Air Force Institute of Technology

Educating the Future Leaders of America’s Armed Forces

AFIT
Information Assurance
Education and Research

Gregg H. Gunsch, Ph.D., PE, CISSP
Center for INFOSEC Education and Research

Integrity - Service - Excellence
AFIT VISION

A premier team providing universally respected engineering and management education to sustain the technological supremacy of America’s Air and Space Forces

AFIT MISSION

Provide responsive, defense-focused graduate and continuing education, research, and consultation to improve Air Force and joint operational capability
AFIT Background

- First degrees awarded in 1956 -- North Central and ABET accreditation
- Over 14,500 degrees granted (920 Bachelors, 13,406 Masters, and 333 Doctoral)
- Eleven alumni have become astronauts
- Nine Fellows of national professional societies on faculty
What is AFIT’s Graduate School of Engineering and Management?

- Graduate education and research institution
  - Masters and Ph.Ds
    - Aero/Astro/Computer/Electrical Engineering, Computer Science, Engineering Physics, Operations Research, Engineering Management
    - 18-month Masters, 36-month Ph.D
  - U.S. military (officer and enlisted), DoD civilians, international officers, non-DoD civilians (U.S. citizens)
- Located at Wright-Patterson AFB in Dayton Ohio
- Co-located with Air Force Research Laboratory, Air Force Materiel Command, and the National Air Intelligence Center
Current USAF IO Doctrine

Information Superiority

Information Operations

Information In Warfare (Gain and Exploit)
- ISR
- Weather
- Precision
- Navigation/Positioning
- Other Information Collection and Dissemination Activities (Information Exploitation)
- (Electronic Support)

Information Warfare (Attack and Defend)
- Offensive Counterinformation
  - PSYOP
  - Electronic Warfare
  - Military Deception
  - Physical Attack
  - Information Attack
- Defensive Counterinformation
  - Information Assurance
  - OPSEC
  - Counterintelligence
  - Counter PSYOP
  - Counterdeception
  - Electronic Protection
AFIT has a long history of teaching, research, and consulting on Information Warfare (IW) and Information Assurance (IA) topics

- Command/Control/Communications
- Electronic Warfare and Combat
- Radar/Microwave/Lasers/Infrared
- Optics/Electro-Optics/Imaging
- Data Security/Cryptography
- Artificial Intelligence
- Pattern/Target Recognition
- Signal Processing
- Computer Networking
- DoD Internet Dependencies - DOS
- Access Control List Performance
- Data Mining
- Computer Operating Systems
- Database Reliability
- Modeling and Simulation
- Decision and Risk Analysis
- Space Surveillance and Intelligence
- Analyst Decision Support Systems
- Information Resource Management
- Information Engineering
- Systems Analysis and Design
- Steganography
- Satellite Communications Analysis
- IW Targeting
Master’s Degree Program
Computer Engineering, Computer Systems or Computer Science
Information System Security/Assurance specialty

- Satellite Communications (EENG 571)
- Distributed Software Systems (CSCE689)
- Design Principles of Computer Architecture (CSCE 692)
- Intro to Software Engineering (CSCE 593)
- Advanced Microprocessor Design Lab (CSCE 687)
- Design and Analysis of Algorithms (CSCE 586)
- Introduction to Artificial Intelligence (CSCE 523)
- Database Systems (CSCE 546)

Introduction to IW (CSCE 525)

Information Systems Security, Assurance & Analysis I (CSCE 625)

Information Systems Security, Assurance & Analysis II (CSCE 725)

Master’s Thesis

Computer Communication Networks (CSCE 654)

Data Security (CSCE 544)

- Introduction to Database Systems (CSCE 546)
- Information Assurance Education

Research-Capable, IA/IW-Knowledgeable, Independent Thinker

- Introduction to IW (CSCE 525)
- Information Systems Security, Assurance & Analysis I (CSCE 625)
- Master’s Thesis

Research-Capable, IA/IW-Knowledgeable, Independent Thinker
ISS/A Sequence

Required Courses
- CSCE 525 Introduction to Information Warfare
- CSCE 625 Info Systems Security, Assurance & Analysis I
- CSCE 725 Info Systems Security, Assurance & Analysis II

Recommended Electives
- CSCE 523 Artificial Intelligence
- CSCE 544 Data Security (highly recommended)
- CSCE 654 Computer Communication Networks
- CSCE 689 Distributed Software Systems
- EENG 571 Satellite Communications
- EENG 580 Introduction to Signal Processing
- EENG 669 Digital Communications I
Enrollment in ISS/A Courses

- CSCE525 - Intro to IW
- CSCE625 - ISS/A I
- CSCE725 (626) - ISS/A II

Yearly enrollment from 1997 to 2002.
Information Assurance Education

• One of 36 NSA designated Centers
• Masters-level education
  • Majors with specialization in IA
    • Computer Engineering/Science/Systems
    • Electrical Engineering
    • Information Resource Management
    • Information Systems Management
    • Operations Research
• Ph.D-level education
  • Computer Engineering/Science
  • Electrical Engineering
Certification

Students Completing the Following Courses
• CSCE 625  Info Systems Security, Assurance & Analysis I
• CSCE 725  Info Systems Security, Assurance & Analysis II
• CSCE 544  Data Security
• CSCE 654  Computer Communication Networks
• CSCE 689  Distributed Software Systems

Are Eligible for Certification as an

Information Systems Security
(INFOSEC) Professional

Under the National Security Telecommunications
and Information Systems Security Instruction,
NSTISSI No. 4011

http://www.nsa.gov/ isso/ programs/ nietp/ corseval.htm
• Thesis is required for all Masters students
  • Year-long investigations
  • Topics include
    • Vulnerability analyses
    • Intrusion detection systems
    • Wireless systems security
    • Threat analyses and classifications
  • 98% of Masters theses are DoD sponsored

• Ph.D. research
  • Two-year investigations
  • Topics include
    • Networks security
    • Intrusion/threat detection and classification
Some Research Opportunities

- Computer Network/Host Intrusion Detection
- Blind Steganography Detection
- Computer and Network Forensics
- Wireless Network Security
- Insider Threat Trend Analysis
- Detection/Representation of Tainted Information
- Modeling User Trust and Inducing Skepticism
- Operator/Analyst Support
- Satellite Communications Analysis
- Network Modeling and Security
Supporting Facilities

- Laboratory for Information System Security/Assurance Research and Development (LISSARD)
  - Contains isolated network supporting 10+ high-end PCs and Sparc Stations
  - Safe environment for experimentation with computer security tools and techniques
    - penetration testing
    - vulnerability analysis
    - intrusion detection
    - computer forensics
- Network Communications Lab
- Wireless Networks Lab
- New in 2003
  - Cyber Defense Network Lab
Questions?

• Dr. Rick Raines
  • Richard.raines@afit.edu
  • 937 255-3636 x 4715

• Maj Rusty Baldwin, Ph.D
  • Rusty.baldwin@afit.edu
  • 937 255-3636 x 4612

• Dr. Gregg Gunsch
  • Gregg.Gunsch@afit.edu
  • 937 255-6565 x 4281