ASPECTS OF NETWORK AND INFORMATION SECURITY

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Public Diplomacy Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 17 ISSN 1874-6268

Aspects of Network and Information Security

Edited by

Evangelos Kranakis

School of Computer Science, Carleton University, Ottawa, Ontario, Canada

Evgueni Haroutunian

Institute for Informatics and Automation Problems, National Academy of Sciences and Yerevan State University, Yerevan, Armenia

and

Elisa Shahbazian

Lockheed Martin Canada, Montréal, Québec, Canada

IOS Press

Amsterdam • Berlin • Oxford • Tokyo • Washington, DC

Published in cooperation with NATO Public Diplomacy Division

Proceedings of the NATO Advanced Study Institute on Network Security and Intrusion Detection
Yerevan, Armenia
1–12 October 2005

ISBN 978-1-58603-856-4
Library of Congress Control Number: not yet known

Publisher
IOS Press
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the UK and Ireland
Gazelle Books Services Ltd.
White Cross Mills
Hightown
Lancaster LA1 4XS
United Kingdom
fax: +44 1524 63232
e-mail: sales@gazellebooks.co.uk

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

PRINTED IN THE NETHERLANDS

Aspects of Network and Information Security
E. Kranakis, E. Haroutunian and E. Shahbazian (Eds.)
IOS Press, 2008

Preface

An Advanced Study Institute (ASI) "Aspects of Network and Information Security" was held in Nork, Yerevan, Armenia, October 01-12, 2006. The goal of the ASI was to bring together lecturers of international standing to provide instruction on methods, techniques and applications to deal with the issues of Cyber Security. Participants (post graduate) from NATO, Partner and Mediterranean Dialogue countries had an opportunity to learn and exchange ideas with internationally renowned scientists in the domain as well as students from other countries, developing awareness about methods, solutions and on-going research for Critical Infrastructure Protection, Intrusion Prevention and Threat Assessment globally. This publication is the Proceedings of the Institute.

An ASI is a high-level tutorial activity, one of many types of funded group support mechanisms established by the NATO Science Committee in support of the dissemination of knowledge and the formation of international scientific contacts. The NATO Science Committee was approved at a meeting of the Heads of Government of the Alliance in December 1957, subsequent to the 1956 recommendation of "Three Wise Men" - Foreign Ministers Lange (Norway), Martino (Italy) and Pearson (Canada) on Non-Military Cooperation in NATO. The NATO Science Committee established the NATO Science Programme in 1958 to encourage and support scientific collaboration between individual scientists and to foster scientific development in its member states. In 1999, following the end of the Cold War, the Science Programme was transformed so that support is now devoted to collaboration between Partner-country and NATO-country scientists or to contributing towards research support in Partner countries. Since 2004, the Science Programme was further modified to focus exclusively on NATO Priority Research Topics (i.e. Defense Against Terrorism or Countering Other Threats to Security) and also preferably on a Partner country priority area.

This ASI was conceived as a result of discussions that occurred during the NATO ASI # 979583 between the two co-directors (Dr. Elisa Shahbazian and Prof. Evgueni Haroutunian). The topic of Network Security is one of the currently most critical topics, and both in Canada and in Armenia there are many Universities where various aspects of this topic are being investigated. Being on the Board of Directors of the Canadian University/Industry Network Centre of Excellence on Mathematics of Information Technology and Complex Systems (MITACS) Dr. Shahbazian was confident that many prominent Canadian experts in the domain will be very enthusiastic to lecture in the ASI as well as will be able to involve high calibre experts from other NATO countries, while Prof. Haroutunian was confident that he can involve many prominent expert in the domain from former soviet republics and Eastern Europe.

Network security is concerned with creating a secure inter-connected network that is designed so that on the one hand users cannot perform actions that they are not allowed to perform, but on the other hand can perform the actions that they are allowed to. Network security not only involves specifying and implementing a security policy that describes access control, but also implementing an Intrusion Detection System (IDS) as a tool for detecting attempted attacks or intrusions by crackers or automated attack tools

and identifying security breaches such as incoming shellcode, viruses, worms, malware and trojan horses transmitted via a computer system or network. Intrusion detection is traditionally achieved by examining network communications, identifying heuristics and patterns of common attacks, and taking action to alert network and system managers.

An intrusion-prevention system is a system which when combined with intrusion monitoring and detection via an application layer firewall may terminate connections. Thus, an intrusion prevention system exercises access control in order to protect computers from exploitation by inspecting network traffic (for signs of intrusions) at a deeper level and can make decisions based not only IP address or ports but also on application content and may also act at the host level to deny potentially malicious activity.

