Information Assurance
Training & Awareness
Products & Resources

George Bieber
Defense-wide IA Program (DIAP)
(703) 602-9980
George.Bieber@osd.mil
Agenda

Training and awareness opportunities available to federal employees
Army Reserve Readiness Training Center (ARRTC) - 1

Ft McCoy, Wisconsin: http://arrtc.mccoy.army.mil

Open to federal employees; contact
RIM@arrtc-exch.mccoy.army.mil
or call
608-388-7307 or 1-800-982-3585, x 7307

◆ Physical Security Basic Course
◆ Security Manager Course
◆ DITSCAP (DOD Information Technology Security Certification and Accreditation Process)

Scot Wiedenfeld
scot.wiedenfeld1@us.army.mil
Comm: 608-388-7293
DSN: 280-7293
Army Reserve Readiness Training Center (ARRTC) - 2

- Systems Administrator/Network Manager Security Course (2 weeks)
  - Policies, Laws and Ethics
  - JAG/MI Briefing (Current Threats)
  - Windows NT 4.0/2000 Security
  - Solaris, Unix Security
  - Understanding C2 Attack Technologies
  - Web Security & Encryption
  - Communications Security
  - Cisco Router Security
  - Intrusion Detection Systems
  - Deploying Firewalls

- Computer Network Defense Course (2 weeks)
  - C2 Attack Technologies
  - Intranet / Extranet / Web
  - Footprinting & Enumeration
  - Forensic Examination & Preserving Evidence
  - Countermeasures
  - Advanced Communication Security
  - Advanced Cisco Router Security
  - Intrusion Detection Systems
  - Sidewinder Firewalls
  - “Latest & Greatest”
Privacy Protection in the Information Age

http://www.don-imit.navy.mil

◆ Department of the Navy CIO CD-ROM
◆ Federal Reserve Bank video: Its Your Identity: Protect It
◆ Resources
  ◆ Public Privacy Laws and Legal Guidance
    ◆ Public Laws
    ◆ Executive Guidance
    ◆ Federal Reports
  ◆ Reading List
◆ Web-sites
◆ Brochures
◆ Templates
Resource to help inform the DoD and other members of the Government about Critical Infrastructure Protection, CIP-related documents, and educational programs

Topics

- OSD CIP (Mission, Contacts, Strategy, Terrorism Timeline 88-01)
- Training
- CIP Team
- Studies (Federal, Training Gap Analysis, Other)
- Practices
- References (Executive Orders/Directives, Federal Regulations, Publications, Slide Shows, Glossary)

CIP POC for training and awareness: LtCol Will Smith; wilburn.smith@osd.mil
Critical Infrastructure Protection (CIP-101) WBT

- In development by OASD CIP and DISA
- When completed will be available at http://iase.disa.mil

- Provides basic awareness level information - CIP 101
- Contents
  - CIP Overview
    - What is CIP
    - Why is it important
    - Critical infrastructures
  - CIP Organization
    - National
    - DOD
    - Relationships
  - DOD responsibility for CIP
    - DOD Infrastructure Sectors
  - DOD CIP Life-Cycle
- POC for CIP training & awareness: LtCol Will Smith
  wilburn.smith@osd.mil
Commercial CBTs

- SmartForce (formerly CBT Systems):
  http://www.smartforce.com

- NETg:
  http://www.netg.com
  - Netg is partner of new government golearn.gov training site
Public Broadcasting Service (PBS); FRONTLINE series $20.00 (60 min)

http://www.pbs.org

Search on “Science and Technology”

Who are hackers

Risks of the Internet’s vulnerabilities

Who’s responsible for security

How to be vigilant

Interviews with hackers and security experts

Also at the site:

Video transcript

Transcript of live chat that followed original broadcast

Clips from the video
3 vignettes; Internet works both ways

Web sites can be set up to:
- Collect information
- Track activities
- Take over your computer

Web sites can be customized, altered/mirrored to:
- Send/release malicious code
- Messages to misinform/deceive

Types of information that can be collected
- Cache
- Names, addresses, phone numbers
- Credit card numbers
- Bank account numbers

