Proposal to Establish
the IEEE CS
Task Force on Information Assurance

presented by

Jack Cole

1. Motivation

- Information Assurance is a youthful and extremely active, rapidly growing field overlaying a greater number of existing areas of information technology. The need to draw these many areas together to form Information Assurance answers is equally urgent, and needs to be equally rapid to make Information Assurance succeed.

- In its youthful beginning, Information Assurance heavily emphasizes operational aspects, while relevant research and standards are just beginning.

.

- There is immediate need for great strides in technology to effect Information Assurance even in modestly distributed computing environments. Information Assurance technology needs to mature to the point that it leads the target through research and imagination.

- Computing and Communications Technologies are advancing rapidly, much more rapidly than Information Assurance Technology, presenting an increasingly unbalanced and difficult environment in which to effect Information Assurance.

- Growth is phenomenal in kinds and volume of information to which proper access must be assured.

- Malicious human attacks on information systems are rapidly evolving, mutating into even greater numbers and kinds of attacks. And there are no good answers for insider attacks.

- Advances needed in Information Assurance Technology can be greatly expedited by the leadership of this Technical Committee to coalesce the present array of many splintered efforts, bringing experts and other interested parties together, speaking with a central voice, become an authority based in IEEE, and providing a “home” for Information Assurance.

- No known accredited standards development organizations are developing Information Assurance standards. This TC will work together with a committee of the IEEE toward development of standards.

- No other single technical committee (of IEEE, ACM, etc) covers the breadth of technical areas required to advance Information Assurance Technology through a holistic approach. Although this proposal recognizes the existence of committees that focus on topics integral to Information Assurance.

2. Names of individuals involved in the TF Executive Committee (TENTATIVE, no particular order):

   - Mr. Jack Cole, initial TF chair
     Computer Technologist, US Army Research Laboratory (ARL)
     Information Assurance Center (IAC)

   - Mr. Robert J. Reschly, Jr
     Engineering Technician, ARL IAC
     Architect of the Defense Research Engineering Network (DREN)
     ARL Lead for the IAC's Center for Intrusion Monitoring and Protection (CIMP)

   - Dr. Gerrald Masson
     Director of the Johns Hopkins Information Security Institute
     Former Department Head for the JHU EE&CS Department

   - LTC Dan Ragsdale
     Assistant Professor and Senior Research Scientist
     The United States Military Academy
     Information Technology and Operations Center

   - Dr. Ethan Miller
     Assistant Professor, Department of Computer Science
     University of California at Santa Cruz

   - Mr. Ken Renard
     Security Consultant
     WareOnEarth Communications, Inc

   - Mr. Robert Chadduck
     Computer Systems Analyst
     National Archives and Records Administration

   - Dr. Ray Vaughn
     Associate Professor, Department of Computer Science
     Center for Computer Security Research
     Mississippi State University

- LTC Donald J. Welch
  Associate Professor, Electrical Engineering & Computer Science
  The United States Military Academy

- MAJ Gregory Conti
  Instructor, Electrical Engineering & Computer Science
  Military Intelligence Information Systems Engineer
  The United States Military Academy

3. Individuals who will be interested in working in the TF
   (an understated list of likely sources of individuals):

   - Members of the TF Executive Committee

   - Individuals who currently organize these and other workshops

     2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop
     http://www.itoc.usma.edu/Workshop/2001/Workshop2001.htm

     Information Assurance Technical Framework Forum
     http://www.iatf.net/

     Workshop on Information-Security-System Rating and Ranking
     http://www.acsac.org/measurement/index.html

     IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'00)
     Concurrent Engineering Research Center
     West Virginia University
     http://www.cerc.wvu.edu/

     ACM Symposium Access Control Models and Technologies
     ACM Conference Computer, Communications Security

   - People who currently publish in

     - International Association for Cryptologic Research Journal of Cryptology
     - Transactions of the Systems, Man, and Cybernetics (SMC) Society
     - Others Publications

   - Editor of the SMC Transactions, Journal of Cryptology, …
   - Faculty who teach IA Courses
   - Practitioners in the fields of IA, Security, Networking, Mobile Networking, Network Management, Net-attached Storage, Data Engineering, Operating Systems, Communications, Datamining, Pattern Recognition, Software Engineering, Mobile

Code, Cryptology, Privacy, Computer Forensics (Carpe Machina), Document Management

- Members from Government agencies:

  - DARPA Research on Survivable Systems, Predictability and Security of High Performance Networks, etc
  - DOD NSA National InfoSec Education and Training Program (NIETP) Centers Of Academic Excellence in Information Assurance Education
  - DOD Defense Research & Engineering High Performance Computing Modernization Program
  - DOD Defense Information Systems Agency (DISA), DOD Computer Emergency Response Team (CERT)
  - DOD Army Research Laboratory (Information Assurance Center, Center for Intrusion Monitoring and Protection, Biometrics Research, …)
  - DOD Navy, Office of Naval Research (ONR), Multidisciplinary University Research Initiatives (MURIs) in Critical Infrastructure Protection (CIP)
  - DOD Defense Wide Information Assurance Program (DIAP)
  - DOE LLNL Computer Security Technology Center Network Intrusion Detection (NID) Software
  - DOE Computer Incident Advisory Center (CIAC)
  - FBI National Infrastructure Protection Center (NIPC)
  - National Archives and Records Administration (NARA)
  - NIST National Information Assurance Partnership (NIAP)
  - NCO (National Coordination Office, an office of the White House), Information Technology R&D, Producers of PITAC Report, High Confidence Systems & Software Coordination Group

- Members from Non-Government Activities
  - Forum of Incident Response and Security Teams (FIRST)
  - Security Proof of Concept Keystone (SPOCK)
  - GridForum (cluster computer and the infrastructure for things like remote data access, see TFCC)
  - Information Assurance Technical Framework Forum
  - The Privacy Foundation

- Members from Academic institutions
  - Johns Hopkins Information Security Institute
  - United States Military Academy Information Technology and Operations Center
  - Institute for Security Technology Studies at Dartmouth
  - Mississippi State University, Center for Computer Security Research
  - Carnegie Mellon Software Engineering Institute Computer Emergency Response Team (CERT©) Coordination Center
  - Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University

- Members from Professional Societies, SDOs
  - IEEE Computer Society (TFCC, TCSP, MSC 1363 Public Key Cryptography standards, …)
  - IEEE Communications Society
  - IEEE Systems, Man, Cybernetics Society
  - The Internet Society
  - Association for Information and Image Management (AIIM)
  - National Committee for Information Technology Standards (NCITS)
  - The International Association for Cryptologic Research
  - ACM Special Interest Group (SIG) on Security Audit & Control (SAC) http://www.acm.org/sigsac/

4. Method for attracting new members

- Substantial Advertising of New IEEE Task Force on Information Assurance
  - In IEEE and ACM Publications
  - At Online E-zines in Related Fields
  - Through E-Mail Reflectors of Various Groups
  - By direct contact with other organizations within IEEE (including Communications Society), ACM, NCITS, AIIM
  - Through personal contact and participation in symposia, conferences, and business meetings

- Direct Contact with each of the numerous organizations with interest
- Sponsoring Meetings Around the US, and Overseas When TF Matures
- Establishing a web presence
- Recruitment from Information Assurance workers in industry, government, and academe

5. Plans which the TF hopes to accomplish over the next two+ years

- 2001:
  - Solidify Executive Committee (Expect 20-30 members), Organize ExCom according to work needed, talent available
  - Establish Web Presence and Email Reflectors
  - Build General Membership
  - Develop Real Budget
  - Refine Task Force Charter
  - Prepare Plans for Publications, Workshops/Symposia/Conferences, Projects
  - Initiate a newsletter on current projects within the TF or sponsored by the TF.
  - Apply for Elevation to Technical Committee

- 2002:
  - Sponsorship of the first conference on Information Assurance
  - Cooperate in several existing conferences, workshops etc.
  - Propose theses and/or research projects to institutes

- 2003:
  - Regular Sponsorship of a biennial conference on Information Assurance
  - Transition newsletter into a magazine.

6. The way to benefit CS members

   Regular members who work in the Information Assurance profession and student members working toward information assurance degrees will be able to participate in a technical committee with a scope of topics matching their experiences.

   Policy makers in Government and Industry will easily identify the Technical Committee for Information Assurance as a group that understands the breadth of area, and promotes research and standards in this area as an IEEE authority.

   The independence of the IEEE Technical Committee for Information Assurance from proprietary interests in commercial products and political interests in other groups will permit it to assume a position of trust in evaluating technologies for Information Assurance.

   The IEEE Technical Committee for Information Assurance will be directly involved with a companion standards committee for information assurance. The TC will work closely with the SC in its study groups and in its development of guides, recommend practices, trial use standards, and full standards. Initially, the committee is interested in standards for protocols and platforms used in intrusion detection.

