

# International Workshop

## *Mathematical Methods, Models and Architectures for Computer Networks Security*

May 21-23, 2001, St. Petersburg, Russia

<http://space.iias.spb.su/mmm2001/>

### **Sponsored by:**

US Air Force: European Office of Aerospace Research and Development (EOARD)

US Navy: European Office of Naval Research International Field Office (ONRIFO)

Russian Foundation of Basic Research (RFBR)

### **Call for Participation**

#### **Organized by:**

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with Russian Foundation of Basic Research (Russia),  
US Air Force Research Laboratory/Information Directorate,  
Binghamton University (USA)

#### **Scope of the Workshop**

The goal of this workshop is to facilitate personal interaction between leading researchers working on various aspects of information technology relevant to security problems arising in large-scale computer networks engaged in information storing, transmitting, and processing. The workshop will provide for an environment conducive to joint brain storming of mathematical and technological problems, developing of mutual understanding and awareness of common “dead ends”, and resulting in generating a methodology in computer networks assurance.

#### **Workshop Chairs:**

Rafael Yusupov, SPIIRAS (Russia)

Victor Skormin, Binghamton University (USA)

#### **Program Co-Chairs:**

Vladimir Gorodetski, SPIIRAS (Russia)

Victor Skormin, Binghamton University (USA)

Leonard Popyack, US AFRL/IF (USA)

#### **International Program Committee**

Kurt Bauknecht (Switzerland)

Harold Carter (USA)

Peter Chen (USA)

Dipankar Dasgupta (USA)

Jose G. Delgado-Frias(USA)

Lynette Drevin (South Africa)

Jiri Fridrich (USA)

Dimitris Gritzalis (Greece)

Alexander Grusho (Russia)

Yury Karpov (Russia)

Igor Kottenko (Russia)

Martin Kutter (Switzerland)

Anatoly Maliuk (Russia)

Catherine A. Meadows (USA)

Nikolay Moldovian (Russia)

Vladimir Orlov (Russia)

Gyorgy Papp (Hungary)

Hartmut Pohl (Germany)

Ravi Sandhu (USA)

Igor Sokolov (Russia)

Mikhail Sycheov (Russia)

Andrey Terekhov (Russia)

Leonid Ukhlinov (Russia)

Vijay Varadharajaran (Australia)

Minerva Yeung (USA)

Louise Yngstrom (Sweden)

Piotr Zegzhda (Russia)

## **International Organizing Committee**

Rafael Yusupov (Director SPIIRAS, Russia)–Chair

Anatoly Tkatch (Russia)–Co-Chair

Irina Podnozova (Russia)

Dmitry Bakuradze (Russia)

Barry Mckinney (USA)

Michael Morgan (USA)

Christopher Reuter (USA)

## **Local Organizing Committee**

Anatoly Tkatch (Russia)-Chair

Raisa Belova (Russia)

Arkady Druzhinin

Liudmila Fedorchenko (Russia)

Oleg Karsaev (Russia)

Igor Lysenko (Russia)

Alexander Pasmurov (Russia)

Anatoly Solodukhin (Russia)

Liudmila Sukhinina (Russia)

## **Preliminary Program**

### **Session 1: Mathematical Methods, Models for Computer Networks and Systems Security**

#### **Invited Speakers**

R.Sandhu (USA). Securing Cyberspace: The OM-AM and RBAC Way.

V.Varadharajan (Australia). Secure Networked Computing.

#### **Regular Presentations**

J.Jurjens (UK). Composability of Secrecy.

O.Karsaev, I.Kotenko (Russia), V.Gorodetski, L.Popyack, and V.Skormin (USA). Agent-based model of Network Security System: A Case Study.

M.Smirnow (Germany). Security considerations and Models for Service Creation in Premium IP Networks.

K.Knorr, and H.Weidner (Switzerland). Analyzing Separation of Duties in Petry Net Workflow.

D.Gritzalis, K.Moulinos, and K.Kostas (Greece). A privacy-enhancing e-business model based on infomediaries.

A.Kostogryzov (Russia). Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ).

P.Zegzhda, and D.Zegzhda (Russia). Secure Systems Design Technology.

### **Session 2. Methods and Models for Intrusion Detection**

#### **Invited Speaker**

D.Dasgupta (USA). Intelligent Decision Support Systems for Intrusion Detection and Response.