Steps you can take to increase your security
Warriors of the Net

* Animation
* Copyright 1999 Ericsson Radio Systems AB
* Free use for information purposes and non-commercial use
* Introduces internet/e-mail technology: packets, routers, firewalls

Download at: http://www.warriorsofthe.net
Awareness 2001: A Security, Counterintelligence and OPSEC Update

- Burning Issues (USGov) (14 min)
  - Intersection of classified and unclassified environments

- Web Content Vulnerabilities (25 min)
  - Briefing by Joint Web Risk Assessment Cell (JWRAC)
  - Advice on how to protect information posted to the internet
  - Applicable to all organizations

- D*I*C*E 2001 (38 min)

- In the Public Domain (10 min)
Betrayal - NCIX

The National Counterintelligence Executive (NCIX)
http://www.ncix.gov

◆ **Betrayal: Protecting Industry Trade Secrets** (17 min)
  ◆ Insider threat
  ◆ Highlights the Avery Dennison/Four Pillars case, a joint effort by US Industry and the US Government to successfully combat economic espionage.
  ◆ Distributed by Filmcomm Inc., 641 North Avenue, Glendale Heights, IL 60139, phone 800-944-9134.
  ◆ $13.85 per copy, (includes shipping and handling)
IA Scholarship Programs

- DoD Information Assurance Program (IASP)
  - Administered by NSA
- National Science Foundation Scholarship for Service Program
  - Administered by OPM
  - Open to all federal Departments and Agencies

Visit the Scholarship Booth Today
IA Centers of Academic Excellence (CAEs)

32 Public / Private Non-DoD Institutions
- Carnegie Mellon
- Florida State
- George Mason U
- Idaho State
- Iowa State
- James Madison U
- Drexel University
- University of Maryland (Baltimore County)
- University of North Carolina, Charlotte
- West Virginia U
- Georgia Tech
- Syracuse U
- Purdue U
- Stanford
- UC Davis
- University of Illinois
- University of Idaho
- University of Tulsa
- Mississippi State U
- Norwich U

4 DoD Institutions
- Naval Postgraduate School
- United States Military Academy, West Point
- Information Resources Management College (IRMC)/National Defense University (NDU)
- Air Force Institute of Technology
- George Washington U (DC)
- Indiana University of Pennsylvania (PA)
- New Mexico Tech (NM)
- North Carolina State U (NC)
- Northeastern University (MA)
- Polytechnic University (NY)
- State University of New York at Buffalo (NY)
- State University of New York at Stonybrook (NY)
- Towson University (MD)
- University of Maryland, University College (MD)
- University of Nebraska at Omaha (NE)
- University of Texas at San Antonio (TX)
Disciplines & Programs of Study

- Computer Science
- Computer Engineering
- Software Engineering
- Computer Programming
- Computer Support
- Data Base Administration
- IA Training, Education & Mgmt
- Defensive Information Systems
- Threat & Vulnerability Assessment
- Computer Systems Analysis
- Information Security
- Electrical Engineering
- Electronic Engineering
- Mathematics
- Biometrics
- And more…
- Operations Research
- Risk Management
- Systems Security Engineering
- Information Security
Resources: IA Publications

Information Assurance Technology Center (IATAC)
- IA tools reports
- Critical reviews and technology assessment reports
- State-of-the-art reports
- IA Newsletter
  - Published by DTIC/IA Technical Analysis Center (IATAC)
  - 703-289-5454 or iatac@dtic.mil or http://iac.dtic.mil/iatac
Information Assurance Digest (distribution limited to DoD)
- Published by DTIC/IATAC for the Joint Staff
- Request
  - Fax to Joint Staff (J6) @ 703-614-7814
  - E-mail to iatac@dtic.mil
- Articles extracted from magazines & newsletters (IA “early bird”)
- Integrated Conference/Meeting Event Calendar
  - To add event E-mail iatac@dtic.mil
Resources: IA Publications

- **Tech Trend Notes (Preview of Tomorrow’s Information Technologies)**
  - Published by NSA: 301-688-0842, or ttnotes@tycho.ncsc.mil

- **Computer Forensics Communication**
  - Published quarterly by Defense Computer Forensics Lab
  - http://www.dcfl.gov (look under “quarterly bulletins”)

