capture device and intrusion detection system
Developed, tested, and documented process for automated secure Linux server installations
Customized “Kickstart” installation
Worked with PKCS system administrator to incorporate post-install hardening scripts
Developed and documented high speed (gigabit) traffic capture and analysis system using low cost servers.

Implemented and tuned IDS for network core

Developed custom capture and traffic analysis scripts
CSI – Student Operations Group

- Based on success of SISMAT
- 6 undergraduate (10’s and 11’s) interns
- Working in Berry Machine Room under guidance of PKCS Staff and CS Faculty
- Assist in security monitoring and attack analysis