

# Tutorial on Applied Computing and Applications

## TUTORIAL ORGANIZERS



**CYBERCOM GROUP**

<http://www.cybercom.com/>



**WSEAS**

<http://www.wseas.org>



**Information  
Technologies  
Research**

<http://www.itr.gr>

**Head of Organizing Committee, Dr. Nikolaos G. Bardis**, CEO and founder of Information Technologies Research (ITR), Adjunct Professor, University of Military Education, Hellenic Army Academy, GREECE



**Nikolaos G. Bardis** received the diploma of Computer Engineering and the PhD degree from National Technical University of Ukraine (Polytechnic Institute of Kiev) in 1995 and 1999 respectively. He is an Adjunct Professor University of Military Education,- (Hellenic Army Academy, Hellenic Naval Academy, Hellenic Air force Academy), research scientist at the National Centre for Scientific Research "Demokritos"- Greece on Institute of Informatics and Telecommunications - Net Media Lab and adjunct an Assistant Professor in the Automation Department at the Technological Education Institute (T.E.I) of Chalkida (Greece). His research interests include cryptography and data security, information theory, artificial intelligence, databases, software engineering and applications in Defence and in the Military Applications. He is a member of the Technical Chamber of Greece, TPC COMSOC - IEEE, WSEAS, and ITR.

**Chairman: Ross W Tsagalidis**, CEO and founder of Consulting Security Informatics (CSI).



**Ross W Tsagalidis** is the CEO and founder of Consulting Security Informatics (CSI). He has more than 20 years experience in the field of Information Security Management (ISM) and Risk Management (RM). He received his M.Sc. degree in Computer Science from the Royal Institute of Technology/SU. Ross's professional background: Corporate Security Officer in the corporate sector, Chief Information Security in the Defence Industry as well as Chief Engineer in Information Security in a Swedish Department of Defence Authority. He has also been the CEO for a Telemedicine Company in Sweden and Business Manager Nordic for a US- company. His mission is to increase the awareness, considering benefits of implementing ISM and RM, of Corporate Management and Board of Directors

# **Design of Efficient Algorithms for the Development of High Efficiency Cryptographic Systems and Data Coding for Applications of Secure Information Transmission**

**Marilena Mitrouli**, Assistant Professor, Department of Mathematics, National University of Athens



**Nikolaos Doukas**, Lecture, Department of Mathematics and Engineering Sciences, University of Military Education, Hellenic Army Academy

Time: 20-30 min

## *Abstract:*

Results and Applications of the Research were supported by a grant by the Greek Ministry of Development - General Secretariat for Research and Technology and the European Community Social Funds. The main part of this Research was carried out when the authors where attending the Operational program "PENED 2003:

## **Identification and Access Management (Entitlement Management)**



**Henrik Johansson**, Director Business Unit, Cybercom Sweden East AB

Time: 30-40 min

## *Abstract:*

Entitlement Management is a fairly new term and not always used in a consistent manner. We use it to describe emerging technologies enabling real-time and enterprise-wide enforcement of authorization based on an organization's overall policies. It offers fine-grained and context-aware access controls that adapt to dynamically changing requirements. Full-blown Entitlement Management handles the entire life-cycle of access policy management creation,

enforcement, monitoring, auditing and final archiving of access control policies. Standardized authorization services of this type will be base components in all future IT infrastructures.

These are some typical characteristics:

- 1) **Standards-based.** Rather than embedding authorization in application code, a standardized language is used for access request-response queries. XACML is an obvious choice.
- 2) **External to applications.** Maintenance of access control policies is carried out from a central point. Applications and services are protected by Policy Enforcement Points (PEP) which query the authorization service to determine if access should be granted or denied.
- 3) **Fine-grained.** Fine-grained Access policies consider all aspects of an access request is the subject, the action, the resource being accessed and even the context of the request. High-level and generic policies can be expressed but also very detailed and precise rules matching unique situations.
- 4) **Context-aware.** Environment parameters such as time of day or network location can be considered in access control enforcement but also other types of dynamically changing conditions such as the state of a related application, for instance in a workflow, project or document management system

*Target groups:* Bank, Government, middle-large public business, health care

## IT-Forensics



**Björn Lindeberg**, Director Business Development

Time: 30-40 min

*Abstract:*

The Nordic Forensic Team (NFT) is a part of the Cybercom Group AB, a Swedish Nasaq-OMX public traded company in the IT-consultancy field with at focus on IT-Security.

NFT operates in two major areas: IT-Forensics and Counter Intelligence Services (CIS). In IT-Forensics we investigate Industrial Espionage, International money laundering, Fraud and more specifically credit card fraud under PCI-DSS where we are the only Nordic/Baltic certified QFI.

In Counter Intelligence Services we operate as a private intelligence organization for major European companies. NFT is one of Europe's largest IT-Forensic Investigators and the largest PCI-Forensic Investigator in the Nordic/Baltic region, but more importantly we are one of very few companies that have successfully investigated Industrial Espionage cases, Organized

Crime and Multinational fraud schemes and provided evidence used in a court of law against criminals now behind bars.

We are a contracted IT-Forensic task force team C.E.R.T. to several world leading banks. We are hired by multiple secret services around the globe and have an exceptional track record of handling tough Industrial Espionage cases spanning borders where international police forces have a hard time acting effectively.

*Target groups:* Banking, Finance, Retail, Counter Intelligence, IT Security Emergency counter measures

## **PCI DSS (Payment Card Industry Data Security Standard)**



**Björn Lindeberg**, Director Business Development

Time: 30-40 min

Abstract:

**PCI DSS** - We protect your customers payment card transactions

Many consumers are still hesitant about using their credit cards over the Internet. And often quite rightly, due to the number of crimes involving stolen credit card details is increasing. In view of this, major players such as Visa, MasterCard and more, have agreed on a common standard for handling credit card information. This standard, the Payment Card Industry (PCI) Data Security Standard (DSS), is an international standard that stipulates relatively strict and concrete security requirements. This affects all players handling payment card transactions.

Cybercom helps our customers to identify the card handling environment from a technical and organizational perspective. Our work results in concrete action plans to achieve a secure Card Data Environment quickly and cost-efficiently. Our long-term approach gives our customers a guarantee that PCI DSS compliance is not a one-off occurrence.

*Target groups:* Banking, Finance, Retail

## **Connected Ambulance Care- how to get life vital information across Health Care Service points without losing focus**



**Henrik Johansson**, Director Business Unit, Cybercom Sweden East AB

Time: 30-40 min

*Abstract:*

This session focuses on the benefits of implementing an on-line ambulance information system but also discusses the potential obstacles and ways to avoid them. The session also includes a short demo of the next generation of AmbuLink(R) Mobile from Cybercom. By combining years of experience from the medical area and modern user interface design and technology from the Connected Car concept, Cybercom provides a solution that lets the ambulance personnel focus on their main task at hand - saving lives - without risking to lose vital information!

Cybercom's AmbuLink(R) Mobile is a complete, flexible on-line ambulance information system that uses the Internet and mobile communication solutions to ensure that vital information always reaches the correct location. AmbuLink(R) can be used alongside existing information systems and can be connected to future national systems, such as the National Patient Summary. This means that patient-specific information about medication, allergies, etc. can be accessed directly. AmbuLink(R) Mobile therefore increases patient safety and makes the work of nursing staff/paramedics that bit easier, regardless of where in the country an incident occurs.

AmbuLink(R) is developed in line with current professional requirements and in consultation with nursing staff and experienced system specialists within the healthcare sector.

*Target groups:* Health Care