- **The Internet as an Investigative Tool**
  - National White Collar Crime Center (NW3C) www.nw3c.org
  - Basic Internet Tools

- **News and Views**
  - Published by Federal Information System Security Educators’ Association (FISSEA)
  - E-mail fisseamembership@nist.gov for membership and newsletter
    - IA awareness, training and education
    - Upcoming conferences, seminars
Resources: Information Assurance Support Environment (IASE)

- Web Site: http://iase.disa.mil
- Information Desk: Operational
  7:30 a.m. - 4:30 p.m. M-F, EST
  - E-mail: iase@ncr.disa.mil
  - Phone: (703) 681-IASE DSN 761
- Notices on What’s New Area
- IA Daily News
- Question of the Week
- Chat Room
- Bulletin Board System
- Mail List Subscriptions
Resources: Security Guides - DISA

Security Technical Implementation Guide (STIG)
Download -- http://ia.se.disa.mil/techguid/stigs.html

- Database STIG
- Logical Partition STIG
- MVS STIG
- Network Infrastructure STIG
- Novell Netware STIG
- Windows NT STIG
- Tandem STIG
- Unisys STIG
- UNIX STIG
- Web Application STIG

- Windows 2000

Best Practices
Resources: Security Guides - NSA

- Systems and Network Attack Center (SNAC)
  - Guide to Securing Microsoft Windows NT Networks & Applications
  - 410-854-6529

- Windows 2000 Security Recommendation Guides (SRG)
  - inf. Files
  - configuration guide
  - supporting documents

- Cisco Router Guides
- E-mail and Executable Content Guides
- Supporting Documents

Best Practices
The Center for Internet Security

- [http://www.cisecurity.org](http://www.cisecurity.org)
- Non Profit Consortium of Government, Industry, Academia
  - Security Benchmarks
  - Best Global Practices
  - Make-up: Network Security Vendors, Hardware Software Developers, Consultants
- Member Supported
Resources

◆ National Cyber Security Alliance: Stay Safe Online
  ◆ http://www.staysafeonline.info/
  ◆ Corporate and government members, sponsors
  ◆ Educate home/small business computer users in basic computer security practices,
  ◆ Personal computer security self-test
  ◆ Beginner’s guides on various security topics
  ◆ One-hour online course on security fundamentals

◆ CyberCrime
  ◆ http://www.cybercrime.gov
  ◆ Maintained by DOJ, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division
  ◆ Ways computers can be used to commit crimes
  ◆ How and to whom to report computer crimes
  ◆ What to do if you are the victim of computer crime.
  ◆ Links to cases, laws, legal issues, and policy issues surrounding hacking, intellectual property infringements, and other online offenses
Resources

◆ Hoax Busters
  ◆ http://hoaxbusters.ciac.org
  ◆ DOE Computer Incident Advisory Capability (CIAC)
  ◆ Clearinghouse of information about various types of Internet hoaxes
    ◆ Fake viruses and other malicious code
    ◆ Chain letters
    ◆ Urban myths
    ◆ Sympathy letters and other cons
  ◆ How to recognize hoaxes and what to do about them.

◆ Center for Education and Research in Information Assurance and Security (CERIAS)
  ◆ http://www.cerias.purdue.edu/
  ◆ Free security seminar on diverse security topics (Weds afternoons)
  ◆ Access via live internet stream.
  ◆ Computer security resources for K-12 teachers
    ◆ background information
    ◆ lesson plans
    ◆ links to other web resources
Resources

- Computer and Information Ethics on WWW
  - [http://www.ethics.ubc.ca/resources/computer/](http://www.ethics.ubc.ca/resources/computer/)
  - University of British Columbia’s Centre for Applied Ethics
  - Lists web sites, electronic & print publications on ethical issues in computing.
  - Courses in computer ethics
  - Provides links to online syllabi to classes
  - Links to relevant organizations.

- Security Statistics
  - Statistics on computer security incidents
  - Information on
    - Security spending,
    - Known vulnerabilities,
    - Numbers of reported security breaches
    - Economic impact of incidents
    - Arrests and convictions,
  - Accuracy of reported statistics not guaranteed; but sources are provided