Today's computer infrastructure is exposed to several kinds of security threats ranging from virus attacks, unauthorised data access, sniffing and password cracking. Understanding network vulnerabilities in order to protect networks from external and internal threats is vital to the world's economy and should be given the highest priority. Computer and network security involves many important and complicated issues and this gathering of scientists will help not only in raising awareness but also in teaching participants the state-of-the-art of security techniques.

Topics in the following three main areas were discussed during the ASI:

I. Network Security
II. Information Security
III. Coding

The theme of the Institute was scientific communication and exchange of ideas among academic and industrial groups having a common interest in understanding the issues and development of approaches of cyber security.

The technical program was conceived to emphasise the methods and theory in the first week and simulation and applications in the second week. The program included a presentation discussing European Union grant opportunities in Europe for multi-national teams and the ASI ended with a Plenary Discussion on Cyber Security Research Future Developments and International Collaboration. Already during the ASI four groups of participants from various countries started discussions of potential collaborations, namely:

1. Armenia, Switzerland, Italy
2. Armenia, Canada
3. Armenia, US
4. Russia, Canada

The Armenia-Canada collaboration was successfully put in place supported by a NATO Strategic Grant # ESP CLG 982237 in April 2006.

Sixty four lecturers, co-authors and students from Armenia, Austria, Belgium, Canada, Czech Republic, Estonia, Germany, Hungary, Italy, Russia, Switzerland, Turkey, UK and USA participated at the ASI. All lecturers were internationally very highly regarded experts in their domains. Unfortunately due to the fact that the ASI was in October, some other very prominent experts from these and other countries (Greece, Kyrgyz republic, Italy, Russia, Turkey, etc.), who initially expressed much interest and provided abstracts of their lectures, regretfully informed at the last minute that were unable to participate due to teaching commitments. Some of the participants had to also miss a few days from the full 2 weeks of the ASI from the start or the end due to their teaching schedules. At the same time the fact that the ASI was in October and in Yerevan

was very favourable in terms of attracting very large number of Armenian students. 24 Armenian students participated (students and University staff) who attended all days of the ASI. While additional 36 Armenian students signed in and participated in the ASI partially. These were considered as ”visitors” and were not reported as students however gained very valuable opportunity to meet internationally renowned experts and hear their presentations in various aspects of cyber security.

The distinguished faculty of lecturers was assembled and the technical program was organized with the assistance of the Organizing Committee composed of Dr. Elisa Shahbazian (Canada) and Prof. Evgueni Haroutunian (Armenia), Prof. Evangelos Kranakis (Canada) and Gregory Kabatiansky (Russia).

The value to be gained from any ASI depends on the faculty - the lecturers who devote so much of their time and talents to make an Institute successful. As the reader of these proceedings will see, this ASI was particularly honored with an exceptional group of lecturers to whom the organizers and participants offer their deep appreciation.

We are grateful to a number of organizations for providing the financial assistance that made the Institute possible. Foremost is the NATO Security Through Science Programme which provided the most significant portion of the financial support for the Institute. In addition, the following sources made significant contributions: The Mathematics of Information Technology and Complex systems (MITACS) Network Centre of Excellence, Lockheed Martin Canada and Bell University Laboratories of Canada.

We would like to thank the management and the staff of hotel Regineh http: www.hotelregineh.am for ensuring that all the requirements of the ASI were fulfilled and for a truly enjoyable and memorable two weeks in Yerevan. We would like to thank the Institute for Informatics and Automation Problems of National Academy of Sciences of the Republic of Armenia, for allocating personnel to greet the participants at the airport and to facilitate their arrival/departure to/from the hotel. We would like to thank Anna Galstyan, our local interpreter and receptionist, whose competence and warm friendliness made all the attendees feel welcomed at the ASI and comfortable in Armenia. We would also like to thank Armen Malkhasyan and Karine Gasparian for their dedicated efforts to address various local resource requirements, such as ordering conference bags and stationary, communication, transportation and entertainment requirements of the ASI participants, so that the Organizing Committee was able to fully concentrate on the technical program issues.

A very special acknowledgement goes to Ani Shahbazian who Developed and maintained the ASI web site as well as undertook the very challenging task of first performing the English Language editing of all the lecturers' manuscripts and then re-formatting all lectures after the technical editing was complete, producing a camera-ready document to IOS Press Publishers. Thank you for your long hours and hard work.

And, finally, all of our thanks go to the people of Armenia, who certainly displayed, in every way, their warmth and hospitality.

Evangelos Kranakis
Ottawa Canada

Evgueni Haroutunian
Yerevan Armenia

Elisa Shahbazian
Montreal, Canada

October 2007

Contents