   Thus the CS and its members which till now have barely participated in such activities, possibly at the individual level only, will benefit from finding itself a part of this new technology and trend. It is expected that the ability to participate in this committee will result in a great number of new IEEE and CS members from the enormous pool of workers in information assurance who will be recruited.

7. The way to become a "major player" in the particular area of concentration

   The Information Assurance Workshop sponsored by the IEEE Systems, Man, and Cybernetics (SMC) Society will hold its second annual workshop this June. The organizers of the workshop have stated that the association with the SMC Society is weak, and that they would be pleased to be sponsored by the CS TF for Information Assurance. Note that the SMC Society has activities in areas relevant to Information Assurance (pattern recognition, man-machine interface, etc), and that the TFIA will make a strong effort to draw expertise from the SMC Society.

Contacts with industry developing hardware and software products, services for Information Assurance already exist for members of the TFIA ExCom and for elements of the CS. The existence of the TFIA (later TCIA) would confirm and strengthen these ties.

The TCIA will become the rallying point for every activity that sits in the mainstream of Information Assurance, thus avoiding dispersion in related fields, for practitioners of the field, for interested institutes and commercial interests.

8. Budget: Details for two years

Once approved, the TFIA ExCom will have to develop a specific budget for the remainder of 2001, and be prepared for the January submission of a full-year budget, submitting an estimate earlier on.

The maximum budget for a new TF ($3K?) is not an excessive amount to cover reasonable expenses of the TF in its operations. The TF will attempt to rely on the sponsoring organizations of its members for coverage of travel costs and donation of other resources.

TAB assistance in funding for meetings and communications should be avoidable or quite minimal in 2001.

Funds for Newsletter and related expenses (communication among committees, authors, etc.) will depend on the size of the mailing list developed, the need for FEDEX/UPS of documents (avoidable), the need for art work/graphics for newsletters, brochures, and the cost of advertising. At the time of this proposal, those costs are less knowable than after the first ExCom meeting.

After approval, the TFIA will discuss the necessity for TAB funding assistance to take over the existing SMC sponsored workshop.

Travel support for the officers to attend the meetings necessary to organize the workshop may be an issue, but sponsor support for this, too, will be sought.

Funding to create a new magazine might be substantial, but associated costs will not occur until 2002. The TFIA will discuss costs with individuals such as the “COMPUTER” magazine staff.

9. Type and Frequency of Communication the TF should have with its membership

The TFIA will produce a quarterly newsletter. At first, this newsletter will be distributed online and in print. If the readership does not need the print version, only the online version will be supported.

Yes, there will be lots of e-mail among individuals, and if necessary, faxes sent. News groups are less used now than ten years ago, but threaded discussion groups will be established online.

10. TC's, SIG's and other organizations which have an interest and/or activities in this area. Type of services which the TF provides and other groups do not.

    While groups exist that relate to Information Assurance as a fringe area of CS, no engineering groups exist which are dedicated to Information Assurance and *collectively* to these activities (*not an exhaustive list*):

    - cryptography
    - networking
    - software engineering
    - microarchitecture
    - simulation
    - pattern recognition
    - human factors
    - visualization
    - data engineering, mass storage systems, digital libraries
    - clustered computing
    - distributed processing

    The TC will be breaking new ground, presenting the same holistic view of these topics held by groups in industry, academe, and government. The TC formed will be viewed as being entirely independent of other technical committees, and will not be absorbed by others.

    However, the TC formed will collaborate promiscuously with other groups and organizations, including IEEE CS TCs focusing on these sub-areas.

    To understand why Information Assurance is a unique area, it is important to define "Information Assurance", and to see where Information Assurance began, what its present activities are.

    The broadest definition of "Information Assurance" is:

    > To assure undisturbed, timely availability of information according to authenticated recipient and authorized uses in highly-distributed, heterogeneous computing environments.

    Information is the raison d'etre for computing, and the value of information is greatest when it can be accessed at the time of need. While there is great emphasis on cyber attacks to systems and networks, Information Assurance pertains as well to impediments (disturbances) to access from other causes, including accident and unbalanced development

in areas of information technology. An example of the latter: storage capacity is growing at ten times the rate of storage throughput.

Consider the Presidential Decision Directive 63 (May 1998, Clinton) which gave rise to Information Assurance:

> ”Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation’s critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.”