#### **Regular Presentations**

A.Tarakanov (Russia). Information Security with Formal Immune Networks.

I.Kotenko (Russia). Mathematical Models of Distributed Attacks against Computer Networks.

D.Summerville, and V.Skormin (USA). Development of the Attack Detection Procedures by Mining of Data Traffic in Computer Networks.

V.Skormin, J. Delgado-Frias, D.McGee, J.Giordano, L.Popyack (USA), V.Gorodetski, and A.Tarakanov. (Russia). BASIS: Biological Approach to System Information Security.

A.Seleznev (Finland). A Methodology to Detect Analyzes in User Behavior Basing on its Temporal Regularities.

H.Singh (UK). Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining.

### **Session 3. Mathematical Basis of Cryptographic Protocols and Steganography**

#### **Invited Speakers**

C.Meadows (USA). Open Issues in Formal Methods for Cryptographic Protocol Analysis.

A.Grusho (Russia). Mathematical Models for Covert Channels.

## **Regular Presentations**

- V.Korjik (Mexico), and K. Morozov (Russia). Generalized Oblivious Transfer Protocols Based on Noisy Channels.
- V.Yakovlev (Russia), and V.Korjik (Mexico). Key Distribution Protocol Based on Noisy Channel and Error Detecting Codes.
- B.Izotov, A.Moldovyan, N.Moldovyan (Russia). Controlled Operations as a Cryptographic Primitive.
- G.Chaddoud, I.Chrisment, and A.Schaff (France). Dynamic Group Key Management Protocol.
- V.Gorodetski, V.Samoilov (Russia), L.Popyack, and V.Skormin (USA). SVD-based Approach to Transparent Embedding Data into Digital Images.

## **Session 4. Applied Cryptographic Systems**

### **Regular Presentations**

- N.Goots, A. Moldovyan, and N.Moldovyan (Russia). Fast Encryption Algorithm SPECTR-64.
- A.Durante. R.Focardi, and R.Gorriery (Italy). CVS at Work: A Report on New Failures upon some Cryptographic Protocol.
- S.Kavut and M.D.Yücel (Turkey). On some Cryptograph IC Properties of RIJNDAEL.

## **Session 5. Access Control, Authentication and Authorization**

### **Regular Presentations**

- S.Barker (UK). A Temporal RBAC Authorization Method.
- I.Cervesato (USA). Typed MSR: Syntax and Examples.
- T.Ryutov, and C.Neuman (USA). The Set and Function Approach to Modeling Authorization in Distributed Systems.
- D.Zegzhda, P.Stepanov, and A.Otavin (Russia). Fenix Secure Operating System Model and Architecture.

### **Round Table Discussion** (preliminary)

What are the important open problems in computer security and how can mathematical methods and models contribute?

## **Workshop Languages**

The Workshop work languages will be English and Russian. Each session presentations will be simultaneously translated.

## **Workshop Proceedings**

Proceedings of the Workshop are published by Springer Verlag Publishers in their series "Lecture Notes in Computer Science".

## **Registration**

All participants are required to register. To get registered for the workshop, please fax the completed and signed registration form at +7-(812)-328-0685 to Ms. Irina Podnozova. Registration form can be downloaded from the Workshop Web site at <http://space.iias.spb.su/mmm2001> linked to the "Registration Form". For any questions concerning registration please contact Prof. Gorodetski V.I. via e-mail [mmm2001-pc@mail.iias.spb.su](mailto:mmm2001-pc@mail.iias.spb.su), or phone (voice) 7-(812)-323-3570 or Ms. Irina Podnozova at [ipp@mail.iias.spb.su](mailto:ipp@mail.iias.spb.su), voice 7-(812)- 328-4446, Fax 7-(812)-328-0685.

Information about registration fee and lodging can be found in Registration form and partially is duplicated below.

## Registration Fee

Technical Program	Early Registration (Before April 15, 2001)	Late Registration (After April 15, 2001)	On Site Registration (Cash only)
	Regular/Student*	Regular/Student*	Regular/Student*
Monday, May 21– Wednesday May 23	\$380 US/\$190 US	\$420 US/\$210 US	\$420 US/\$210 US
Accompanying person	\$120 US	\$150 US	\$150 US

*\*Important: A proof of a student's status must accompany your registration form*

Please note that banking costs should be paid by the participants.

