Information Assurance Program at West Point

Daniel-Ragsdale@usma.edu    John.Hill@usma.edu
Scott.Lathrop@usma.edu      Gregory.Conti@usma.edu
USMA Information Assurance Program

IA Research Center (ITOC)

- NSA Support
- USMA CERT
- Information Warfare Lab (IWAR)
- Cyber Defense Exercise
- Courses and Curriculum
- IA Workshop and Conferences
- Outreach/Research
- Summer Internships
- Student IA Club (SIGSAC)

Institutional Support

Quality Personnel

Tremendous Interest

IA Savvy Personnel

2003

Duty, Honor Country
USMA IA Program

IA Research Center (ITOC)

- IA Conferences
- Outreach/Research
- Summer Internships
- Student IA Club (SIGSAC)
- Courses and Curriculum
- Cyber Defense Exercise
- USMA CERT
- Information Warfare Lab (IWAR)
- NSA Support

Duty, Honor Country
USMA IA Program Mission


  ~LTC Dan Ragsdale  
  ITOC Director
Information Assurance Courses

- **Primary**
  - CS482 *Information Assurance*
  - IT460 *Policy and Strategy of Cyberwar*
  - MA489 *Cryptography*
  - LW489 *Cyberlaw*

- **Supporting**
  - CS484 *Computer Networks*
  - IT105 *Introduction to Information Technology*
  - IT305 *Introduction to Military Information Technology*

- **Other computer science courses**
  - Have IA awareness woven into them
Student IA Club

• ACM SIGSAC Chapter
• Formed January 2001
• 450+ Members
  – Interdisciplinary (All Academic Departments Represented)
• Won 2001-2002 ACM Outstanding Activities Award
  – SIGSAC IWAR Lab
  – Speakers
  – Community Service
• www.itoc.usma.edu/sigsac/
Summer Internships [1 of 2]

- NSA - Network Evaluation Intern Program
- US Secret Service, Electronic Crimes Branch – Honeypot research
- Joint C4ISR Battle Center - Enhanced C4ISR Homeland Security Operations (ECHO)
- ITOC - Information Assurance Vulnerability Alert (IAVA) Compliance Prototype
- AMC-DOD - UAV multi-mission payload analysis
- Microsoft – Microsoft Intern
Summer Internships [2 of 2]

- US Army Information Technology Agency - Network Security Services - Pentagon
- Livermore National Laboratory - UAV Simulation
- High Performance Computing Modernization Office - Network Monitoring Initiative
- RCERT Pacific - Intrusion Detection and Analysis
- 1st IO Command (ACERT, RCERT Korea & Europe) - Intrusion Detection and Analysis
- AMC-DOD - Crowd Simulation in Realistic Simulations
Guest Speaker Program

- Government
- Military
- Academia
- Business
ITOC Research Topics

• Information Technology and Operations Center
  – Decision Support
    • Automated Imagery Analysis
    • Automated Terrain Analysis
  – Information Assurance
    • Network Deception (Honeynets / Network Camouflage)
    • Open Source Tool Employment
    • Intrusion Detection and Response
    • Information Assurance Simulation
    • Network and Computer Forensics
    • Wireless Security
ITOC Outreach Projects

- **Information Assurance Vulnerability Alert (IAVA) Compliance Prototype** – NSA, 1st IO Command
- **Network Deception (Honeynets)** - 1st IO Command, US Secret Service
- **Information Assurance Curriculum and Training Development** – NSF, 1st IO Command
- **Classroom XXI** – Army Training and Doctrine Command
- **Military Academy Attack Defense Network (MAADNet)** – Office of the Secretary of Defense, NSF
- **Network Forensics and Email Recovery** – US Secret Service
- **Wireless Security**
- **T4IA** – NSF
4th Annual IEEE Information Assurance Workshop
June 18-20, 2003
West Point, New York

Sponsored by IEEE and NSA
http://www.itoc.usma.edu/workshop/
Information Warfare Analysis and Research (IWAR) Lab

• Isolated network
  – Wide variety of target machines
  – Full 18 seat classroom
  – Dedicated lab director

• Used to support courses
  – CS482 Information Assurance (primary user)
  – SS490 Policy and Strategy of Cyberwar (primary user)
  – CS484 Networks (projected)
  – IT105 Intro to Information Technology (awareness)
  – IT305 Intro to Military Information Technology
IWAR Laboratory Design Goals

• Realistic
  – Provide a “real world” signature
  – Shared Resources
  – Soft and Hard targets

• Heterogeneous
  – Operating Systems
  – Network Protocols/Equipment
  – Offensive and Defensive Tools

• Reconfigurable
  – Ghost Images
  – Removable hard drives
IWAR Tools and Capability

- Firewalls
- Malicious Active Content Exploits
- Vulnerability Scanners
- Viruses and Worms
- Cryptography and Encryption
- Trojan Horses
- Application and Protocol Wrappers
- Buffer Overflow Exploits
- Honey Pots/Honeynets
- Access Control Methods

- Protocol Exploits
- Integrity Maintenance Systems
- Network Sniffers
- Mail and Protocol Spoofers
- Distributed DoS Tools
- Intrusion Detection Systems
- Race Condition Exploits
- Password Cracking Software
- Forensics Analysis Tools
- Port Scanners
IWAR Networks
IWAR-in-a-Box

Information Warfare Analysis and Research Laboratory

Duty, Honor Country
Cyber Defense Exercise

• Sponsored by the National Security Agency, Director of Information Assurance

• General Concept
  – Defense of a network against an adversarial force
  – Blue Forces
    • US Service Academies and NPS
  – Red Forces
    • National Security Agency
    • 92nd Information Warfare Aggressor Squadron
    • 1st Information Operations Command
  – White Cell
    • Carnegie Mellon
Cyber Defense Network
Cyber Defense Exercise

• Key Educational Aspects
  – Competitive
  – Active learning
  – Project-based

• Developmental Areas
  – Leadership Ability
  – Planning Ability
NSA

- Full Time NSA Liaison
- IA Conference Sponsorship
- NSA Trip
- NSA Internships
- Intelligence Community Access
- CDX Support
- Sabbaticals

- NSA Information Assurance Center of Excellence Program
- NSA Information Assurance Director’s Trophy
Preparation for War

“On the fields of friendly strife are sewn the seeds that upon other fields on other days will bear the fruits of victory…”

GEN Douglas MacArthur
“On the networks of friendly strife are sewn the seeds that upon other networks on other days will bear the fruits of victory…”

MAJ Greg Conti
USMA IA Program

IA Research Center (ITOC)

- NSA Support
- IA Conferences
- Usma CERT
- Information Warfare Lab (IWAR)
- Outreach/Research
- Cyber Defense Exercise
- Summer Internships
- Student IA Club (SIGSAC)
- Courses and Curriculum
USMA IA Program

Institutional Support

IA Conferences
Outreach/Research
Summer Internships
Student IA Club (SIGSAC)

IA Research Center (ITOC)

NSA Support
USMA CERT
Information Warfare Lab (IWAR)
Courses and Curriculum
Cyber Defense Exercise

Quality Personnel

Tremendous Interest

Duty, Honor Country

IA Savvy Personnel
Questions?

• … and a reminder!

4th Annual IEEE
Information Assurance Workshop
June 18-20, 2003
West Point, New York

Sponsored by IEEE and NSA
http://www.itoc.usma.edu/workshop/