The central focus today in Information Assurance is intrusion detection systems and near-real-time reaction (e.g., blocking ports). Operations and detection remain a strong focus of Information Assurance, and great strides are urgently needed in technology for intrusion detection alone. While humans can only read at the rate of 100 kilobytes/day, some information operations guard traffic amounting to terabytes/day.

It is now appreciated that Information Assurance needs both to lead the target and to build Information Assurance into components of systems (networking, storage, software, etc.). The present state of Information Assurance is a superficial response to events and actions which occurred relatively long ago.

IEEE CS TCs with significant overlap

- Security & Privacy
- Data Engineering
- Mass Storage
- Cluster Computing
- Computer Communications
- Digital Libraries
- Distributed Processing
- Fault Tolerant Computing
- Human Centered Information Systems
- Pattern Analysis and Machine Analysis
- Simulation
- Software Engineering
- Visualization and Graphics
- Virtual Intelligence

IEEE CS TCs with lesser overlap
- Complexity in Computing
- Computer Architecture
- Microprocessors and Microcomputers
- Microprogramming and Microarchitecture
- Operating Systems
- Wearable Information Systems

SIGs
- ACM Security Audit & Control SIG

Others
- IEEE Systems, Man, and Cybernetics Society

11. Conferences the TF will create or contribute to

- 2nd Annual Systems, Man, and Cybernetics IA Workshop, June 2001
- Workshop on Security in Storage, Supercomputing, November 2001
- 10th NASA – 19th IEEE Mass Storage Systems Conference, April 2002
- First IEEE Information Assurance Symposium (Month, Location TBD) 2002 in cooperation with …

12. Potential Topics for books/tutorials/videos/disks the TF can produce. This list patterned after the Johns Hopkins Information Security Institute's list of topics. Many or most of these products would be developed in cooperation with a number of other technical committees, IEEE and otherwise. Not all of those committees are listed, nor a notation made at every instance where cooperative effort would be required.

- Technical
  - Information Warfare (Military, Economic, or Socio-Political)
  - Critical Infrastructure Protection (CIP)
  - Multi-disciplinary University Research Initiatives (such as CIP)
  - Insider and outsider intrusion detection
  - Secure wireless and wired telecommunications (in cooperation with LAN/MAN, Communications Society, TCSP)
  - Robust software (in cooperation with software engineering, TCOS, and others)
  - Distributed computing (in cooperating with the community of the same name, the TFCC, and GridForum)
  - Information forensics, surveillance, and audit (in cooperation with ACM SIGSAC)
  - Archival issues (in cooperation with TCMS, TCDE, and others)
  - Cryptology and encryption methodologies (in cooperation with TCSP, P1363)
  - Trusted man/machine interfaces and information search/retrieval of massive databases

  - Management of information security

- Economic and Financial
  - E-commerce and web-based services (e.g., WBEM) security
  - Public policies and standards
  - International electronic business
  - International policy protocols
  - Trusted agents
  - National and international economics
  - Intellectual property protection and digital copyrighting

- Legal & Policy
  - Computer ethics and privacy
  - Computer law and criminology
  - International policy protocols
  - Public policies and standards
  - Web-based Intellectual Property Rights

- Privacy and Ethics
  - Database confidentiality and protection
  - Information authentication
  - Protection of Minors
  - Privacy of Medical Records
  - Privacy of Consumer Purchases, Records
  - Identity Theft
  - Privacy of consumer phone calls, email, …
  - Internet “stalkers”

- Human Dynamics affecting Information Assurance

13. Presenter Information

Jack Cole
Computer Technologist
Information Assurance Center
US Army Research Laboratory

jack.cole@ieee.org
http://www.ieee-sssc.org/cole
01.410.278.9276 desk
01.410.688.1621 cell (6am-10pm ET)

- Sponsor Chair for the IEEE Storage Systems Standards Committee
- Past Chair of the IEEE Storage Systems Standards Working Group
- Led the IEEE Working Group through Development, Balloting and Approval (June and December 2000) of the World's First Storage System Standards.
- Elected Executive Member of the TC for Mass Storage (1999)
- Program Committee Member, Speaker, Tutorial Session Chair for the 18th IEEE – 9th NASA Mass Storage Systems Symposium in San Diego, April 17-20, 2001.
- Elected to Senior IEEE Member status (March 2001)
- Member of the 2002 Program Committee for the 10th NASA Goddard Mass Storage Systems Conference.