**Registration fee covers:** invitation, three days of the workshop, including two coffee-breaks and one lunch daily, participant's kit, one copy of the workshop proceedings, welcome reception, workshop dinner, transportation from and to airport upon arrival and departure, one city tour.

**Registration fee for accompanying person(s) covers** invitation, lunch daily, welcome reception, workshop dinner, transportation from and to airport upon arrival and departure, one city tour.

### Way of payment *(except on-site registration)*

Registration fee should be in US\$ and forwarded by bank transfer to the account:

SAVING BANK OF THE RUSSIAN FEDERATION

(ST.PETERSBURG CITY OFFICE)

Code SWIFT=SABRRUMMSH1

Account No. 40503840255200201560

St.Petersburg Institute for Informatics and Automation (SPIIRAS)

Please indicate: "Registration fee for participation in the MMM-ACNS-2001 Workshop"

"Name(s) of participant(s)"

*Sorry, we do not accept registration via credit cards.*

### Cancellation Policy

Requests for refunds of registration fee must be directed in electronic form at [mmm2001@mail.iias.spb.su](mailto:mmm2001@mail.iias.spb.su) and faxed at +7-(812)-328-0685 to Prof. V.Gorodetski.

For cancellations received before April 15, 2001 the money will be refunded completely (minus banking interest).

Between April 15 – May 10, 2001, 70 %,

Between May 10 – May 20, 2001, 50 %,

After May 20 – non refundable.

### Workshop Dates

Arrivals: May 20, 2001, Departures: May 24, 2001.

### Housing

Workshop organizers will be willing to assist you with reasonable reservations in downtown hotels from \$52 US/ per room / per night –single room and from \$72 US/per room / per night for double room. For hotel reservation, please contact directly our official Workshop Service agent Intertimes group “ SoFintour “ travel company:

INTERTIMES group.

"SoFintour" travel company,

Al. Nevskij Sq., 2-2016, Hotel "Moskva"

193317, St. Petersburg, RUSSIA

Voice: +7(812)2746001, 2743018, 2743025

Fax: +7(812)2743071, 2746056

E-mail: [tanya@itimes.spb.ru](mailto:tanya@itimes.spb.ru)

Internet: <http://www.itimes.spb.ru>

Contact person: Tatiana Koulikova

More information on this matter including information about hotels and prices see at the Workshop Web site at <http://space.iias.spb.su/mmm2001/>.

### **Preliminary Information about the Workshop Venue**

St. Petersburg is located on the bank of the Finish Gulf in the north–west of Russia and is famous for its lay-out, rivers, canals, bridges, other architectural beauties, art and science museums. May in St. Petersburg is the best time for productive work as well as for visiting theatres and numerous museums. The weather is friendly though unpredictable. More details about St. Petersburg, museums, etc. will be available at the Workshop Web site <http://space.iias.spb.su/mmm2001/>.

Brief information about the Workshop venue can be found at the Workshop Web site <http://space.iias.spb.su/mmm2001/>.

### **Cultural Program**

Organizes are pleased to offer you private tours with your own family or friends, the convenience of sightseeing at your own pace, and the flexibility of a selecting a tour with your own interests in mind. Having your own personal English-speaking guide along with a driver makes all of this possible. More information on this matter including list of sightseeing tours and prices see at the Workshop Web site at <http://space.iias.spb.su/mmm2001/>.

### **Visa and Visa Application Letters**

To come to Russia each participant from abroad will need an entering visa. As a host institution SPIIRAS will handle this issue through arranging for a formal invitation from the Russian Federation Ministry of Foreign Affairs to every participant. To apply for such an invitation we shall need the following details for every individual (workshop participants and accompanying persons):

name of the company:

full business address:

tel & fax ##

position (title):

**&**

***fax copy of the valid passport page with***

first name:

surname:

date of birth:

place of birth:

citizenship:

passport No.:

date of issue:

expiration date:

place of issue:

Please fax the above information to Ms. Irina Podnozova at 7-(812)-328-0685, and e-mail it to her at

[ipp@mail.iias.spb.su](mailto:ipp@mail.iias.spb.su).

For any questions concerning visa arrangement please contact Ms. Irina Podnozova at [ipp@mail.iias.spb.su](mailto:ipp@mail.iias.spb.su), voice 7-(812)- 328-4446, Fax 7-(812)-328-0685.