International Federation for Information Processing

TC-11 Security and Protection in Information Processing Systems

Factsheet

WG 11.10

Critical Infrastructure Protection

Version: 22 May 2006

Introduction

(Strategic issues / questions: Introduction and mission statement)

Working group 11.10 Critical Infrastructure Protection was founded in February 2006.

The “information infrastructure” – comprising computers, embedded devices, networks and software systems – is vital to day-to-day operations in every sector: agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Global business and industry, governments, indeed society itself, cannot function effectively if major components of the critical information infrastructure are degraded, disabled or destroyed.

Starting in the late 1990s, several countries launched critical infrastructure protection efforts. These efforts grew in size and scope in the aftermath of the September 11, 2001 terrorist attacks. Practically every developed country instituted sustained infrastructure protection programs within the various sectors, and undertook strong efforts to understand the interdependencies between sectors. But the information infrastructure is a global resource, and serious attempts must be made to draw the international community – governments, private sector entities and researchers – to the shared task of critical infrastructure protection.

The United States, the European Union and other countries are cooperating on several major initiatives related to critical infrastructure protection. However, these international initiatives mainly involve governmental and quasi-governmental agencies and the private sector. Few efforts have engaged academia and the larger international research community to address scientific and engineering problems that are crucial to securing the global information infrastructure.

IFIP Working Group 11.10 on Critical Infrastructure Protection seeks to fill this void. IFIP WG 11.10 will attempt to engage the international information security research community to work

together on applying scientific principles and engineering techniques to address current and future problems in information infrastructure protection. In addition to engaging the research community, IFIP WG 11.10 will strive to draw other interested parties (government agencies, infrastructure owners, operators and vendors, and policy makers) in a constructive dialog on critical infrastructure protection. IFIP WG 11.10 will endeavor to cooperate with other IFIP TC 11 working groups. Furthermore, WG 11.10 will reach out to other IFIP working groups, especially WG 10.4 (Dependable Computing and Fault Tolerance).

Aims and scope ***(last revised / reconfirmed February 2006)***

(Strategic issues / questions: What does the TC address, what does it want to achieve, what are the groups of people the working group focuses on, what are the boundaries of the work area)

The principal aim of IFIP WG 11.10 is to weave science, technology and policy in developing and implementing sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. Information infrastructure protection efforts at all levels – local, regional, national and international – will be advanced by leveraging the WG 11.10 membership's strengths in sustained research and development, educational and outreach initiatives.

The scope of IFIP WG 11.10 is:
• To identify information security challenges and implementation issues that are common (as well as unique) to infrastructure sectors.
• To elucidate the interdependencies existing between infrastructure sectors and their information security implications.
• To identify core security principles and techniques that can be applied to address problems in information infrastructure protection.
• To develop sophisticated information infrastructure protection solutions that blend scientific methods, engineering techniques and public policy.

Products, services and activities ***(last revised / reconfirmed February 2006)***

(Strategic issues / questions: What are the products and activities the working group will deliver)

IFIP WG 11.10 will host an annual international conference as well as one or more technology transfer workshops each year.

• International Conference: The Annual IFIP WG 11.10 International Conference will provide a forum for presenting original, unpublished research results and innovative ideas related to information security and critical infrastructure protection. The annual conference will attract key members of the community – researchers, infrastructure owners, operators and vendors, and policy makers – to examine the current state of research and practice in the discipline, analyze problems and trends, and discuss potential solutions. Each conference will be organized around a specific theme based on the interests of the WG 11.10 membership and pressing research issues related to critical infrastructure protection. To maintain an intimate working group atmosphere and enhance personal interactions between researchers and practitioners, the annual conferences will be limited to 50-60 attendees.
WG 11.10 will disseminate, to the widest possible extent, the results of each annual conference and the accompanying discussions, including original research, practical experiences and innovative ideas in

critical infrastructure protection. Research results from the annual IFIP WG 11.10 conferences will be published by Springer (New York) as books in the new series, Critical Infrastructure Protection: Issues and Solutions. In addition, selected papers from the conferences will be published in special issues of scholarly journals.

• Technology Transfer Workshops: Between one to three technology transfer workshops will be organized each year to showcase advances in critical infrastructure research and practice to the larger community of stakeholders, and to solicit input on research trends and needs. The technology transfer workshops will provide important visibility for WG 11.10, while ensuring that the research results related to critical infrastructure protection have practical application. To allow for effective interactions, workshop attendance will be limited to approximately 60 invited participants.

Membership rules ***(last revised / reconfirmed February 2006)***

(Strategic issues / questions: Membership rules)

IFIP Working Group 11.10 will have two membership categories: members and observers. No membership fees will be levied on members and observers.

• Members: IFIP WG 11.10 members are expected to be qualified researchers, practitioners and/or educators with strong interests and experience in critical infrastructure protection. Members will be nominated by the Working Group Chair, subject to IFIP approval. Members are expected to participate in Working Group activities. At a minimum, members must present a paper at a WG 11.10 conference or workshop, or take an active role in the organization of a conference or workshop at least once every three years. A three-year period of inactivity is taken to indicate that a member is no longer interested in the technical area.

• Observers: IFIP WG 11.10 observers are expected to be qualified researchers, practitioners and/or educators with interests and/or experience in critical infrastructure protection. Observers will be nominated by the Working Group Chair, subject to IFIP approval. Individuals attending or presenting papers at WG 11.10 conferences or workshops will be offered observer or member status. Observers who do not attend at least one WG 11.10 event every three years will lose their status. A three-year period of inactivity is taken to indicate that an observer is no longer interested in the technical area.

Contact details

Contact of working group chair:

- xx
  Telephone:
  Fax:
  E-mail:

Home page and mailing address of the group:

- http://

Annex a. Membership

- **Officers, current**

Chair:	Sujeet Shenoi, USA	first three-year term, Febr. 2006 – Febr. 2009
Vice-chair:	Eric Goetz, USA	first three-year term, Febr. 2006 – Febr. 2009
Secretary:		first three-year term, May 2006 – May 2009

- **Membershiplist, confirmed in TC-11 meeting of May 2006**

Australia	Andrew Clark, Queensland University of Technology
Australia	Jill Slay, University of South Australia
Australia	Craig Valli, Edith Cowan University
Canada	Eric Byres, British Columbia Institute of Technology
Canada	John Kluver, Industry Canada
Italy	Paolo Donzelli, Prime Minister's Office
Italy	Marcelo Masera, European Commission, Joint Research Centre
Netherlands	Eric Luiijf, Clingendael Center for Strategic Studies and TNO Defence
New Zealand	Malcolm Shore, University of Canterbury
Norway	Stig Johnsen, SINTEF
South Africa	Les Labuschagne, University of Johannesburg
South Africa	Martin Olivier, University of Pretoria
Spain	Javier Lopez, University of Malaga
Switzerland	Myriam Dunn, Swiss Federal Institute of Technology
Switzerland	Adrian Gheorghe, Swiss Federal Institute of Technology
Switzerland	Tillman Schulze, EBP
UK	Maitland Hyslop, Northumbria University
USA	Robert Bruce, Dartmouth College
USA	Benjamin Cook, Sandia National Laboratories
USA	Robert Cunningham, MIT/Lincoln Laboratories
USA	Matthew Devost, Terrorism Resource Center
USA	Scott Dynes, Dartmouth College
USA	Eric Goetz, I3P/Dartmouth College
USA	Seymour Goodman, Georgia Tech
USA	Yacov Haimes, University of Virginia
USA	Jeffrey Hunker, Carnegie Mellon University
USA	Shari Lawrence-Pfleeger, RAND
USA	Ulf Lindquist, SRI International
USA	Wayne Meitzler, Pacific Northwest National Laboratories
USA	Mauricio Papa, University of Tulsa
USA	Jeffrey Picciotto, MITRE
USA	Christine Pommerening, George Mason University
USA	William Sanders, University of Illinois
USA	Sujeet Shenoi, University of Tulsa
USA	Duminda Wijesekera, George Mason University
USA	Rae Zimmerman, New York University

- **Officers, history**

WG 11.10 was established in 2006, the current team of officers are the first officers for this working group.

Annex b. Workplan

- Past events / products / achievements

- Planned events / activities

Officers and members of the working group will present papers in a special session of the security stream as part of the IFIP World Computer Congress 2006 in August, Santiago de Chile.